



Department for
Constitutional Affairs

Public Sector Data Sharing

Guidance on the Law

NOVEMBER 2003

Foreword by the Secretary of State



This guidance sets out the legal framework which applies to data sharing – in particular the use of personal data by the public sector, across traditional organisational boundaries, to achieve better policies and deliver better services for individuals and society as a whole. It is

generally recognised that the framework is complex. This guidance will not remove that complexity: when dealing with the application of many facets of the law, some complexity is inevitable. What this guidance aims to do, however, is provide a route map through the law. It has been produced by the Department for Constitutional Affairs and represents the consensus of legal opinion across Government.

Our view is that there is no inherent incompatibility between the increasingly ambitious scope of public authority service delivery and the legal and administrative conditions that have to be met in order to share data to help achieve that goal. The law, rightly, puts in place safeguards for the use of individuals' data and there are organisational costs involved in meeting those conditions. In a democratic society, it is important that those safeguards exist and are properly applied. This does not mean, however, that further and better use of information should not be made in order to serve the best interests of the individual, of groups, and of society more widely. An appropriate balance must be struck in the specific circumstances that surround each service or policy.

If applied properly, we believe that this guidance will enable public sector bodies to understand that data sharing *can* take place in a way that helps deliver the better services that we all want, while still respecting people's legitimate expectations about the privacy and confidentiality of their personal information.

A handwritten signature in black ink, appearing to read 'C Falconer', written in a cursive style.

Lord Falconer of Thoroton

Contents

| | | |
|----------|---|-----------|
| 1 | Introduction | 6 |
| 2 | Overview of Existing Legal Framework | 8 |
| 3 | Administrative powers | 11 |
| 4 | The Human Rights Act 1998 and the European Convention on Human Rights | 18 |
| 5 | Common Law, Statutory Obligations of Confidence and Statutory Restrictions on the Disclosure of Data | 21 |
| 6 | Key Elements of the Data Protection Act 1998 relevant to Data Sharing | 24 |
| 7 | Any other issues | 30 |
| 8 | Conclusions | 31 |
| | APPENDIX 1 | |
| | Is Data Sharing Intra Vires? | 33 |
| | APPENDIX 2 | |
| | Relevant Considerations for Lawful Sharing of Personal Data | 34 |
| | APPENDIX 3 | |
| | Checklist of Relevant Legal Considerations Relating to Data Sharing Partnerships | 35 |
| | APPENDIX 4 | |
| | The Data Protection Principles | 37 |
| | APPENDIX 5 | |
| | Conditions in Schedule 2 and 3 to the Data Protection Act 1998 | 38 |

1 Introduction

- 1.1 This guidance is intended to be general and to offer key information on relevant legal issues to lawyers and to other interested professionals working in the public sector (including those working for local authorities). It is not intended to be a substitute for specific legal advice on particular issues that may affect different public bodies in different ways. It is hoped that the guidance will increase understanding of the existing legal framework which governs public bodies' powers to collect, use and share personal data. The guidance will also set out how these powers interact with the Data Protection Act 1998, the Human Rights Act 1998, the common law tort of breach of confidence and other relevant legal provisions.
- 1.2 The guidance is written with reference to the law of England and Wales and the statutory provisions that apply in those jurisdictions. However, certain key statutes (such as the Data Protection Act 1998 and the Human Rights Act 1998) apply equally to Scotland.
- 1.3 The guidance is born out of concerns that the existing data sharing powers of public bodies are insufficient to meet policy objectives and to improve service delivery. For example, many local authorities would like to use names and addresses held on council tax databases for other purposes such as debt recovery and the verification of entitlement to benefits and concessions. It would also be more efficient if local authorities could maintain a single database of citizens' names and addresses that they could access for multiple purposes. Legal uncertainty over what is, and what is not, permissible may be inhibiting data sharing by local authorities. Similarly, some government departments have been inhibited from setting up new data sharing initiatives because of doubts as to what their legal powers allow them to do.
- 1.4 One of the purposes of this guidance is to explore the nature and legitimacy of doubts about the existence of data sharing powers and to help bring about a consistency of approach within the public sector. Facilitating lawful data sharing and good practice amongst the public sector is a clearly a key outcome. A detailed survey of the safeguards (legal and otherwise) that exist to ensure the privacy of individuals is, however, outside of the scope of this guidance. Compliance with those safeguards is equally necessary in order to gain the trust of individual citizens and to comply with principles of law in the field of data protection.
- 1.5 Although this guidance is not intended to – and indeed, cannot – address the detail of every circumstance of public sector data sharing, it is appropriate to mention here two specific areas about which particular concerns have arisen. The first is in relation to disclosures of health information for non-health purposes. The level of sensitivity about such information, on the part of both individual data subjects and health professionals, means that the sharing of such data may be particularly problematic. If public bodies, other than those in the health sector, are considering whether access to health information may be useful for *their* purposes, they should bear this caveat in mind. Helpful guidance on the confidentiality of health data can be found in the NHS publication 'Confidentiality: NHS Code of Practice', which can be found at www.doh.gov.uk/ipu/confiden/protect/index.htm The second area that is often raised as of particular concern is that of sharing personal data for statistical purposes. In practice we do not see this as an area of difficulty. If the data to be shared is fully anonymised, then no problems should arise: if the need is for personal data on identifiable individuals, then the sharing should be approached

in the same way as for any other circumstances, as explained in this guidance, i.e. with a clear basis in law and with proper regard for Human Rights, confidentiality and the requirements of the Data Protection Act 1998.

- 1.6 In preparing this guidance, we have consulted with the Information Commissioner, the Local Government Association and with interested government departments.

2 Overview of Existing Legal Framework

Sources of law

- 2.1 There is no single source of law that regulates the powers that a public body has to use and to share personal information. The collection, use and disclosure of personal information is governed by a number of different areas of law as follows:
- the law that governs the actions of public bodies (administrative law);
 - the Human Rights Act 1998 and the European Convention on Human Rights;
 - the common law tort of breach of confidence;
 - the Data Protection Act 1998; and
 - European Union law.
- 2.2 The interrelationship between the above areas of law is quite complex. The starting point is always to determine whether the public body has the power to carry out any proposed data sharing. This will be a matter of administrative law. The next stage is then to consider whether the proposed data sharing might nevertheless be unlawful due to the operation of the Human Rights Act 1998, the Data Protection Act 1998 or the common law tort of breach of confidence. All of these provisions should be interpreted in the light of relevant principles contained in the European Convention of Human Rights and in European Union law. It is recognised that it is not always easy to determine whether data sharing is, or is not, permissible and specialist legal advice will often be necessary.

How to approach questions about data sharing

- 2.3 There is a straightforward sequence of consideration, which should enable a sound judgement to be made about the ability of a public body to share personal data in the public interest:
- a. Establish whether you have the power to carry out the function to which the data sharing relates. In doing so it will be important to ascertain whether there are express statutory restrictions on the data sharing activity proposed, or any restrictions which may be implied by the existence of other statutory, common law or other provisions (see section 3).
 - b. Decide whether the sharing of the data would interfere with rights under Article 8 of the European Convention on Human Rights in a way which would be disproportionate to the achievement of a legitimate aim and unnecessary in a democratic society (see section 4).
 - c. Decide whether the sharing of the data would breach any common law obligations of confidence (see section 5).
 - d. Decide whether the sharing of the data would be in accordance with the Data Protection Act 1998, in particular the Data Protection Principles (see section 6).

In brief: Administrative Law

- 2.4 Administrative law is the body of law that regulates the activities of public bodies. It is an area of law

that has grown rapidly in the last twenty years and it is now well established that the actions of all public bodies are subject to control by the courts by way of judicial review. The jurisdiction of the courts in this regard is 'supervisory' which means that the courts do not generally review the merits of a public law decision but rather its legality, rationality or procedural propriety. Of these three grounds for challenging administrative actions, it is the rules relating to 'illegality' that are most relevant to data sharing. The doctrine of 'illegality' is a fundamental principle of administrative law that states that a public body may not act in excess of its powers. If it does act in excess of its powers, then the act is *ultra vires*. Acts within a public body's powers are said to be *intra vires*. Where questions involving the European Convention on Human Rights are involved, however, the Court will pay much closer attention to the merits of the decision.

- 2.5 According to the principle of legality, powers exercised by central government departments headed by a Minister must be derived expressly or implicitly from statute, common law or the royal prerogative. If there is a relevant statutory provision, then this may operate so as to exclude a department's common law or prerogative powers. This reflects the doctrine of parliamentary sovereignty.
- 2.6 Public bodies that are not central government departments headed by a Crown Minister, for example, the Inland Revenue, Customs and Excise and local authorities, derive their powers entirely from statute. These bodies must not act outside those limited statutory powers. It is a well established principle that express statutory powers should be interpreted so as to authorise by implication the performance of acts reasonably incidental to those expressly granted. This principle is reflected in section 111(1) of the Local Government Act 1972 that provides that local authorities are expressly empowered to do anything which is calculated to facilitate, or is conducive or incidental to, the discharge of any of their functions.
- 2.7 There is no general statutory power to disclose data, just as there is no general power to obtain, hold or process data. As a result, it will be necessary to consider the legislation that relates to the policy or service that the data sharing supports. From this,

it will be possible to determine whether there are express powers to share data, or whether these can be implied from the terms of the legislation. Clearly, express powers to share data give the highest degree of certainty, but it should be borne in mind that such express powers to share data are relatively rare and tend to be confined to specific activities and be exercisable only by named bodies. Implied powers will be more commonly invoked.

- 2.8 It is the function to which the data sharing is ancillary that one must ascertain, rather than an implicit power to share data per se. If the *vires* to do the fundamental activity are not present, there is nothing into which a data sharing power can be implied.
- 2.9 In the case of central government departments headed by a Crown Minister even if a power to share data cannot be reasonably implied, it may still be possible to find a power to share data by relying on prerogative or common law powers. This is an area where complex legal issues often arise.
- 2.10 In exercising a statutory power, it is also necessary for the power to be exercised for the purpose for which it is created. If it is not, the exercise of the power will also be *ultra vires*.

Human Rights, in particular Article 8 of the European Convention on Human Rights

- 2.11 Disclosure of a person's personal data prima facie engages rights under Article 8.1 of the European Convention on Human Rights: this provides that 'Everyone has the right to respect for his private and family life, his home and his correspondence.' While this right is not absolute, interference with it must be justified. In order to justify interference, the public authority will need to show that it is:
- In accordance with the law;
 - In the pursuit of a legitimate aim; and
 - Necessary in a democratic society.

These elements are examined in more detail in Section 4.

Common law and Statutory Duties of Confidence

- 2.12 The common law protects from disclosure information (whether personal or not) that is given in circumstances giving rise to an obligation of confidence on the part of the person to whom the information has been given. Statute also imposes specific obligations in relation to information given for certain purposes.
- 2.13 At common law, and where the statute in question contains a discretion to disclose, the public interest may favour disclosure of the confidential information. So confidentiality is not an absolute bar to disclosure, but one must make a judgement as to where the public interest lies (the more sensitive and damaging the information, the stronger the public interest in disclosure will need to be). This topic is examined in more detail in Section 5.

The Data Protection Act 1998

- 2.14 The current legislative provision relating to data protection is the Data Protection Act 1998 (DPA). The DPA replaces the Data Protection Act 1984 and it implements an EC Data Protection Directive (Directive 95/46/EC) 'on the protection of individuals with regard to the processing of personal data and the free movement of such data' which was adopted on 24 October 1995. The Directive was a response to the greater ease with which data can be processed and exchanged as a result of advances in information technology. Essentially, the DPA provides individuals with a number of important rights to ensure that personal information covered by the Act is processed lawfully. In general terms the Act regulates the manner in which personal data can be collected, used and stored and so is of prime importance in the context of data sharing. Key principles in the DPA that are relevant to data sharing are considered in section 6.

Any other issues

- 2.15 European Law. This is dealt with further in Section 7.

3 Administrative Powers

Relevance of classification of type of public body

3.1 There are many bodies that exercise public and/or governmental functions and are, therefore, subject to public law controls. These bodies include government departments, local authorities, the police, the armed forces, the courts and numerous non-departmental government bodies. The nature of the body, and the relevant statutory provisions which govern its activities, will play a crucial part in determining the legal basis upon which it acts and whether its activities are lawful. In this section detailed consideration will be given to the administrative laws that govern the powers of public bodies to collect, use and share data. It should be noted that if a public body does not have the power or *vires* to collect, use or share data it will be acting unlawfully and the fact that an individual may have consented would not make the activity lawful.

Government departments

3.2 Government departments can be of two types. Firstly, those that are headed by a Crown Minister such as the Treasury, the Home Office, the Department for Work and Pensions, the Department for Education and Skills and the Department for Constitutional Affairs. Secondly, those that are created by statute and that are not headed by a Minister, such as the Inland Revenue and Her Majesty's Customs and Excise.

3.3 In relation to those government departments headed by a Crown Minister, the legal position is that the department derives all of its powers including its powers to collect, use and share data from the following sources:

- Express statutory powers.
- Implied statutory powers.
- Prerogative and common law powers.

3.4 Those government departments that are established by statute do not have prerogative or common law powers but must look to their statutory powers (express and implied) to provide a legal basis for data collection, use and sharing.

Express statutory powers

3.5 Reference to express statutory powers or 'gateways' to share data has already been made. Often these gateways will be enacted to provide for disclosure of information for particular purposes. Such gateways may be permissive or mandatory. Examples of permissive statutory gateways include section 115 of the Crime and Disorder Act 1998 and Regulation 27 of the Road Vehicles (Registration and Licensing) Regulations 2002 (considered further below).

Examples of mandatory statutory gateways include: section 17 of the Criminal Appeal Act 1995 that makes it obligatory for a public body to provide information, when requested, to the Criminal Cases Review Commission in connection with the exercise of its functions; and section 8 of the National Audit Act 1983 that imposes a legal obligation on public bodies to provide relevant information to the National Audit Office.

3.6 It is a matter of statutory construction as to whether a particular statutory gateway authorises disclosure for the particular purpose or purposes contemplated. In construing the statute account must be taken of the HRA and of the DPA.

Assuming that the statute is compatible with the ECHR (particularly Article 8) and that the DPA is complied with in making the disclosure, disclosure in accordance with the provisions of the statute will be lawful. Indeed, the fact that a statutory gateway has been enacted seems likely to satisfy the 'in accordance with law' requirement of Article 8. When considering compliance with the ECHR, a Court will look at whether the particular act of disclosure is compatible as well as the framing of the provision in the abstract.

- 3.7 Questions relating to the scope of express statutory powers to share data may arise. For example, in the Road Vehicles (Registration and Licensing) Regulations 2002 that regulate the keeping of the vehicle registration register it is provided that:

'The Secretary of State may make any particulars contained in the register available for use:

- a. *by a local authority for any purpose connected with the investigation of an offence or of a decriminalised parking contravention;*
- b. *by a chief officer of police;*
- c. *by a member of the Police Service of Northern Ireland;*
- d. *by an officer of Customs and Excise in Northern Ireland; or*
- e. *by any person who can show to the satisfaction of the Secretary of State that he has reasonable cause for wanting the particulars to be made available to him.'* (Regulation 27)

- 3.8 The scope of paragraph (e) in particular may need to be determined as it raises the question of what is a 'reasonable cause' for wanting particulars of the register to be made available. 'Reasonable cause' is not defined in the Regulations nor is it defined in the Vehicle Excise and Registration Act 1994 (under which the Regulations are made). The term 'reasonable cause' must, therefore, be given its plain and ordinary meaning and interpreted in the context of the Regulations. It will be given an objective interpretation. To be a 'reasonable cause'

the cause must be: (a) related to the registration and ownership of vehicles; and (b) it must be for a purpose which reasonably requires the information to fulfil a task which requires a person knowing the identity of a keeper of a vehicle. It would, for example, be appropriate to disclose information about the identity of the keeper of a vehicle to an insurance company where there has been a road accident and the insurance company needs to trace a vehicle in order to pursue a civil claim. Here the ability to establish legal rights depends upon the information being made available. On the other hand, it would not be lawful to disclose particulars from the register for the purposes of a commercial mail shot because, although it may be convenient for the applicant to have the information, it cannot be said that there is reasonable cause. In particular, commercial purposes are not closely linked to the identity of the driver and his link to a vehicle. Lastly, the power to disclose information from the register only relates to individual cases and not to bulk disclosure.

- 3.9 Where the State's coercive powers are engaged, these should not encroach upon individual's rights more than reasonably necessary. The powers of the Serious Fraud Office were considered in *Morris v. Director S.F.O. [1993] Ch 372*, where it was held that its compulsory powers of criminal investigation (under s3(5) Criminal Justice Act 1987) to obtain documents from auditors contained no implied power to subsequently disclose those documents to liquidators or other office-holders. Where office-holders sought disclosure of documents that had been so obtained, those from whom the documents had been seized, or the true owners of the documents (if different) were generally entitled to make representations on the matter.

Implied statutory powers

- 3.10 Where there is no express statutory power to share data it may still be possible to imply such a power. In *A-G v Great Eastern Railway Co (1880) 5 App Cas 473* Lord Selborne LC dealing with the doctrine of *ultra vires* said that:

'... this doctrine ought to be reasonably, and not unreasonably, understood and applied, and that whatever may fairly be regarded as incidental to, or

consequential upon, those things which the Legislature has authorised, ought not (unless expressly prohibited) to be held, by judicial construction, to be ultra vires.'

- 3.11 Many activities of statutory bodies will be carried out pursuant to implied statutory powers particularly as it might be difficult to expressly define all the numerous activities that a public body may carry out in connection with its day-to-day operations. This is particularly so in relation to activities such as data collection and sharing which are not of themselves usually express statutory functions. In order to imply a power to share data, one must first of all be satisfied that the body in question has the *vires* to carry out the basic function, to which the sharing of data is ancillary. Without the power to do the activity there can be no implicit power to share data.
- 3.12 It is clear that government departments that are created by statute do have implied powers to share data where there is no express statutory power to do so. There are a number of authorities that support this in the context of disclosing confidential information to prevent wrongdoing. For example, in *R v Chief Constable of the North Wales Police, ex parte AB [1998] 3 All ER 310* the extent of data sharing power was considered in relation to the disclosure of information about paedophiles to individuals living in an area that put them at risk. Here it was accepted that the police had the power (either implied statutory or common law) to disclose information for the purposes of performing their public duties. A similar conclusion was reached in the case of *Woolgar v Chief Constable of Sussex Police [2000] 1 WLR 25* where it was accepted that the police had the power to disclose information to a regulatory body for the purposes of an inquiry as this was in the public interest. Here, there was clearly a strong public interest for making the disclosure in question.
- 3.13 Whether power to share data can be implied will depend on the facts of the case. Clearly, power to disclose personal information to prevent a crime may be implied if there is no express statutory power. However, where disclosure is for other purposes, for example, where it may be thought to be necessary to promote the economic well-being of the country, it is unclear whether the courts would accept that government departments have authority to make disclosures of personal information particularly if it is on a wholesale basis. Where the public interest justification is not especially strong it would be necessary to take into account the HRA and the principles contained in Article 8 of the ECHR in determining whether powers to disclose data can be implied i.e. whether the disclosure is in accordance with law, is in pursuit of a legitimate aim and is necessary in a democratic society.
- 3.14 The routine disclosure of information by one government body to another public body for that body's purposes on a wholesale basis might be *ultra vires* depending on the purposes for which the information was to be disclosed. For example, if the Driver and Vehicle Licensing Agency regularly disclosed up-to-date address information to the UK Passport Service so that it could issue renewal reminders to passport holders six months before their passport is due to expire, this would be likely to be *ultra vires*. The disclosure of wholesale information in circumstances such as this where the purpose of the disclosure is to ensure that individuals keep their passports up-to-date would also amount to a breach of the common law obligation of confidence.
- 3.15 Finally, in relation to implying powers to share data, account should also be taken of other relevant statutory provisions that might expressly or implicitly prohibit the data sharing that is being proposed. For an example of how a statutory provision might restrict the sharing of data see the section on local authorities and council tax data at paragraph 3.28.
- 3.16 As regards the collection of data pursuant to implied statutory powers, similar considerations apply. Consideration may need to be given as to whether the collection of the data is reasonably incidental to existing statutory powers. For many purposes it will be clear that the maintenance of a database is reasonably ancillary to express statutory powers, e.g. in connection with administrative or personnel functions. Of more concern will be the maintenance of a database that does not clearly fall within a particular public body's existing statutory functions. This is a question that could arise if one or more

public bodies wishes to set up a shared database of information that may enable each to fulfil its statutory functions and so has a multiplicity of purposes. Here the maintenance of the database itself may not fall squarely within the express statutory function of the data collector so reliance may need to be placed on statutory powers implicit to that function.

Prerogative and common law powers

- 3.17 If there is no relevant express or implied statutory power to data share, government departments that are headed by a Minister of the Crown may be able to rely on common law or prerogative powers to share data. The general position is that the Crown has ordinary common law powers to do whatever a natural person may do (unless this power has been taken away by statute), in contrast with bodies which have powers conferred on them by statute and no powers under the common law. Government lawyers have called this principle 'the Ram Doctrine' as it is explained in a Memorandum by the then First Parliamentary Counsel, Sir Granville Ram, dated 2 November 1945. The principle is derived from the Crown's status as either a corporation sole or, alternatively, as a corporation aggregate¹ having all the powers and legal capacity to do things which an ordinary person has power and capacity to do save as may be prohibited by statute whether expressly or implicitly.
- 3.18 In addition to common law powers, the Crown also has 'prerogative' powers. In this guidance the term 'prerogative' is used to refer to powers that are unique to the Crown such as the powers that the Crown has in relation to foreign affairs, defence and mercy. However, the term 'prerogative' is sometimes used to describe all the powers that the Crown has that are not contained in statutory provisions that represent the residue of royal authority left over from the time before the Crown was controlled by law. Historically, prerogative powers are not powers that have been created by the common law.
- 3.19 In accordance with the rule that parliament is supreme, prerogative powers may be limited by statutory provisions whether expressly or implicitly in the same way that common law powers would. Where by statute the Crown is empowered to do what it might previously have done by virtue of its prerogative power, the rule is that it can no longer act under the prerogative power and must act pursuant to the conditions imposed by statute (*A-G v De Keyser's Royal Hotel* [1920] AC 508). Some statutes may expressly preserve the right to act under the prerogative, for example, section 11(1) of the Crown Proceedings Act 1947. There may, however, be a difference between a government department's prerogative and common law powers insofar as an affirmative statutory provision may not remove common law powers.
- 3.20 In relation to data collection, use and sharing, it may be possible to rely on common law or, perhaps, prerogative powers. This has not often been considered by the courts, so there might be an element of risk involved if a government department chose to do so. The degree of risk involved would depend on the facts particularly the nature of the information proposed to be collected and disclosed, the purposes for which it was to be collected and disclosed and the identity of the bodies acting as recipients. For example, in relation to data already being collected pursuant to existing functions, if the purpose of the disclosure is to prevent crime or other serious form of wrongdoing, it seems clear that a government department could rely on its common law or prerogative powers to share data.
- 3.21 The Court of Appeal case of *R v Secretary of State for Health, ex parte 'C'* 2000 1 FLR 627 is authority for the proposition that the Crown has common law power to engage in certain forms of data collection and sharing. This case concerned the lawfulness of the Consultancy Service Index (a list of people about whom there are doubts about their suitability to work with children) established and maintained by the Department of Health. Guidance regarding

¹ A corporation is a number of persons united together so as to be considered one person for the purposes of the law. Corporations can be either aggregate (consisting of many persons) or sole (consisting of one person). Opinion is divided as to whether the Crown is a corporation sole or a corporation aggregate.

the operation of the list was contained in Circular NO. LAC (93) 17. At the time of judgement there was no statutory basis for the list although one is now contained in the Protection of Children Act 1999. In giving the leading judgement Lady Justice Hale relied on the words of Professor Wade as quoted in the case of *R v Somerset ex parte Fewings* [1995] 1 All ER 513 as follows:

'The powers of public authorities are ... essentially different from those of private persons. A man making a will may, subject to any rights of his dependants, dispose of his property just as he may wish ... This is unfettered discretion. But a public body may do none of these things unless it acts reasonably and in good faith and on lawful and relevant grounds of public interest ... The whole conception of an unfettered discretion is inappropriate to a public authority, which possesses powers solely in order that it may use them for the public good.'

3.22 In conclusion, the court found that the operation of the list (that was compiled after seeking representations from the person included and made available to employers in the childcare field only when a decision was taken to offer employment) was lawful and reasonable. The case predated the Human Rights Act 1998 and so no view was expressed as to whether the operation of the list complied with Article 8 of the ECHR. However, the operation of the Consultancy Service Index was further considered in *R v (1) Worcester County Council (2) Secretary of State for Health ex parte SW Case No CO/4550/99* (unreported) where Newman J sitting in the High Court expressed the opinion that the operation of the Index would be compatible with Article 8 of the ECHR even in the absence of a relevant statutory framework.

3.23 The extent of the state's ability to rely on non-statutory powers to tap telephones was raised in the case of *Malone v Commissioner of Police for the Metropolis (No 2)* [1979] 2 All ER 620 that was subsequently heard in the European Court of Human Rights (see *Malone v UK (1984) 7 EHRR*). This case concerned the lawfulness of telephone tapping in the UK at a time when the UK had no statutory regime for tapping telephones. In the Chancery Division it was held that the state could carry out telephone tapping because there was

nothing to make it unlawful. However, it isn't clear from the judgement under what legal power or powers the relevant authorities might be acting as it is stated that tapping would not require any statutory or common law power. The lawfulness of the telephone tapping was not, ultimately, upheld by the European Court of Human Rights as it was found that the lack of clear and accessible legal basis for the infringement contravened Article 8 of the ECHR. As telephone tapping represents a particularly serious form of interference with private life it is probably for that reason the law requires the powers to be particularly precise. For the purposes of other forms of interference, it may, therefore, still be possible to rely on common law or prerogative powers.

3.24 It is worth noting that even where common law or prerogative data sharing powers are compatible with Article 8 of the ECHR, they may still not provide a suitable basis for public sector data sharing for other reasons. Sometimes a statutory framework is necessary in order, for example, to impose criminal sanctions on officials for non-compliance. Such a statutory regime can be found, for example, in section 182 of the Finance Act 1989 and section 6 and Schedule 1 to the Taxes Management Act 1970 that make it an offence for a person to disclose any information which he holds, or has held, in connection with the exercise of his tax, tax credit or social security functions. Such a sanction could not be imposed by the common law or in reliance upon prerogative powers.

Local authorities

3.25 Local authorities, like non-ministerial government departments, are creatures of statute. Similar considerations will, therefore, apply as those outlined above in relation to statutory powers (express and implied) as local authorities will only be able to do what is expressly or by implication authorised by statute. Of particular relevance to local government are the following statutory powers:

- Section 111(1) of the Local Government Act 1972 that provides that a local authority 'shall have power to do anything ... which is calculated to facilitate, or is conducive or incidental to, the discharge of any of their statutory functions'.

- Section 2(1) of the Local Government Act 2000 that provides that a local authority shall 'have power to do anything which they consider is likely to achieve any one or more of the following objects – (a) the promotion or improvement of the economic well-being of their area; (b) the promotion or improvement of the social well-being of their area; (c) the promotion or improvement of the environmental well-being of their area'.

3.26 Of direct relevance to local authority data sharing is the case of *Peck v the United Kingdom* (ECHR judgement 28 January 2003) which concerned the disclosure of CCTV footage by Brentwood Council to the media. The footage showed Mr Peck walking in public late at night wielding a knife, prior to attempting suicide in the centre of Brentwood. The footage itself did not show the attempted suicide. On the question of whether the disclosure satisfied the 'in accordance with law' requirement of Article 8 of the ECHR, the European Court of Human Rights determined that section 163 of the Criminal Justice and Public Order Act 1994 gave the council express statutory power to use CCTV cameras to promote the prevention of crime and the welfare of victims in their area. Moreover, section 111(1) of the Local Government Act 1972 provided the council with power to distribute CCTV footage to the media in the discharge of their functions under section 163 of the 1994 Act. The disclosure did, therefore, have a basis in law and was, with appropriate legal advice, foreseeable. The Court went on to find that the disclosure was not justified as it represented a disproportionate interference with Mr Peck's Article 8 right to privacy given that the Council did not obtain Mr Peck's consent to the disclosure nor did it attempt to mask his identity.

3.27 Also of relevance to local authority data sharing are cases such as *R (A) v Hertfordshire County Council* [2001] All ER (D) 259 where the Court of Appeal accepted that there was an implied statutory power to share data under the Children Act 1989. No reliance was placed on section 111(1) of the Local Government Act 1972. Here the local authority had notified the director of education that there was reasonable cause for suspecting that a particular head teacher posed a risk of significant harm to children in his care. Relying on cases such as

R v Local Authority and Police Authority in the Midlands ex parte LM [2000] 1 FLR 612 and *R v Chief Constable of North Wales Police, ex parte AB* [1999] QB 396 it was held that disclosure should only be made where there is a 'pressing social need' for that disclosure.

3.28 Where a local authority has obtained data pursuant to a statutory function it is important to take account of any express or implied limitation on disclosure that might be operative. For example, many local authorities would like to access council tax data for other purposes such as reducing fraudulent benefit claims, debt recovery and verification of entitlement to various concessions. Some would like to share data internally which would reduce the need for local authorities to keep a number of name and address databases in relation to, for example, council tax, the electoral roll and housing benefit. A relevant consideration is whether paragraph 17 of Schedule 2 to the Local Government Finance Act 1992 prohibits the use of council tax data for secondary purposes. Paragraph 17 provides that:

- (1) *Regulations under this Schedule may include provision that an authority –*
- may supply relevant information to any person who requests it for a purpose not relating to Part 1 or II of the Act; and*
 - may charge a prescribed fee for supplying the information.*
- (2) *For the purposes of sub-paragraph (1) above information is relevant information if –*
- it was obtained by the authority for the purpose of carrying out its functions under Part 1 or Part II of this Act; and*
 - it is not personal information.'*

3.29 This provision is taken to mean that, as it is prohibited to make regulations allowing for the supply of personal information, **all** disclosures of personal information for non-council tax purposes are prohibited. The Information Commissioner has obtained advice to this effect. Similarly, if other databases are to be shared (whether externally or internally) relevant legislative provisions will need to be considered to determine whether or not they permit the data sharing in question. For example,

in relation to information from the electoral roll, the provisions of the Representation of the People (England and Wales) (Amendment) Regulations would need to be considered to determine if they expressly or implicitly restrict the disclosure of information from the electoral roll.

- 3.30 If there are no relevant statutory restrictions it may then be possible for local authorities to share data either internally or externally in reliance on section 111(1) of the Local Government Act 1972 or section 2 of the Local Government Act 2000. The power that is contained in section 2 of the Local Government Act 2000 is of particular relevance as it is designed to ensure that service delivery is co-ordinated in ways which minimise duplication and maximise effectiveness². Section 2 would permit many types of data sharing partnership between local authorities and others where the proposed data sharing will achieve one of the objects set out in section 2(1) and where there is no statutory prohibition (express or, in very rare cases, implied) restricting the data sharing proposed. Section 2(5) makes it clear that a local authority may do anything for the benefit of a person outside their area if it achieves one of the objects of section 2(1). It should be noted that the Information Commissioner has not expressed a view as to whether section 2 can be relied upon to permit the sharing of council tax data for secondary purposes.

- 3.31 Local authority data sharing is an area where there may be specific legislative reform in future. For example, Section 85 of the Local Government Act 2003 adds new provisions in the Local Government Finance Act 1992 which expressly allow local authorities to use council tax data to identify empty properties.

Other public authorities

- 3.32 Besides central government departments and local authorities there are, of course, numerous other public bodies that derive their powers from statute or from common law. For example, the Welsh National Assembly that derives its powers from statute and non-departmental government bodies like the Legal Services Commission. In relation to these bodies careful consideration should be given to the particular statutory regime that might govern the activities of the particular body in determining whether or not there might be express or implied power to collect, use and share data.

A flow chart setting out the relevant considerations in determining the question of *vires* is at Appendix 1.

² Guidance has been issued by the Department for Environment, Transport and the Regions (now the Office of the Deputy Prime Minister/Department for Transport) entitled 'Power to Promote or Improve Economic Social or Environmental well-being' (March 2001).

4 The Human Rights Act 1998 and the European Convention on Human Rights

4.1 The Human Rights Act 1998 (the HRA) came into force on 2 October 2000 and it gives effect to the principal rights guaranteed by the European Convention on Human Rights (the Convention). The Convention was adopted by the Council of Europe in 1950 and ratified by the United Kingdom in 1951. It contains a number of fundamental rights and freedoms including the right to life, the right to a fair trial, freedom of thought, religion and speech and the right to respect for private and family life. Before the HRA, rights contained in the Convention could only be enforced in the European Commission and the Court of Human Rights established in Strasbourg. Since the HRA the Convention rights have become part of domestic law and can be enforced directly in our courts by any person who claims to be a 'victim' of an infringement. There remains a right to bring cases in the Strasbourg court after pursuing domestic remedies.

4.2 The key aspects of the HRA are that:

- all legislation must be interpreted so far as is possible to do so to be compatible with the Convention (section 3(1));
- it is unlawful for a public body to act in a way that is incompatible with convention rights (section 6);
- all courts and tribunals are required to take account of relevant decisions of the European Court of Human Rights, and to have regard to the opinions and decisions of the Commission (section 2); and
- higher courts may make a declaration of incompatibility in respect of incompatible primary legislation, and in certain circumstances, of secondary legislation. Such declarations do not, however, change the law. That is for Parliament to do, if it so wishes. See section 4 of the HRA.

Article 8 of the Convention is of particular importance in the context of data sharing and privacy. Article 8 provides that:

8.1 Everyone has the right to respect for his private and family life, his home and his correspondence.

8.2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

4.3 Article 8 is broad in scope and covers the collection, use and exchange of personal data as well as issues such as telephone tapping, parental access and custody of children, the right to be free from noise and environmental pollution and a person's right to express his or her identity and sexuality. In the case of *R (Robertson) v City of Wakefield Metropolitan Council* [2002] 2 WLR 889 Kay J sitting in the Administrative Court held that Article 8 was engaged by the provision of a person's current name and address under statutory electoral roll obligations; Article 8 was not exclusively concerned with more obviously sensitive details than simply a name and address. In determining whether Article 8

was engaged it was necessary to take into account not simply the information that was disclosed but also the anticipated use to which it would be put. Where names and addresses were to be passed on to commercial concerns for direct marketing purposes this would amount to an interference with the right to private life.

4.4 Article 8 is not an absolute right. It is a qualified right that allows a public authority to interfere where that interference is:

- in accordance with law;
- in the pursuit of a legitimate aim; and
- necessary in a democratic society.

4.5 The first element requires a legal basis to permit data sharing that is a clear, reasonably accessible legal basis for the interference. Legislation, delegated legislation, the common law and even rules of a professional body may suffice. The second element means that the data sharing must be for one of the purposes specified in Article 8(2). It is usually fairly easy to satisfy this requirement. Satisfaction of the third element, 'necessary in a democratic society', will probably be the key factor in the majority of cases. In determining this element courts are required to look at all the circumstances of the case and assess whether the exercise of the power was 'proportionate'. This assessment is not straightforward and will involve the court in considering whether the means chosen were necessary, whether adequate safeguards are in place and whether the aims were legitimate and sufficiently well defined. In the recent House of Lords case of *R v Secretary of State for the Home Department, ex parte Daly* [2001] UKHL 26 Lord Steyn set out a new test to be adopted by the courts in assessing the proportionality principle. In his judgement he emphasised the high level of intensity of review under the proportionality approach in that:

- The reviewing court may need to assess the balance which the decision maker has struck;
- The court may need to direct attention to the relative weight accorded to interests and considerations;

- The proportionality test may require the court to go further than the test of 'heightened scrutiny' previously adopted on judicial review. In particular, the test of heightened scrutiny was developed in *R v Ministry of Defence, ex parte Smith* [1996] 1 All ER 257 which was heard by the Court of Appeal before the HRA came into force. Here it was held that the more substantial the interference with human rights, the more the court would require by way of justification before it was satisfied that the decision was reasonable. However, the court would still only interfere with an administrative decision where it was satisfied that the decision was beyond the range of reasonable responses open to a reasonable decision-maker.

4.6 The European Court of Human Rights has considered a number of cases involving the disclosure of personal data between public authorities. In the case of *M.S. v Sweden*, (Application number 00020837/92 dated 27 August 1997) the applicant contested the disclosure of her medical history to the Swedish Social Insurance Office following a claim for industrial injury compensation. The disclosure was made pursuant to relevant provisions in Swedish law, namely, the Secrecy Act and the Insurance Act. The court found that the disclosure was not in breach of Article 8 of the ECHR because: (a) there was a legal basis for the interference; (b) the object of the disclosure was to determine the allocation of public funds and so was in the pursuit of a legitimate aim, namely, the economic well-being of the country; and (c) the disclosure was necessary as the medical records were relevant to the applicant's compensation claim. In addition, disclosure was subject to effective and adequate safeguards as the relevant legislation provided that duties of confidentiality applied which were subject to criminal and civil penalties if breached. Accordingly, the measure was not disproportionate to the aim pursued.

4.7 Other important relevant cases have considered the compulsory provision of information to public bodies. In *X v UK* 30 DR 239 1982 the court found that a statutory requirement for the compulsory provision of information, backed up by criminal sanctions to be used in the event that an individual refused to comply, in connection with a national census was a justifiable interference with Article 8 privacy rights.

The interference could be considered necessary in a democratic society given that an individual's privacy was sufficiently protected and the aim of the census was the legitimate one of the pursuit of the economic well-being of the country. Similarly, in the case of *X v Belgium* 31 DR 231 1982 the court found that the obligatory provision of details of private expenditure to the tax authorities in connection with an income tax return could be justified in the circumstances as the authorities had a legitimate need for evidence considering the disposal of substantial assets.

- 4.8 The cases of *X v the UK* and *X v Belgium* also illustrate that when a failure to provide information constitutes a criminal offence the interference with Article 8 privacy rights may still satisfy the 'in accordance with the law' requirement where the obligation is enshrined in statute. But even where an obligation to provide information is enshrined in statute, it is still necessary to show that the interference is necessary in a democratic society, and that the aim of the collection of information is the legitimate one of serving the economic well-being of the country.
- 4.9 Despite its wide scope, the HRA does not remove the requirements of other areas of law (although there may be some overlap). For example, the requirements of the Data Protection Act 1998 still need to be satisfied.
- 4.10 The Court of Appeal recently stated in its judgement in *Douglas and others v Hello! and others* [2003] EWHC 786 Ch, at para 229, that no general, free-standing right to privacy existed under UK law. Amongst other things, the breadth of the subject of privacy makes it such that it is better left to Parliament to make any such law in this area.

5 Common Law, Statutory Obligations of Confidence and Statutory Restrictions on the Disclosure of Data

5.1 The law of tort is an area of civil law that provides individuals with a cause of action for damages if there is a breach of legal duty. As regards the collection, use and disclosure of personal information, the tort of breach of confidence is of particular relevance. Breach of confidence is a tort, which protects information provided that it can be shown that:

- The information in question has the necessary 'quality of confidence'. This means that the information should not be in the public domain or readily available from another source and that it should have a degree of sensitivity and value;
- The information in question was communicated in circumstances giving rise to an obligation of confidence. The obligation of confidence may be express or implied from the circumstances such as where there is a special relationship between professionals, for example, relationships between doctors and bankers and their clients;
- There was an unauthorised use of that material. From the authorities it seems that it is not always necessary to prove damage or detriment nor is it necessary to prove dishonesty. These elements were identified in *Coco v A.N.Clark Engineers Ltd [1969] R.P.C. 41*.

5.2 Confidentiality is not, however, an absolute right. It has long been established that just cause or excuse and acting in the public interest are defences to an action for breach of confidence. For example, the defence extends to crimes, frauds and other forms of wrongdoing where disclosure is in the public interest. Now that the HRA is in force, it is also necessary for the courts to take into account

Strasbourg case law relating to the justification of interferences with the Article 8 right to privacy. So, for example, where Article 8 rights are engaged the interference must be necessary and proportionate to the end pursued in order for it to be in the public interest. The European Court of Human Rights applied these principles in the case of *Campbell v UK (1993) 15 EHRR 137* when it held that the blanket opening of prisoners' mail to determine whether it contained prohibited material was not justified since the lesser measure of opening mail where there was a reasonable ground to suspect that it contained such material would have sufficed. In any event, an application of Convention principles may yield the same result as that obtained from the application of common law principles. Where one is seeking to disclose information of a confidential nature, rights under Article 10 of the ECHR (to freedom of expression) may also come into play.

5.3 Recent judicial pronouncements in relation to confidence (in *Campbell v M.G.N [2002] EWCA Civ No 1371* and *A v B [2002] EWCA Civ 337*) have confirmed that, while public figures are entitled to have privacy respected, they must expect closer scrutiny of their actions by the media and that the media are entitled to 'set the record straight' where they have misled the public as to aspects of their behaviour.

5.4 As regards data sharing, government departments and local authorities that have access to confidential information relating to citizens may owe duties of confidence. In relation to information held by public authorities the same principles apply as would apply to information held by private persons and organisations. It follows that public authorities cannot do what they like with personal information without adhering

to principles arising from the common law tort of confidentiality. For the purposes of the law of confidence it is clear that different government departments are treated as separate legal persons which means that information cannot be freely disclosed between government departments without taking into account the common law of breach of confidence.

- 5.5 It is likely that names and addresses of individuals that are supplied to public bodies in pursuance of their functions would in some cases amount to confidential information subject to the common law tort of breach of confidence.
- 5.6 Related to civil obligations of confidence, are miscellaneous statutory obligations that may prohibit the disclosure of certain types of information by imposing specific obligations of confidence. Legislation of this nature is disparate, covering topics such as:
- Medical confidentiality (for example the Abortion Act 1967 and the Access to Medical Reports Act 1988);
 - Information supplied in connection with legal proceedings (various rules of court);
 - Health and safety (section 27 and 28 of the Health and Safety at Work Etc Act 1974);
 - Information supplied to the Inland Revenue (section 182 of the Finance Act 1989 and section 6 and Schedule 1 to the Taxes Management Act 1970);
 - Information supplied to the Child Support Agency (section 50 of the Child Support Act 1991);
 - Information obtained under powers in the Companies Act 1985 (section 449);
 - Information relating to an individual which comes into the possession of a public authority pursuant, inter-alia, to the exercise of its functions under the Enterprise Act 2002 (sections 237 and 238).
- 5.7 It is important to ensure that any proposed disclosure of personal data by a public body does not result in it

inadvertently committing a criminal offence. As noted above, there are a number of statutory restrictions on the use and disclosure of information which preclude a public body from sharing information and provide that any disclosure of certain information will constitute a criminal offence unless that disclosure falls within one of the statutory gateways of the relevant legislation.

- 5.8 Some statutory prohibitions may, however, contain discretion to disclose. In any event, it is possible that statutory obligations of this type may be overridden in a similar way to common law obligations of confidence as outlined above.
- 5.9 As there may be uncertainty as to when it will be in the overriding public interest to disclose confidential information, legislation is sometimes enacted in this area. Some of this legislation imposes an *obligation* to disclose information, such as the provisions of the Child Support (Information, Evidence and Disclosure) Regulations 1992 (SI 1992/1812). These regulations provide that certain categories of people (including local authorities and Crown servants) shall furnish such information or evidence as is required by the Secretary of State to enable him to make certain decisions under the Child Support Act 1991 (reg 2).
- 5.10 Other legislation provides for a power to make disclosures in certain circumstances. Examples of this latter type of provision are to be found in s115 of the Crime and Disorder Act 1998, which gives the power to disclose information where the disclosure is necessary or expedient for the purposes of that Act. It does not *require* disclosure to be made in such circumstances. The fact that the disclosure is so necessary or expedient would need to be weighed against any competing obligations (such as confidence) that may pertain to the information in question, so a balancing exercise would need to be carried out.
- 5.11 Section 17 of the Anti-Terrorism, Crime and Security Act 2001 allows (but does not require) disclosures to be made under statutory provisions (specified in Schedule 4 to the Act) for fairly broad purposes connected with criminal investigation and prosecution. No disclosure shall be made under s17 unless the public authority making the disclosure is satisfied

that it is proportionate to the aim that is to be achieved (s17(5)). This imports the balancing exercise required by Article 8 of the European Convention on Human Rights (see Section 4), whereby an interference with the right to private life must be proportionate to the achievement of a legitimate aim. Where proportionality can be shown, this would provide sufficient grounds for overriding any duty of confidentiality owed in respect of the information.

6 Key Elements of the Data Protection Act 1998 relevant to Data Sharing

Application of the Data Protection Act (DPA)

- 6.1 The DPA applies to 'data controllers' and regulates whether and how they process personal data. Those individuals who are the subject of personal data ('data subjects') are also given rights under the Act such as the right of access and the right to prevent processing likely to cause damage or distress, however detailed consideration of those rights is outside the scope of this guidance. The Act implements the Data Protection Directive (Directive 95/46/EC), and regard must be had to the Directive when interpreting the Act.
- 6.2 'Data controller', 'data subject', 'processing', 'personal data' and other relevant terms are defined in section 1 and section 2 of the Act. Government departments and other public bodies are data controllers for these purposes. 'Processing' means essentially anything which may be done to personal data, including obtaining, holding, using, disclosing or destroying them. 'Data' is defined in section 1(1) of the Act and includes all automatically processed (i.e. computerised) information and some manual records³, and 'personal data' means 'data' relating to an identified or identifiable living individual. Many types of public sector data sharing will involve information held on computer so that, if the information relates to identified or identifiable individuals, it will be clear that the DPA applies. Certain categories of personal data⁴ are defined in section 2 as 'sensitive', and the DPA imposes additional requirements in relation to such data.

The Data Protection Principles

- 6.3 The eight data protection principles set out in Schedule 1 to the DPA are of central importance. These principles are included in Appendix 4 to this Guidance.
- 6.4 The First and Second Data Protection Principles are particularly important in determining if data sharing will be lawful. Both of these principles are considered in further detail. The legal remedies that arise when there is a breach of any of the Data Protection Principles are considered at paragraph 6.36.

The First Principle

- 6.5 Under the first Data Protection Principle, personal data are required to be processed 'fairly' and 'lawfully'. The requirement that the personal data be processed 'lawfully' means that those legal obligations both statutory and common law must be complied with. The DPA cannot render lawful any processing which would otherwise be unlawful. In the context of public sector data sharing this means that the public body must have the *vires* to carry out the processing (or the function to which the processing of the data is ancillary), that the processing is not in breach of the law of confidence, that the processing is not in breach of any other relevant domestic statute or common law principle, and that it is compliant with the HRA, the ECHR (Article 8 in particular) and any applicable principles of EU law. Accordingly, the DPA overlaps with other areas of law.

³ Guidance to government departments on the extent to which manual records are covered by the DPA can be found in the Lord Chancellor's Guidance on Handling Subject Access requests.

⁴ For example, personal data consisting of information as to racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, the commission or alleged commission of any offence, or criminal proceedings.

- 6.6 Part II of Schedule 1 to the DPA contains interpretative provisions relating to the data protection principles, of which paragraphs 1 to 4 relate to the requirement of 'fairness' in the first principle. Paragraph 1 (1) states that in determining whether personal data are processed fairly, regard is to be had to the method by which the data were obtained, and in particular whether the person from whom the data are obtained is 'deceived or misled' as to the purposes for which they are to be processed. It is further stated in paragraph 1 (2) that, subject to paragraph 2 (see below), data are to be treated as obtained fairly if they consist of information obtained from a person who is authorised by, or under, enactment to supply it or is required to supply it by, or under, any enactment or by any convention, or other instrument, imposing an international obligation on the United Kingdom.
- 6.7 Paragraph 2 indicates that personal data are not to be regarded as being processed fairly unless, at the first time that processing takes place, or very soon afterwards, the relevant data subject is provided with, or has made readily available to him, certain information ('the information requirements'). This information includes the identity of the data controller or any nominated representative, the purposes for which the data are intended to be processed and any further information that is necessary in order for the processing to be regarded as fair having regard to the circumstances. These requirements apply whether the data controller obtains the data from the data subject or from elsewhere. However, by paragraph 3, in the case of data obtained other than from the data subject there is an exemption where the provision of the information would involve a disproportionate effort, or where the recording or disclosure of the data is necessary for compliance with a legal obligation, provided that the further conditions prescribed in the Data Protection (Conditions under Paragraph 3 of Part II of Schedule 1 Order (S.I. 2000 No 185) are met. In particular, the information must be provided to any individual who requests it, and a data controller who relies on the disproportionate effort ground must keep a record of the reasons or his view that disproportionate effort would be involved.
- 6.8 In practical terms, the principle of fairness will require that even where data are obtained pursuant to statutory powers, data subjects should be given the information set out in paragraph 2 which includes details of the identity of the data controller and details of the purpose or purposes for which their data is to be processed. Careful consideration should, therefore, be given to the ways in which individuals are provided with this information.
- 6.9 If the general requirements that the processing be 'fair' and 'lawful' are met, it is a particular requirement that (a) at least one of the conditions of 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.
- 6.10 The conditions for processing personal data set out in Schedules 2 and 3 are set out in Appendix 5. Those conditions that are particularly relevant to public sector data sharing are considered in more detail at paragraph 6.13.
- 6.11 In many of the conditions referred to it is required that the processing is 'necessary' for a particular function or purpose. In our view the word 'necessary' in this context encompasses matters which are 'reasonably required or legally ancillary to' the accomplishment of the specified purposes, it is not limited to those matters which are 'absolutely essential' to the accomplishment of those purposes. This construction was supported in *A.G v Walker 3 Ex 242, per Pollock CB*, cited in Stroud's Judicial Dictionary, p.1660. In determining whether processing is 'necessary' in any particular case the sensitivity of the data may be relevant.
- 6.12 The Administrative Court in *R v Chief Constable of Essex, ex parte Ellis [2003] EWHC 1321 (Admin)*, 12th June 2003 considered the meaning of 'necessary' in the context of sections 29 and Schedules 2 and 3 to the Act. The case concerned an 'Offender Naming Scheme' under which photographs together with the names of persons convicted of certain offences would be displayed in the area in which the crimes were committed. The inclusion of a candidate in the Scheme would have to be shown to be necessary for the discharge of a duty cast upon the police to formulate and implement policies

designed to reduce crime and disorder. The reference to 'necessary' in this context requires that the police's action should be a proportionate response to a pressing social need (i.e. an assessment of the type required by Article 8 of the European Convention on Human Rights). The Court did not have enough information before it to decide whether the possible benefits of the Scheme were proportionate to the interference with an offender's rights under Article 8 of the ECHR, and refused to grant a declaration that the Scheme was not capable of being operated lawfully during a trial period. The Court mentioned the rights of the offender's family and the detrimental effects that publication of his photograph might have. In the context of data sharing, one can draw support from this decision for the proposition that the sharing need not be absolutely essential to the activity in question. Whether it is 'necessary' will depend on the circumstances of the case, and the Courts will look at effects that the disclosure may have on third parties.

Schedule 2 conditions of particular relevance to public sector data sharing

Paragraph 3

6.13 This states that the processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract. If there is a relevant statutory gateway that imports a legal obligation to disclose data, then the condition in paragraph 3 of Schedule 2 will be relevant. For example, this condition would be relevant to data processing by public bodies that are under a legal obligation to provide relevant information to the National Audit Office under section 8 of the National Audit Act 1983.

Paragraph 5 (a)

6.14 This states that the processing is necessary for the administration of justice and it is likely to be of application to courts and tribunals and other bodies that have judicial functions.

Paragraph 5 (b)

6.15 This states that the processing is necessary for the exercise of any function conferred on any person by or under any enactment. This will cover data processing that is carried out pursuant to express

statutory powers or that is reasonably required or ancillary to the exercise of express or implied statutory functions.

Paragraph 5 (c)

6.16 This states that the processing is necessary for the exercise of any functions of the Crown, a Minister of the Crown or a government department. The condition will cover data processing relating to functions carried out by central government departments that derive from the Crown's common law, prerogative or statutory powers.

6.17 In relation to paragraphs 5 (b) and (c), it is important to bear in mind that when data is shared, there are two instances of processing: one by the person making the disclosure, the other by the recipient of the disclosure. Each of these must be justified by reference to a Schedule condition.

Paragraph 5 (d)

6.18 This states that the processing is necessary for the exercise of any other functions of a public nature exercised in the public interest by any person. The condition will cover data processing connected with public sector data sharing which is not carried out pursuant to express or implied statutory functions or as part of the functions of the Crown, a Minister of the Crown or a government department, provided that the data sharing relates to 'functions of a public nature exercised in the public interest'. It would, for example, cover processing by voluntary organisations or private bodies provided that it is in support of a public function that is in the public interest.

Paragraph 6

6.19 This provides that 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. The concept of 'legitimate interests' is not defined in the DPA and is potentially of very wide application. It involves a case by case consideration of the balance between the legitimate interests of the data controller and the data subject.

Schedule 3 conditions of relevance to public sector data sharing

6.20 The conditions set out at paragraph 7(1)(a), (b) and (c) of Schedule 3 are worded in a similar way to those set out at paragraph 5(a), (b) and (c) of Schedule 2 which are considered above. In the context of Schedule 3, however, these conditions must also be read in conjunction with Article 8.4 of Directive 95/46/EC, which is the basis for these conditions⁵.

Consent: Paragraph 1 of Schedule 2; Explicit consent: Paragraph 1 of Schedule 3

6.21 Consent may also form the basis for legitimate data sharing. However, in the context of public sector data sharing that is *intra vires* it is likely that the processing involved will meet at least one of the conditions in Schedule 2 or Schedule 3 mentioned above and, where this is the case, consent is not a necessary precondition. As a general rule the Information Commissioner has indicated that consent should be 'informed' and 'unambiguous'. Consent is notoriously hard to define, although most people (we imagine) would feel able to recognise it when they saw it. An evaluation of the adequacy of consent in the circumstances where it is not obvious that it has been given or that it is fully 'informed', make it difficult to generalise.

The Second Principle

6.22 This provides that 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.

6.23 The interpretation provisions in Part II of Schedule 1 to the DPA indicate, at paragraph 5, that the purpose or purposes for which personal data are obtained may, in particular, be specified either in a notice given to the data subject pursuant to the information requirements referred to above, or in a notification given to the Commissioner under Part III of the Act (see paragraph 6.35).

6.24 As to further processing operations, in our view, the requirement of compatibility has a relatively low threshold. Compatible does not mean 'identical to', and purposes which are quite different from the original purposes can still be compatible with those original purposes. We believe that, provided the further processing is for a purpose that is not *contradictory* to the originally specified purpose or purposes, it will be consistent with the second principle. For example, data sharing that is carried out pursuant to section 115 of the Crime and Disorder Act 1998 would not contravene the requirement that data should not be processed for purposes that are incompatible with the purpose for which it was originally obtained.

Exemptions

6.25 There are a number of important exemptions contained in the DPA that may be relevant in the context of public sector data sharing. Practitioners may, however, wish to consider whether it is nonetheless possible to achieve the same outcome by acting in accordance with the data protection principles even if an exemption is available.

6.26 Each exemption is quite specific as to the particular provisions of the DPA to which it relates, therefore it is important to be clear as to the terms of any exemption before seeking to rely on it.

6.27 Certain exemptions apply to 'the non-disclosure provisions' which are defined in section 27(3) and (4) as including:

- a. the first data protection principle, except to the extent to which it requires compliance with the conditions in Schedules 2 and 3; and
- b. the second, third, fourth and fifth data protection principles, 'to the extent to which they are inconsistent with the disclosure in question'. This is an important caveat, as if in any particular case compliance with (for

⁵ Article 8.4 of the Directive permits member states to lay down exemptions to the prohibition on processing sensitive personal data for reasons of substantial public interest and subject to suitable safeguards.

example) the fairness requirement in the first data protection principle is not inconsistent with the disclosure in question, there will be no exemption from that requirement.

- 6.28 Other exemptions apply to 'the subject information provisions' which are defined in section 27(2) as including the information requirements referred to at paragraph 6.7.

National Security

- 6.29 Pursuant to section 28 of the DPA personal data are exempt from certain provisions of the Act if exemption from the provision in question is required for the purpose of safeguarding national security. This exemption covers all of the Data Protection Principles. It follows that a public body can share personal data without having to comply with key provisions in the DPA if exemption from those provisions is required for the purpose of safeguarding national security. By section 28(2), a certificate signed by a Minister of the Crown certifying that exemption from the provisions specified is required for the purpose of safeguarding national security is conclusive evidence of that fact, subject to a right of appeal to the Information Tribunal under section 28(4).

Crime and taxation

- 6.30 Section 29 of the DPA exempts from certain provisions of the Act personal data processed for (i) the prevention or detection of crime; (ii) the apprehension or prosecution of offenders; or (iii) the assessment or collection of any tax or duty or of any imposition of a similar nature; but only where the application of those provisions would be 'likely to prejudice' any of these purposes. This exemption applies to, among other matters, the First Data Protection Principle (except to the extent to which it requires compliance with Schedules 2 and 3) and the non-disclosure provisions. Accordingly, this exemption would cover disclosures of personal information for the specified purposes provided that a Schedule 2 or Schedule 3 condition is also met. Public bodies may benefit from this exemption particularly those for whom the investigation of crime, the collection of tax or the prosecution of offenders is their primary purpose. It should be noted that the 'likely to prejudice' test is not a light one and must be satisfied in the circumstances

of a particular case; thus the exemption must be applied on a 'case by case' basis and could not be used to justify routine data matching or sharing.

Research

- 6.31 Section 33(2) of the DPA provides that for the purposes of the second data protection principle, the further processing of personal data only for research purposes (which includes statistical or historical purposes) is not to be regarded as incompatible with the purposes for which they were obtained. The processing must comply with two conditions, namely the data must not be processed to support measures or decisions with respect to particular individuals, and 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.

Information available to the public by or under an enactment

- 6.32 By section 34 of the DPA, personal data which the data controller is obliged by or under any enactment to make available to the public are exempt from the non-disclosure provisions and the subject information provisions. Public registers established by statute would be covered by this exemption.

Disclosures required by law

- 6.33 Similarly, by section 35 of the DPA, personal data are exempt from the non-disclosure provisions where the disclosure is required by or under any enactment, by rule of law or by order of the court, where the disclosure is necessary in connection with legal proceedings or for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights. Section 35 of the DPA would apply in relation to mandatory statutory gateways such as section 17 of the Criminal Appeal Act 1995 that makes it obligatory for a public body to provide information, when requested, to the Criminal Cases Review Commission in connection with the exercise of its functions.

Schedule 7

- 6.33 Further specific exemptions to the subject information provisions may be found in Schedule 7 to the DPA. They include information processed for

the purpose of assessing suitability for judicial office, and to confidential employment references provided by the data controller.

Notification

6.35 Subject to certain limited exceptions which are unlikely to be relevant in the context of public sector data sharing, section 17 of the DPA prohibits data controllers from processing personal data unless they are registered with the Information Commissioner. In notifying the Commissioner, the data controller must provide certain particulars which are specified in sections 16 and 18 and which include a description of the personal data being processed, a description of the purposes for which the data are being processed, a description of any recipients to whom the data may be disclosed and details of security measures in place.

Enforcement of the DPA and consequences of non-compliance

6.36 The Information Commissioner has a duty to promote good practice and is responsible for enforcing the DPA. He has the following powers to investigate alleged breaches of the requirements of the Act:

Information Notices (section 43)

6.37 If the Information Commissioner receives a request for a section 42 assessment or reasonably requires any information for the purposes of determining whether a data controller has complied or is complying with the data protection principles, he may serve an Information Notice requiring the data controller to supply specified information relating to processing activities.

Enforcement Notices (section 40)

6.38 The Information Commissioner may serve an Enforcement Notice where he is satisfied that any of the Data Protection Principles is being contravened. An Enforcement Notice may require the data controller to stop processing personal data or stop processing personal data in a particular manner. An Enforcement Notice may also require the data controller to take certain steps to remedy the unlawful processing and set out a time limit within which this must be done.

Section 42 Assessments

6.39 Any person who is, or believes himself to be, directly affected by any processing of personal data may request the Information Commissioner to carry out an assessment of whether it is likely or unlikely that any particular processing activity carried out by a data controller is carried out in compliance with the DPA. The Information Commissioner has power to make the assessment in the manner that he thinks appropriate and must notify the data subject of any assessment made and any view formed or action taken as a result.

6.40 In relation to the service and extent of notices, the data controller has a right of appeal to the Information Tribunal.

Civil remedies

6.41 A further remedy that is available for data subjects is a right to bring a civil action pursuant to section 13 of the DPA. Compensation may be awarded if the data subject has suffered damage, or distress and damage, as a result of any contravention by a data controller of any of the requirements of the Act.

Criminal sanctions

6.42 A number of criminal offences are created by the DPA such as processing without notifying (section 21) or failing to comply with an Information or Enforcement Notice (section 47). Criminal proceedings under the Act may only be instituted by the Information Commissioner or by or with the consent of the Director of Public Prosecutions (section 60). By section 63(5), a government department is not liable to prosecution under the Act.

7 Any Other Issues

- 7.1 Membership of the European Community has meant that the laws of Great Britain are now subject to European Community law. In broad terms this means that provisions of statutes and rules of common law which are incompatible with Community law are unenforceable. There are also certain provisions emanating from Europe which have direct effect, for example, regulations. As the Data Protection Act 1998 implements EC Directive 95/46, EC law is relevant when construing provisions within the DPA. The general principle is that the courts must construe legislation so as to accord with the relevant EC Directive. The approach to construction in such circumstances is 'purposive' in the sense that the courts must construe the legislation so far as is possible to give effect to the objects and purposes of the Directive.

8 Conclusions

Summary of legal considerations

8.1 The legal framework within which public sector data sharing takes place has been set out in the preceding sections of this guidance. The framework is, in some respects, complex and overlapping. As can be seen, there is no single source of law that regulates public sector data sharing. The DPA and the HRA are, clearly, of importance (and the application of the common law of confidence must be considered) but the first issue that needs to be determined is whether or not a public body has the *vires* to share data in the way proposed. It may also be necessary to consider whether a particular public body has the *vires* to collect the relevant data. If there is no power to carry out the proposed data sharing and/or collection then it may be that the only way the proposed activity can be done, if it can be done at all, is by enacting legislation. A flow chart illustrating the relevant considerations for lawful data collection and sharing is at Appendix 2. A checklist further summarising the relevant legal issues that arise in relation to a data sharing partnership is set out at Appendix 3.

Use of Codes of Practice

8.2 The use of codes of practice is one way of helping to ensure good practice in carrying out data sharing activities. Such codes do not have statutory force but will contain details of relevant legal rights and other standards that are to be adhered to. Under the Data Protection Act 1984 one of the tasks of the Data Protection Registrar was to promote the adoption of such codes. The position under the

1998 Act is that the Information Commissioner has the power to prepare codes of practice when he considers it to be appropriate, and for this purpose the Commissioner must engage in consultation with trade associations, data subjects or persons representing data subjects as appear to him to be appropriate. There is also provision in the DPA for the Secretary of State by order to direct the Information Commissioner to produce a code of practice.

8.3 One example of a code of practice is the Department for Work and Pensions Code of Practice on Obtaining Information under the Social Security Fraud Act 2001 that was issued in January 2002. This code of practice is guidance for staff and for local authority officers as to how to exercise their statutory powers in obtaining information from specified organisations in combating fraud against the benefit system. Included in the Code of Practice are provisions about confidentiality and security and procedures for dealing with complaints.

Useful contacts and websites

8.4 The Department of Constitutional Affairs at www.dca.gov.uk. A copy of the Lord Chancellor's Guidance on Handling Subject Access requests can be viewed on this site.

The Home Office has an information sharing website that focuses on crime reduction at www.crimereduction.gov.uk/informationsharing/index.htm

The Office of the Deputy Prime Minister at www.odpm.gov.uk. A copy of the guidance on section 2 of the Local Government Act 2000, 'Power to Promote or Improve Economic, Social or Environmental Well-being', can be viewed on this site.

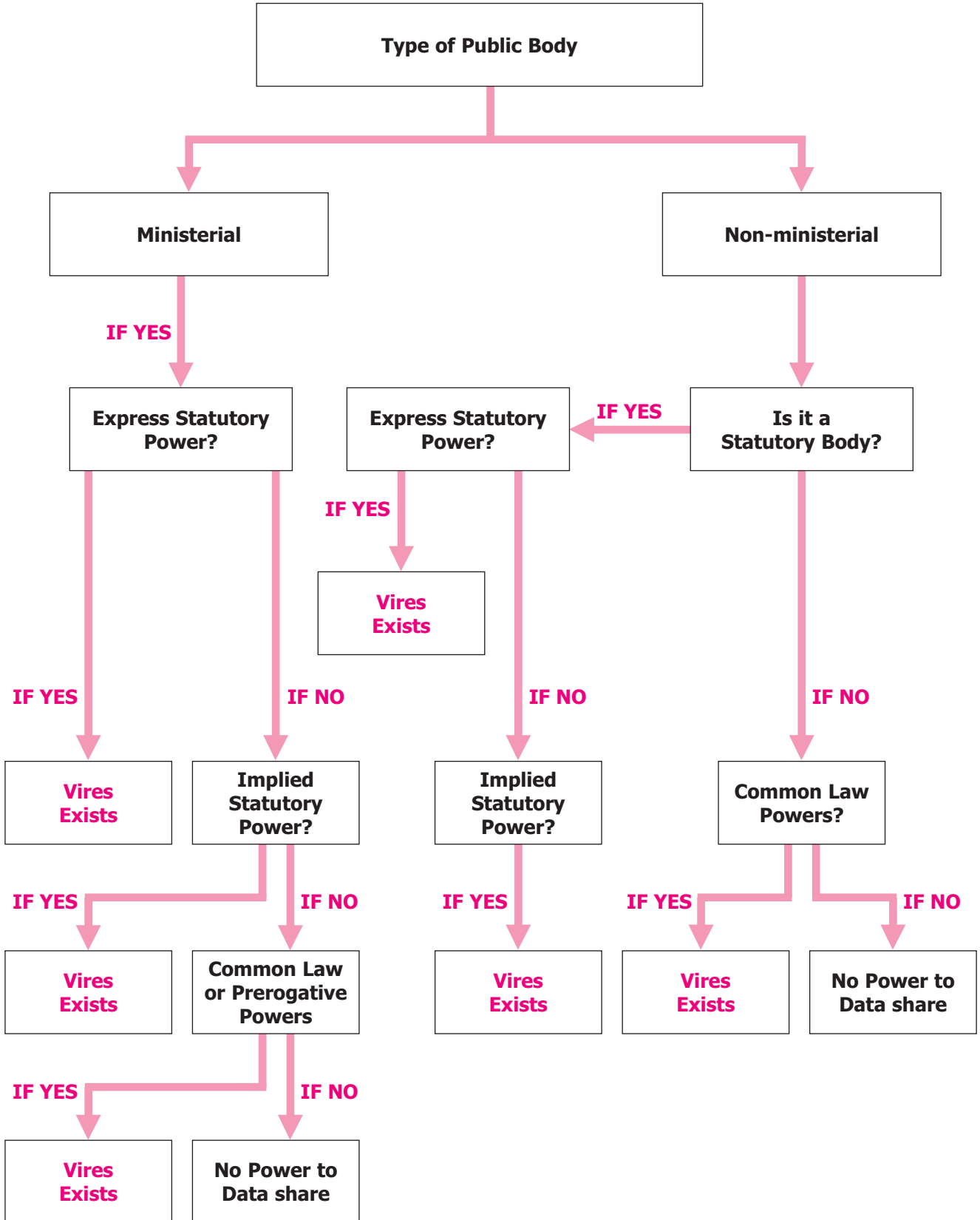
The Office of the Information Commissioner at www.informationcommissioner.gov.uk. The Information Commissioner's legal guidance on the Data Protection Act 1998 can be found on this site.

HMSO has the text of legislation including the Human Rights Act 1998 at www.legislation.hmso.gov.uk/acts.htm

European Court of Human Rights case law database at www.echr.coe.int/Hudoc.htm

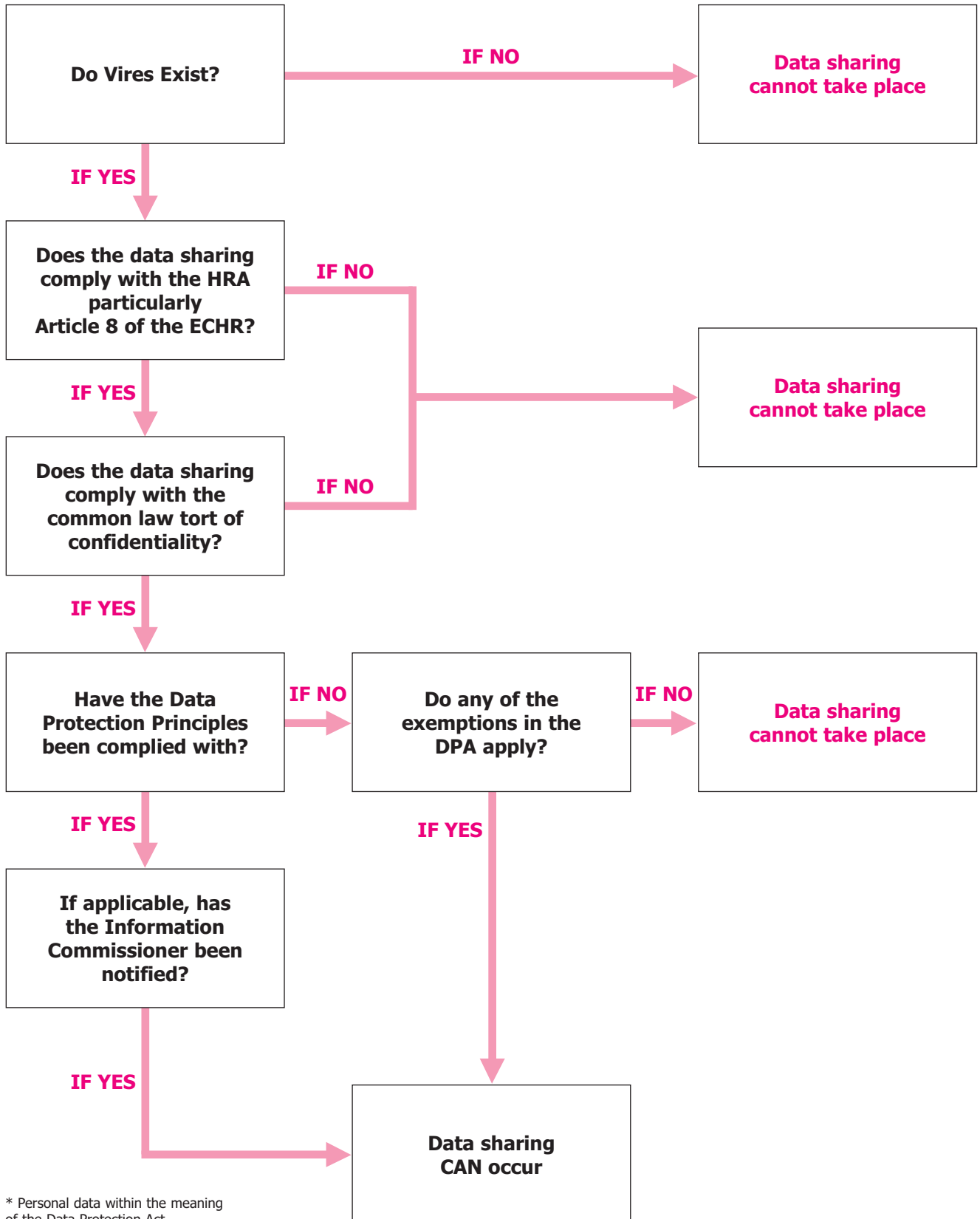
APPENDIX 1

Is Data Sharing Intra Vires?



APPENDIX 2

Relevant Considerations for Lawful Sharing of Personal Data*



* Personal data within the meaning of the Data Protection Act

APPENDIX 3

Checklist of Relevant Legal Considerations Relating to Data Sharing Partnerships

A new data sharing initiative may involve two or more public bodies who wish to share information with each other in order to set up a central database of useful information that they may each access. This information could be, say, limited to up-to-date names and addresses of citizens. Alternatively, it could be information about children thought to be at risk of serious physical harm. Consideration will need to be given to the following legal issues:

Vires issues

- Does the body that it is to hold and administer the database (the 'data controller') have the *vires* to do so? In determining this question careful consideration will need to be given to the existing legal powers that that body has and whether these powers extend to the holding and operation of the new database.
- Is the existing data that is to be shared subject to relevant statutory prohibitions whether express or implied? For example, the sharing of information relating to council tax may be subject to a relevant statutory prohibition that would make any sharing of that information *ultra vires*.
- Even if there are no relevant statutory restrictions, do the bodies sharing the data have the *vires* to do so? This will involve careful consideration of the extent of express statutory, implied statutory and common law and prerogative powers if relevant.

If there is no existing legal power for the proposed data collection and sharing, then consideration should be given to establishing a statutory basis by enacting new legislation.

Human Rights Act issues

- Is Article 8 of the ECHR engaged i.e. will the proposed data collection and sharing interfere with the right to respect for private and family life, home and correspondence? If the data collection and sharing is to take place with the consent of the data subjects involved, Article 8 will **not** be engaged.
- If Article 8 of the ECHR is engaged, is the interference (a) in accordance with the law; (b) in pursuit of a legitimate aim; and (c) necessary in a democratic society?

Common law of confidence issues

- Is the information confidential i.e. does it (a) have the necessary 'quality of confidence?'; (b) was the information in question communicated in circumstances giving rise to an obligation of confidence?; (c) Has there been an unauthorised use of that material? Consider here whether the information has been obtained subject to statutory obligations of confidence. If the data collection and sharing is to take place with the consent of the data subjects involved, the information will **not** be confidential.
- If the information is confidential is there an overriding public interest that justifies its disclosure? The law on this aspect overlaps with that relating to Article 8 of the ECHR.

Data Protection Act issues

- Does the DPA apply i.e. is the information personal data held on computer or as part of a 'relevant filing system'?
- If the DPA applies, can the requirement of 'fairness' in the First Data Protection Principle be satisfied?
- Can one of the conditions in Schedule 2 be satisfied? Of particular relevance to public sector data sharing are the requirements in paragraph 5 that relate to public functions.
- If the data are sensitive personal data can one of the conditions in Schedule 3 **also** be satisfied? Paragraph 7 which is in similar terms to paragraph 5 of Schedule 2 may be applicable.
- Can the requirement of compatibility that is in the Second Data Protection Principle be complied with?
- Do any of the exemptions that are set out in the DPA apply?
- For further information about the above, please refer to the relevant parts of this guidance. Depending on the facts of the case, there may be other legal issues to consider.

APPENDIX 4

The Data Protection Principles

- **The First Principle:** *'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.'*
- **The Second Principle:** *'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.'*
- **The Third Principle:** *'Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.'*
- **The Fourth Principle:** *'Personal data shall be accurate and, where necessary, kept up to date.'*
- **The Fifth Principle:** *'Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.'*
- **The Sixth Principle:** *'Personal data shall be processed in accordance with the rights of data subjects under this Act.'*
- **The Seventh Principle:** *'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.'*
- **The Eighth Principle:** *'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.'*

APPENDIX 5

Conditions in Schedule 2 and 3 to the Data Protection Act 1998

Conditions in Schedule 2:

Paragraph 1: The data subject has given consent to the processing.

Paragraph 2: The processing is necessary for (a) the performance of any contract to which the data subject is a party; or (b) for the taking of steps at the request of the data subject with a view to entering into a contract.

Paragraph 3: The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

Paragraph 4: The processing is necessary in order to protect the vital interests of the data subject.

Paragraph 5: The processing is necessary: (a) for the administration of justice; (b) for the exercise of any functions conferred on any person by or under any enactment; (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department; or (d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

Paragraph 6(1): 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.

Paragraph 6(2): The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

Conditions in Schedule 3:

Paragraph 1: The data subject has given explicit consent to the processing.

Paragraph 2: The processing is necessary for the purposes of exercising or performing a legal right or obligation in the context of employment.

Paragraph 3: The processing is necessary to protect the vital interests of the data subject or another in cases where consent cannot be obtained.

Paragraph 4: The processing is of political, philosophical, religious or trade union data in connection with its legitimate interests by any non-profit bodies.

Paragraph 5: The processing is of information made public as a result of steps deliberately taken by the data subject.

Paragraph 6: The processing is necessary in connection with legal proceedings or the seeking of legal advice.

Paragraph 7: The processing is necessary (a) for the administration of justice; (b) for the exercise of any function conferred on any person by or under any enactment; (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

Paragraph 8: The processing is necessary for medical purposes and is carried out by medical professionals or others owing an obligation of confidence to the data subject.

Paragraph 9: The processing is necessary for ethnic monitoring purposes.

Paragraph 10: The personal data are processed in circumstances specified in an order made by the Secretary of State for certain purposes. The *Data Protection (Processing of Personal Data) Order 2000 (SI 2000 No 417)* specifies a number of circumstances in which sensitive personal data may be processed such as crime prevention, policing and regulatory functions (subject to a substantial public interest test); counselling (subject to substantial public interest test); insurance, equality monitoring in the area of disability and religious or other beliefs; and research. A further order relates to the processing of sensitive personal data by MPs and other elected representatives (*The Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002 (SI 2002 2905)*).