Public Sector Data Sharing: Guidance on the Law

- Section 1 - Introduction
- Section 2 - Overview of existing legal framework
- Section 3 - Power to share data
- Section 4 - The Data Protection Act 1998
- Section 5 - The Human Rights Act 1998
- Section 6 - Common law and statutory restrictions on the disclosure of data
- Section 7 - Practical and other issues
Section 1 - Introduction

This document is intended to be a general guide and to offer key information on relevant legal issues on data sharing to lawyers and to other interested professionals working in the public sector (including those working for local authorities). We hope it will increase understanding of the existing legal framework\(^1\) which governs public bodies’ rights to share personal data and their responsibilities when doing so. It is not intended to be a substitute for specific legal advice on particular issues. Any public body contemplating data sharing should seek its own legal advice.

Purpose of this Guidance

This guidance seeks to clarify the legal circumstances in which the data sharing powers of public bodies can be exercised. Effective data sharing can assist in meeting policy objectives and lead to improved services 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. However, there is evidence to suggest that legal uncertainty over what is, and what is not, permissible may be inhibiting data sharing by local authorities. Similarly, some government departments decide not to pursue new data sharing initiatives because of doubts over what their legal powers allow them to do.

This guidance also seeks to explore the legal landscape governing the use of data sharing powers, and to help bring about a consistency of approach within the public sector, by facilitating lawful data sharing and good practice amongst the public sector.

Scope of this Guidance

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:

\(^1\)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) The 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

2) Sharing of personal data for statistical purposes.

If the data to be shared is fully anonymised, then it will be less likely for problems should arise, though consideration still has to be given to the principles in the Data Protection Act 1998 (DPA). If the data required for statistical purposes contains information which may identify individuals (personal data), then the sharing should be approached in the same way as for any other circumstances, as explained in this guidance.

In preparing this guidance, we have consulted the Information Commissioner, the Local Government Association and government departments.
Section 2 - Overview of existing legal framework

Power to share data

1. When considering whether a proposal to share data is lawful, it is first necessary to consider whether the parties to the proposed arrangement have the necessary powers.

2. A public body may only share data if it has power to do so. The power may be set out expressly in statute, or it may be implied from the body’s other statutory powers and functions. Government departments headed by a Minister of the Crown may also have common law powers to share data.

3. It is also 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.

4. For a more detailed discussion, see sections 3 and 6.

The Data Protection Act 1998

5. If it has been established that the parties have the necessary powers, the next step is to consider whether the proposal is compatible with other legal provisions regulating the use of personal data.

6. The principal legislative provision relating to data protection is the Data Protection Act 1998 (‘DPA’), which implements the Data Protection Directive 95/46/EC. The DPA gives individuals a number of important rights to ensure that personal information covered by the Act is processed lawfully. It regulates the manner in which such information 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 4.

7. It is important to note at the outset that the DPA regime does not cease to apply if information about individuals is already in the public domain. Public bodies wishing to share data which has previously been published or has otherwise been made available to the public remain subject to the requirements of the legislation.

8. The DPA only permits data sharing that is ‘lawful’. When considering whether this is the case, it may be necessary to consider other legal regimes, such as

- the Human Rights Act and the European Convention on Human Rights (section 5); and
- duties of confidence (section 6).
Section 3 - Power to share data

General

1. A public body may only share data if it has power to do so. The power may derive from statute (expressly or impliedly), or from the common law. Public bodies that are not central government departments headed by a Minister of the Crown (such as non-departmental public bodies) will normally, but not always, derive their powers entirely from statute.

2. There is no general statutory power to disclose, obtain, hold or process data. So when considering whether a body has statutory power to share data, it will be necessary to consider the specific legislation governing the policy or service that the data sharing would support. That legislation may include an express power to share data, or it may do so impliedly.

3. **Express** powers to share data give the highest degree of certainty, but are relatively rare and tend to be confined to specific activities and be exercisable only by named bodies. It will be more common to rely on **implied** powers.

4. In the case of central government departments headed by a Minister of the Crown, even if a power to share data cannot be reasonably implied from statutory provisions defining the Minister’s powers, the Minister may still have common law powers to share data.

Express statutory powers

5. Some legislation includes explicit ‘gateways’ by which information can be disclosed or received for particular purposes. Such gateways may be permissive (creating a discretionary power to disclose or receive data) or mandatory (requiring data to be transferred in certain circumstances).

6. Examples of permissive statutory gateways include:
   - **Schedule 2 paragraph 18A of the Local Government Finance Act 1992**, allowing local authorities to use council tax data to identify empty properties;
   - **section 115 of the Crime and Disorder Act 1998**, allowing anyone to pass information to certain authorities if it is necessary or expedient for the purposes of any provision of the Act;
   - **section 17 of the Anti-Terrorism, Crime and Security Act 2001**, allowing disclosures under the statutory provisions specified in **Schedule 4** for purposes connected with criminal investigation and prosecution, where such disclosures are proportionate;
• regulation 27 of the Road Vehicles (Registration and Licensing) Regulations 2002, allowing the Secretary of State to make any particulars contained in the vehicle registration register available to a number of specified persons; and
• section 14 of the Offender Management Act 2007, allowing data sharing between specified bodies for various purposes relating to offenders.

7. Examples of mandatory statutory gateways include:
• section 8 of the National Audit Act 1983, imposing a legal obligation on public bodies to provide relevant information to the National Audit Office; and
• section 17 of the Criminal Appeal Act 1995, making 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.

8. The words of the statute must be carefully considered to establish whether a statutory gateway authorises disclosure or receipt for the particular purpose contemplated.2

9. Where the State’s coercive powers are engaged, these should not encroach upon individuals’ rights more than is fairly and reasonably necessary.3

Implied statutory powers

10. Where no express statutory power to share or receive data exists, such a power may be implicit in the provisions defining the relevant powers or functions. Many activities of statutory bodies will necessarily be carried out pursuant to implied statutory powers, given the difficulty of defining expressly all the activities that they may carry out in connection with their day-to-day functions. The courts will interpret implied powers relatively generously.4

11. Activities such as data collection and sharing are not of themselves usually express statutory functions, but may be incidental to other statutory functions.5

---

2 See, for instance, DfT’s guidance on the circumstances in which information in the vehicle registration register can be disclosed under regulation 27 of the Road Vehicles (Registration and Licensing) Regulations 2002 to a person who can show he has ‘reasonable cause’ for wanting the information.

3 Morris v Director S.F.O. [1993] Ch 372

4 Attorney General v Great Eastern Railway Co (1880) 5 App Cas 473, Lord Selborne LC: “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.”

5 For example, in R v Chief Constable of the North Wales Police ex p AB [1999] QB 396 the Court of Appeal accepted that the police had power to disclose information about paedophiles to individuals living in the relevant area, because disclosure was for the purposes of performing their public duties. Similarly, in Woolgar v Chief Constable of Sussex Police [2000] 1 WLR 25 the Court of Appeal accepted that the police had power to disclose information to a regulatory body for the purposes of an inquiry as this was in the public interest.
12. When considering whether a body has an implied power to share data, it is firstly necessary to identify the function or activity to which that sharing would be ancillary. If the body does not have the power to perform that function or activity, there can be no implicit power 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.6

13. In particular, local authorities may have power to share data under the following provisions:

- **Section 111(1) of the Local Government Act 1972**, providing that they “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**, providing that they 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”.7

- **Section 17 of the Children Act 1989**, imposing a general duty on them to provide services to meet children’s needs.8

- Similarly, the police and local authorities have implied power to share data as part of their statutory duty under section 6 of the **Crime and Disorder Act 1998** to formulate and implement strategies for reduction of crime in their area.9

---

6 See, for example, the restrictions on sharing council tax data in paragraph 17 of **Schedule 2 to the Local Government Finance Act 1992**.

7 See DCLG’s guidance **Power to promote or improve economic, social or environmental well-being** (March 2000) and the **Power to promote well-being of the area: Statutory guidance for local councils** (February 2009). In **R (Stanley, Marshall and Kelly) v Metropolitan Police Commissioner [2004] EWHC 2229 (Admin)**, at [21], the court accepted that section 2(1) of the Local Government Act 2000 gives local authorities a legal basis to disclose information about particular individuals who are the subjects of anti-social behaviour orders.

8 **R v Local Authority and Police Authority in the Midlands ex parte LM [2000] 1 FLR 612** (police and social services have the power to disclose to a third party allegations of sexual abuse of children if they genuinely and reasonably believe that it is desirable to do so to protect children); **R (A) v Hertfordshire County Council [2001] EWHC 211 (Admin)**, at [31] (the local authority had an implied statutory power to notify 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).

9 **R (Ellis) v Chief Constable of Essex Police [2003] EWHC 1321 (Admin)** at [32]. See the Criminal Justice System guidance, **Publicising Sentencing Outcomes** (December 2009).
Common law powers

14. If there is no relevant express or implied statutory power to share data, government departments that are headed by a Minister of the Crown may be able to rely on common law powers to share data.

15. Ministers of the Crown have ordinary common law powers to do whatever a natural person may do, 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 1945.10 However, Ministers’ common law powers may be extinguished by statute11 and may otherwise be limited by the requirements of public law, the law of confidence or by agreement.

16. In relation to data collection, use and sharing, reliance on common law powers by public bodies has not often been considered by the courts, so there might be an element of risk in such reliance. The degree of risk 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 recipients12. It is worth noting that even where common law 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.13

17. Public bodies which are neither central government departments nor organisations which derive their powers from statute will need to analyse carefully what powers (if any) they have to process data and whether there are any explicit or implicit restrictions or limitations upon such processing. Because the powers available to any such body will almost entirely depend upon the specific nature of the body concerned and its legal status, it is impossible to provide general guidance on such cases.

---

10 See also R v Secretary of State for Health ex p C [2000] 1 FLR 627, at [13]-[21]; Shrewsbury and Atcham BC v Secretary of State for Communities and Local Government [2008] EWCA Civ 148, at [44]-[49].

11 See R (Hooper) v Secretary of State for Work and Pensions [2005] UKHL 29, especially [6], [46]-[47], [94]-[95] and [123].

12 See R v Secretary of State for Health, ex parte 'C' [2000] EWCA Civ 49 at [16] – [20] (the Crown has common law power to engage in certain forms of data collection and sharing), R v (1) Worcester County Council (2) Secretary of State for Health ex parte SW [2000] EWHC Admin 392 (such powers may be compatible with Article 8 rights even in the absence of a relevant statutory framework); but contrast Malone v Commissioner of Police for the Metropolis (No 2) [1979] 2 All ER 620 which reached the ECHR as Malone v UK (1984) 7 EHRR 14. The case concerned telephone tapping which the ECHR held to be unlawful in the absence of any clear and accessible legal basis for the infringement of Article 8.

13 See, for example, section 182 of the Finance Act 1989.
Section 4 - Data Protection Act 1998

Application of the Data Protection Act

1. The sharing of personal data is primarily governed by the Data Protection Act 1998 (DPA), which implements the EU Data Protection Directive (Directive 95/46/EC). The DPA establishes a legal framework of rights and obligations that protect personal information.

2. The DPA imposes obligations upon ‘data controllers’ when they are ‘processing’ ‘personal data’, and gives rights to ‘data subjects’. Sections 1 and 2 of the DPA define these concepts:

- ‘Data’ includes all automatically processed information as well as some manual records.14
- ‘Personal data’ means data relating to an identified or identifiable living individual. Anonymised data may still be personal data if the data controller can identify who the information relates to.15
- ‘Sensitive personal data’ are personal data consisting of information as to racial or ethnic origin, political opinions, religious and similar beliefs, trade union membership, physical or mental health, sexual life, and the commission or alleged commission of any offence or criminal proceeding. The DPA imposes additional requirements in relation to the processing (including the sharing) of such data.
- The ‘processing’ of personal data includes anything which may be done to personal data, such as obtaining, holding, using, disclosing or destroying it. Many types of public sector data sharing will involve information held on computer, so if the information relates to identified or identifiable individuals, it will be clear that the DPA applies.
- ‘Data controllers’ are persons who determine the purposes for which, and the manner in which, the personal data are processed.
- ‘Data processors’ are persons who process personal data on behalf of a data controller, rather than on their own behalf.
- ‘Data subjects’ are the individuals to whom the personal data relate.

---

14 Further guidance on the definition of ‘data’ can be found on the ICO’s website. See in particular Technical Guidance Note – Determining what information is ‘data’ for the purposes of the DPA dated 28 January 2009

15 Common Services Agency v Scottish Information Commissioner [2008] UKHL 47, at [27] and [75].
3. Government departments and other public bodies are usually data controllers in relation to personal data they process. In this guidance, the term ‘data sharing’ refers to the processing of personal data by one data controller by giving it (or a copy of it) into the custody and control of another data controller. The term ‘data sharing’ is sometimes used in other contexts to describe the transfer of personal data by a data controller to a third party data processor. However in such transfers the control of the data remains at all times with the data controller, so this does not strictly constitute ‘sharing’.

The data protection principles

4. The eight data protection principles set out in Schedule 1 Part I of the DPA form the core of data protection regulation. The following paragraphs consider how each of the principles may apply in relation to data sharing, but as the first principle raises the largest number of legal issues it is treated in greater detail.

The first principle: fairness and lawfulness

5. This requires that “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”.\footnote{Schedule 1 Part 1 paragraph 1}

- The ‘fairness’ requirement is an objective standard that must be applied on a case by case basis. Thus, for example, if a public authority obtains personal data on the ownership of dishwashers for the purposes of a national survey of living standards, further processing of the data for the production of regional statistics, or the sending of ‘thank you’ letters to the participants, is likely to be fair processing. However, were the information to be further processed so as to enable targeted advertising by commercial interests to the survey participants, that processing would not satisfy the ‘fairness’ condition.

Schedule 1 Part II, discussed below, explains in further detail what is required if processing is to be ‘fair’. But Schedule 1 Part II is not an exhaustive description of what fairness requires. Even if its requirements are met, there may be other aspects of the processing that make it unfair.
• The ‘lawfulness’ requirement means that all relevant legal obligations, both statutory and under common law, must be complied with.

The DPA cannot render lawful any processing which would otherwise be unlawful. This means, in particular, that the authority must have power to carry out the processing, as discussed in Section 3. Some other possible legal constraints are discussed in Sections 5 and 6.

It is always necessary to consider whether at least one condition in Schedule 2 (and, for sensitive personal data, one condition in Schedule 3) is met. But even if it is, the fairness requirement must still be considered separately as noted above.

**Schedule 1 Part II: fairness**

6. Schedule 1 Part II of the DPA, paragraphs 1-4, contains interpretative provisions relating to the requirement of ‘fairness’ in the first principle.

“In determining for the purposes of the first principle whether personal data are processed fairly, regard is to be had to the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed”.

• Thus it would be unfair for a public body to share information which it obtained from individuals if it had told them that the information was solely for its own use and would not be further disclosed.

7. Generally “data are to be treated as obtained fairly if they consist of information obtained from a person who (a) is authorised by or under any enactment to supply it, or (b) 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”.

• So where a statute requires the provision of personal data by or to a public body for a specific purpose (e.g. the mandatory registration of all births with the General Register Office), the obtaining of that data for processing is likely to be fair, regardless of what the individual who supplied the data believed.

---

17 Schedule 1 Part II paragraph 1(1).
18 Schedule 1 Part II paragraph 1(2).
However, the overall requirement of fairness imposed by the first principle would not necessarily be discharged merely by virtue of statutory authority or obligation.

8. Generally, personal data are not to be regarded as being processed fairly unless the data subjects of the personal data are provided with (or have ready access to) certain pieces of information, either prior to, or at the time that the processing first takes place, or very soon afterwards.\(^{19}\) 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 specific circumstances.\(^{20}\)

- Usually this requirement is complied with through the provision of ‘fair processing notices’\(^{21}\) which are drawn to the data subject’s attention when they supply the personal data to the data controller. For example, a local authority may include on an application form for ‘meals-on-wheels’ services a statement that the information provided may be supplied to the Department for Work and Pensions in order to assess whether the data subject is entitled to any other benefits and will not be used for any other purpose. Subject to what is said below, the notification requirements apply whether the data controller obtains the data from the data subject or from elsewhere.

- However, where the data was obtained from a source other than the data subject, there is an exemption\(^{22}\) from the provision of this information where it would involve a disproportionate effort, or where the recording or disclosure of the data is necessary for compliance with a legal obligation. This exemption could apply, for instance, where a local authority seeks historical data from the Department for Education about exam results. In that scenario the contact details of data subjects are unlikely to remain accurate, and so informing them is likely to involve disproportionate effort.

- But even when the exemption applies, the further conditions prescribed in the Data Protection (Conditions under Paragraph 3 of Part II of Schedule 1) Order 2000 must be met. For instance, the information must still be provided upon request by the data subject, and a written record of the reasons why providing a fair processing notice would involve disproportionate effort, must be kept.

---

\(^{19}\) Schedule 1 Part II paragraph 2(1).

\(^{20}\) Schedule 1 Part II paragraph 2(3).

\(^{21}\) The Information Commissioner calls these ‘Privacy notices’ in recent guidance.

\(^{22}\) Schedule 1 Part II paragraph 3.
• Note that the exemption only applies to the requirement to provide information (such as a fair processing notice), and does not reduce the other requirements that have to be satisfied before a processing operation could be considered fair under the first principle. Even if the exemption applies (e.g. when data are obtained pursuant to statutory powers), it could still be unfair for the data controller to fail to provide some or all of the relevant information to the data subject. Whether the processing is fair will depend on the assessment of the processing in the round, and so particular circumstances may require part or all of the relevant information to be provided, despite the applicability of the exemption. For example, if insurance companies were obliged by law to share claims information with a public ombudsman, the exemption would apply, but it could be argued that the ombudsman would have to publicise the fact that the companies had to share their data with him in order to render the processing fair. Careful consideration should, therefore, always be given to ways in which individuals can be provided with this information.

Schedules 2 and 3: conditions for processing

9. Processing of personal data will only be compatible with the first principle if at least one of the conditions in Schedule 2 to the DPA is met, and, in the case of sensitive personal data, that at least one of the conditions in Schedule 3 is also met. Those conditions that are particularly relevant to public sector data sharing are considered in more detail at paragraphs 11 - 29 below.

10. As will be seen, several of the conditions include the requirement that the processing should be ‘necessary’ for a particular function or purpose. Data sharing may be ‘necessary’ in this context if it is a proportionate method of achieving a legitimate objective: it need not be absolutely essential to the achievement of that objective. Whether it is ‘necessary’ will depend on the circumstances of each case, including the sensitivity of the data and the effects that the disclosure may have on the data subjects and third parties.

Schedule 2 conditions of particular relevance to public sector data sharing

23 Stone v South East Coast Strategic Health Authority [2006] EWHC 1668 (Admin), at [60], and R (Ellis) v Chief Constable of Essex Police [2003] EWHC 1321 (Admin), at [29], referring to the discussion in R v (Daly) v Secretary of State for the Home Department [2001] 2 AC 532, at [27]-[28], of what is meant by the equivalent concept in Article 8(2) of the European Convention on Human Rights.
Paragraph 1: consent

“The data subject has given his consent to the processing.”

11. Public bodies which share data may be able to rely on the consent of the data subject to satisfy Schedule 2 (and explicit consent in relation to schedule 3). While consent is the most conclusive of the conditions, it frequently cannot be met. Obviously where another Schedule 2 condition is applicable, it is not necessary to obtain consent. In certain circumstances (such as data sharing in the context of regulatory or enforcement functions) it is unlikely that consent would be an appropriate condition and public bodies will wish to rely on other conditions.

12. It is not always straightforward to establish whether the data subject has given consent. As a general rule the Information Commissioner’s guidance – drawing on Article 2(h) of the EU Directive – suggests that consent should be ‘informed’ and freely given, and that there must have been some active communication from the data subject. For example, if one public body conducted a survey about public services and the survey form stated clearly that the information would be processed and shared with a second body for the purpose of improving those services, it is likely that people completing the form would be regarded as having consented not only to the initial use of the information but also to its being processed by both bodies.

Paragraph 3: compliance with a legal obligation

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

13. This provision covers legal obligations arising from any source other than contract, including statute, EU law or the common law. As explained in paragraph 10 above, ‘necessary’ in this context does not mean ‘absolutely essential’.

14. If there is a relevant statutory gateway that imports a legal obligation to disclose data, then this condition is likely to apply. For example, it 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): administration of justice
“The processing is necessary… for the administration of justice.”

15. This condition is likely to apply to a wide variety of processing activities carried out by courts, tribunals and other bodies that have judicial functions. It would, for example, permit a court to provide a defendant’s criminal and other records to a lawyer appointed by the court at short notice to represent the defendant at a hearing following the execution of an arrest warrant.

Paragraph 5(b): functions conferred by or under an enactment

“The processing is necessary… for the exercise of any functions conferred on any person by or under any enactment.”

16. This condition will include processing carried out pursuant to express statutory powers or reasonably required or ancillary to the exercise of express or implied statutory functions.

17. For example, ombudsmen will often fulfil statutory functions that reasonably require the use and sharing of personal data. Similarly, it will often be appropriate for bodies responsible for law enforcement to share information for the purposes of promoting public confidence in the justice system.

18. When data are shared there are two instances of processing, one by the body making the disclosure and the other by the recipient. Each of these bodies must comply with the DPA, and in particular both bodies must have the appropriate vires (the first to disclose, and the second to receive and further process the data). It may be hard to show that the disclosure is necessary to the first body’s functions. This does not matter for the purposes of paragraph 5(b), because the disclosing body can rely on the fact that the sharing of data is necessary for the functions of the receiving body. For the purposes of paragraph 5(b) what matters is the overall objective of the sharing, rather than the specific objective of either body.

19. In any event, as explained in paragraph 10 above above, ‘necessary’ in this context does not mean ‘absolutely essential’, and data sharing may meet this condition if it is a reasonable and proportionate way for a public body to give effect to its functions.

Paragraph 5(c): functions of central government

---

24 See Stone v South East Coast Strategic Health Authority [2006] EWHC 1668 (Admin), at [60]-[63], and the Criminal Justice System guidance, Publicising Sentencing Outcomes (December 2009). See also R (Ellis) v Chief Constable of Essex Police [2003] EWHC 1321 (Admin), at [29] and [32]-[39], and R (Stanley, Marshall and Kelly) v Metropolitan Police Commissioner [2004] EWHC 2229 (Admin), at [40]-[42].
“The processing is necessary… for the exercise of any functions of the Crown, a Minister of the Crown or a government department.”

20. This condition will cover processing relating to functions carried out by central government departments and offices that derive from the Crown’s common law or statutory powers. It is probably the most commonly used condition for all data processing by central government. If the body concerned is acting within its powers, and in compliance with public law, then – as discussed above – it is likely that the processing will meet the requirement that it is ‘necessary’ for the exercise of its functions.

21. As with paragraph 5(b), for these purposes the disclosing body can rely on the functions performed by the receiving body, and does not need to show that the transfer is necessary for a separate function of its own. For instance, the Ministry of Justice might share data with the Home Office so that the latter can perform its departmental functions. The ‘function’ in question would be that of the Home Office, and the Ministry of Justice may rely on paragraph 5(c) even if it has no separate relevant function of its own.

Paragraph 5(d): other public functions

“...for the exercise of any other functions of a public nature exercised in the public interest by any person.”

22. Similar considerations apply to this condition as to paragraphs 5(b) and (c), but the condition is more broadly worded. As explained in paragraph 10 above, ‘necessary’ in this context does not mean ‘absolutely essential’. This condition 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 – for example, the reservation of beds in hostels run by a voluntary body for persons registered with local authorities as homeless.25

Paragraph 6: legitimate interests of the data controller

“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.”

25 See Stone v South East Coast Strategic Health Authority [2006] EWHC 1668 (Admin) at [60].
23. 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. In most cases where data sharing by a public body could satisfy this condition, it is also likely to satisfy one of the other, more specific, conditions explained above. Consequently we recommend that public bodies rely on this condition only where no other condition can be satisfied. An example which might satisfy only paragraph 6 could be the provision by a local authority of the names and addresses of housebound elderly people to commercial organisations offering appropriate care services.

Schedule 3 conditions of particular relevance to public sector data sharing

24. If sensitive personal data are being shared, one of the conditions in Schedule 3 must also be fulfilled. Some of the conditions in Schedule 3 closely mirror those in Schedule 2, and there is no prohibition upon relying upon similar conditions in both Schedules, providing of course that they are properly fulfilled; there are slight differences in wording that must be considered.

Paragraph 1: explicit consent

“The data subject has given his explicit consent to the processing of the personal data.”

25. As previously described in relation to paragraph 1 of Schedule 2, consent may form the basis for legitimate data sharing. In relation to Schedule 3, the consent must be ‘explicit’.

26. There is no clear definition of what ‘explicit consent’ means. But the Information Commissioner’s guidance says that the consent must be absolutely clear: it should cover the specific processing details, the type of information (or even the specific information), the purposes of the processing, and any special aspects that may affect the individual, such as any disclosures that may be made.

27. Public bodies should satisfy themselves when relying on this condition that the individual was fully aware of all the relevant details of the proposed sharing. This should, at a minimum include details of exactly what will be shared, with whom, on what basis and for what purpose.

Paragraph 7(1): public functions

“The processing is necessary (a) for the administration of justice,… (b) for the exercise of any functions conferred on any person by or under an enactment, or (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.”
28. 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 respectively, considered above.

29. However, these conditions are included in Schedule 3 by virtue of Article 8(4) of the EU Directive, which requires that any processing must be for reasons of “substantial public interest and subject to suitable safeguards”. This reinforces the point that public authorities will need to consider particularly carefully how the conditions apply when they wish to share sensitive personal data.

The other data protection principles

The second principle: purposes

“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.”

30. Paragraphs 5 and 6 of Schedule 1 Part II contain interpretative provisions relating to the second principle. Paragraph 5 provides that the purpose or purposes for which personal data are obtained may, in particular, be specified either in a fair processing notice, or “in a notification given to the [Information] Commissioner under Part III of the Act”.

31. Paragraph 6 states that further processing must not be ‘incompatible’ with the purpose for which the data were obtained; incompatible processing would of course not be fair. But 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. 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.

32. For example, it would not offend the second principle for data originally obtained for local authority administrative purposes subsequently to be shared with the police to prevent crime pursuant to the power in section 115 of the Crime and Disorder Act 1998. The two purposes are not incompatible. However, a public authority in receipt of complaints about canvassing by private companies from members of the public which passed complainants’ details to other companies for commercial purposes would clearly be processing their data for an incompatible purpose.
The third principle: adequate, relevant and not excessive

“Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.”

33. When considering a data sharing request or project, public bodies should focus on the objective of the exercise, decide what information is actually required to achieve it, and limit the scope of the shared data accordingly.

34. Hence, bulk transfers of data including irrelevant material should not be conducted merely as a matter of convenience. That said, there may be circumstances in which it would be impracticable or prohibitively expensive to separate particular fields or records from a dataset prior to a transfer. If that is the case, a bulk transfer which includes limited amounts of material which is irrelevant to the intended purpose may not be regarded as excessive.

The fourth principle: accurate and up to date

“Personal data shall be accurate and, where necessary, kept up to date.”

35. In a data sharing exercise, a public body which is the recipient of personal data collected by another organisation will have relatively limited responsibilities in relation to this principle. The requirement is that having regard to the purpose or purposes for which the data were obtained, reasonable steps must be taken to ensure its accuracy. It must store the data so that it remains as accurate as it was when it was received, but it is not responsible for any existing errors.

36. If, however, data subjects inform the sending authority that the data it holds about them is incorrect, it should notify the recipient authority so that it too can rectify or mark the disputed accuracy of, the data. Equally a data subject could notify the receiving authority directly of the alleged inaccuracy. In that case the recipient should also either rectify or mark the data as appropriate, and it is good practice for it to notify the sending authority of the alleged inaccuracy.

The fifth principle: information not to be kept longer than necessary

“Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes”.

26 Paragraph 7, part 2 Schedule 1 DPA
27 And indeed it may be ordered to do so by a court under section 14(3) of the DPA.
37. Unless there is good reason to retain it, information should be destroyed by the recipient once a data sharing project has come to an end. If a data sharing agreement (see Section 7 below) is used it should make appropriate provision for this, and it is often good practice to include a specific deletion schedule. Even where a formal data sharing agreement is not used, it is essential that the recipient makes provision to ensure that the personal data it has received is kept no longer than is necessary for the purpose for which it was received.

38. Section 33 of the DPA provides an exemption to this principle, allowing data controllers to keep personal data indefinitely where necessary for historical, research or statistical purposes, provided that certain conditions are met. See paragraph 61 below.

The sixth principle: rights of data subjects

“Personal data shall be processed in accordance with the rights of data subjects under this Act.”

39. The rights of data subjects are set out in Part 2 of the DPA. These rights apply in the context of public sector data sharing to both the sender and the recipient of the data, as they do to all other processing operations, but no specific considerations arise.

The seventh principle: keeping personal data secure

“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.”

40. High-profile data losses have resulted in greater emphasis on security and the imposition on all central government departments of mandatory minimum security measures.

41. Data sharing agreements should specify the security arrangements, both technical and administrative in nature that each party will put in place.

The eighth principle: transfer outside the EEA

“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.”

28 The EEA includes the EU Member States plus Norway, Iceland and Lichtenstein.
42. Data sharing between UK public bodies and organisations outside the EEA involves considerations which are beyond the scope of this guidance but are comprehensively covered in the ICO’s guidance [Sending personal data outside the European Economic Area](#).

**Exemptions**

43. The DPA provides exemptions from the data protection principles to permit disclosures which would otherwise be in breach of the Act. It is vital to note that the exemptions merely allow data controllers to avoid certain requirements of the DPA in certain tightly-defined circumstances if they wish to do so. They neither *create* any legal power to share or disclose data nor *impose any obligation* to do so.

44. Each exemption is quite specific and it is important to be clear as to its exact scope and terms before seeking to rely on it. Moreover, even if an exemption may be available, public bodies should first consider whether it is possible to achieve their aims by acting in accordance with the data protection principles. This is particularly important when consideration is given to exemptions from the non-disclosure provisions (see below), because such exemptions *only* apply to the extent that the disclosure is inconsistent with those provisions, and no further.

45. This guidance deals only with those exemptions which are most likely to be of relevance to public sector data sharing. It begins with an explanation of the non-disclosure provisions, which are disapplied by several relevant exemptions, and then considers the relevant exemptions themselves. Legal advice should always be sought as to whether other exemptions not considered here may be applicable.

**Exemptions from the non-disclosure provisions**

46. Certain exemptions – relating to crime and taxation (*section 29*), information available to the public by or under an enactment (*section 34*), and disclosures required by law (*section 35*) – permit the disapplication of the following provisions:
• The first data protection principle (i.e. the requirement that processing be fair and lawful), except to the extent to which it requires compliance with the conditions in Schedules 2 and 3;

• The second, third, fourth and fifth data protection principles; and

• Sections 10 and 14(1) to 14(3) (the rights of a data subject to prevent processing and to seek rectification, blocking, erasure or destruction of personal data).

47. These provisions are collectively defined by section 27(3) and (4) as “the non-disclosure provisions”.

48. However, section 27(3) provides that the exemptions only permit the disapplication of the non-disclosure provisions “to the extent to which they are inconsistent with the disclosure in question”. In other words, where a public body proposes to share data in reliance upon an exemption under sections 29, 34 or 35, the disclosure will be exempted from the non-disclosure provisions only to the extent that it is inconsistent with those provisions. Public bodies contemplating data sharing must therefore take a cautious approach to the use of exemptions. They will not necessarily permit the disapplication of all the non-disclosure provisions. Having decided that one (or more) of the above exemptions does apply to the proposed sharing, they must consider each of the non-disclosure provisions and decide which, if any, would be inconsistent with those disclosures. If there are inconsistencies, the data controller may then disapply those provisions but only to the extent of the inconsistency.

49. Consider, for example, a public registry which processes personal data files, and which is obliged by law to disclose selected details from those files to the public upon request. Disclosure of those details is permissible because section 34 provides an exemption from the non-disclosure provisions where the data controller is obliged to make the information in question available to the public under an enactment. The non-disclosure provisions are therefore inconsistent with the disclosure in question.

50. A further example would be of a bank faced with a statutory request for information about a client’s deposits from a body charged with investigating money laundering. The bank could rely on section 34. It will be exempt from the non-disclosure provisions to the extent that the disclosure is inconsistent with them. Hence, it may rely on the exemption in respect of the first data protection principle (fair and lawful processing) and the second principle (processing only for limited and compatible purposes) as they would be inconsistent with the disclosure. However, the disclosure would not be inconsistent with

---

29 Hence even if a disclosure of personal data is exempt from the requirement of fairness and lawfulness, it will still be necessary to comply with one condition in Schedule 2 and (if sensitive personal data are involved) one in Schedule 3.
the third principle (adequacy, relevance and not excessive) and the bank should therefore
disclose only information about the client’s deposits, and not details of his payments.

**Exemptions from the subject information provisions**

51. Other exemptions apply to “the subject information provisions” which are defined in
section 27(2) as including the information to be communicated in fair processing notices
(see paragraph 8 above).

**Exemptions of particular relevance to public sector data sharing**

52. The following exemptions may be particularly relevant in the context of data sharing.

**Section 28: national security**

53. Section 28 provides that personal data are exempt from certain provisions of the Act “if
the exemption from that provision is required for the purpose of safeguarding national
security.”

54. 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 (in
particular all the data protection principles) if exemption from those provisions is required
for the purpose of national security. For instance, the UK Borders Agency might rely on
this exemption when it shares data with police forces and the security services about
specific individuals who have entered the country.

55. While section 28 can be relied on in the same manner as any other exemption, it also
contains an optional certification procedure under 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 Tribunal\textsuperscript{30} under section 28(4).

**Section 29: crime and taxation**

56. Section 29 applies to personal data processed for (a) the prevention or detection of
crime; (b) the apprehension or prosecution of offenders; or (c) the assessment or
collection of any tax or duty or of any imposition of a similar nature.

57. The exemption only has effect to the extent to which the application of the exempted
provisions would be ‘likely to prejudice’ any of these matters.

\textsuperscript{30} Originally the Information Tribunal; now the First-tier Tribunal, Information Rights.
Section 29(1) covers the first data protection principle (except to the extent that it requires compliance with Schedule 2 and, where relevant, Schedule 3) and the rights of data subjects contained in section 7. By section 29(2), those elements of the exemption are transferable to and may be relied upon by a recipient of the data who processes it for the purpose of discharging statutory functions. Section 29(3) is more broadly framed: it exempts the data from all the non-disclosure provisions, but those provisions cannot be relied upon by a transferee of the data.

This exemption will be particularly relevant to public bodies which have as their primary purpose the investigation of crime, the prosecution of offenders or the collection of tax. It could allow the police to share data with another body in relation to a specific case where, but for the exemption; such processing would be prohibited for being unfair because, for example, the data was provided to the original recipient on the basis that it would not be further disclosed. However, 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 cannot be used to justify routine or sharing.

Section 33: research

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.

Section 33(1) provides that the processing must comply with two conditions: the data must not be processed to support measures or decisions with respect to particular individuals, nor be processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

Section 34: information available to the public by or under an enactment

By section 34, 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. Compliance with the DPA when sharing data such as public marriage registers is substantially easier than in relation to other types of data.
Section 35: disclosures required by law

64. By section 35, 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.

65. 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

66. 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 by data controllers

67. 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.

68. In notifying the Commissioner, the data controller must provide certain particulars which are specified in sections 16 and 18 and which include descriptions of the personal data being processed, the purposes of the processing, and any recipients to whom the data may be disclosed; and details of security measures in place.

69. All public bodies which are data controllers should of course already be registered as a matter of course in relation to the processing they undertake for their own purposes. However, as the registration requirements also specifically oblige the data controller to provide a description of any recipients to whom data may be disclosed, public bodies intending to share data must consider whether their notifications should be updated.
Enforcement of the DPA and consequences of non-compliance

Information Commissioner’s powers

70. 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.

Section 43: information notices

71. Section 43 provides that if the Information Commissioner receives a request for a data protection compliance assessment under section 42, 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.

72. The Information Commissioner could issue an information notice to a data controller requesting documents relating to a particular data sharing project if he was concerned that the sharing did not comply with the DPA.

Section 40: enforcement notices

73. Under section 40, the Information Commissioner may serve an enforcement notice where he is satisfied that any of the data protection principles are being contravened. An enforcement notice may require the data controller to stop processing personal data or stop processing personal data in a particular manner, or require the data controller to take certain steps to remedy the unlawful processing within a certain time. The data controller has a right of appeal to the Tribunal against the service and extent of these notices.

74. In the context of data sharing, the Information Commissioner could conclude that an agreement between two bodies involved the sharing of excessive and irrelevant data. He could issue an enforcement notice requiring the bodies to share only specific relevant data.
**Section 42: assessments**

75. **Section 42** provides that 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 complies 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.

**Section 55A: civil monetary penalties**

76. The Information Commissioner has power under section 55A to impose a civil monetary penalty on any data controller who commits a serious contravention of the data protection principles which is likely to cause substantial damage or distress. A penalty can be imposed if the contravention was deliberate, or if the data controller knew or ought to have known that there was a risk of a harmful contravention but did not take reasonable steps to prevent it.

77. A penalty could be imposed on a public authority which shares data if the sharing amounted to a serious contravention of the data protection principles. For example, a public body which obtained personal data by consent solely for the purposes of fulfilling its statutory functions, and then shared it with a commercial organisation in a country not considered ‘adequate’ (e.g. a non EEA country) on payment of a fee, would potentially be in breach of the first, second and eighth data protection principles and could cause substantial damage or distress. In such (admittedly unlikely) circumstances, a civil monetary penalty could be imposed.

**Civil remedies**

78. A further remedy available to data subjects is 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

79. 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). A government department is not liable to prosecution under the (section 63(5)).
Section 5 - the Human Rights Act 1998 and the European Convention on Human Rights

1. Data sharing by public authorities must comply with the European Convention of Human Rights (now part of the UK domestic law as a result of the Human Rights Act 1998), and in particular Article 8, which provides:

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

   *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.*

2. Processing personal data (including sharing it) will often constitute an ‘interference’ with the right to respect for private and family life within the meaning of Article 8.\(^{31}\) However, an interference will be compatible with Article 8 if it meets the requirements of Article 8(2).

   - The interference must be ‘in accordance with the law’: it must have a proper basis in national law and that law must be adequately accessible and foreseeable.\(^{32}\)
   - If a public body has a lawful basis for sharing data, as set out in section 3 above, then it is likely that this requirement will be met.\(^{33}\)
   - The interference must answer a ‘pressing social need’, which will be the case if it pursues a legitimate aim in a proportionate manner and is accompanied by appropriate safeguards.\(^{34}\)

---

\(^{31}\) E.g. *S and Marper v United Kingdom*, App. Nos. 30562/04 and 30566/04, paragraph 67: “The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8... The subsequent use of the stored information has no bearing on that finding... However, in determining whether the personal information retained by the authorities involves any of the private-life aspects mentioned above, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained.” See also *R (Robertson) v City of Wakefield Metropolitan Council* [2001] EWHC 915 (Admin), at [29]-[34].

\(^{32}\) *S and Marper v United Kingdom*, App. Nos. 30562/04 and 30566/04, paragraphs 95-96; *Gillan and Quinton v United Kingdom*, App. No. 4158/05, paragraphs 76-77.


• If data sharing is covered by, and complies with, the DPA then it is almost certain
  that it will also comply with Article 8.  The safeguards in the DPA derive from
  Article 8: the Act gives effect to the Data Protection Directive and the Council of
  Europe Convention on Data Protection, that set out in more detail the
  requirements of Article 8 for the processing of personal data.

3. However, there may be rare occasions where data sharing falls outside the DPA on
  technical grounds (such as because it involves processing of manual records in a way
  that is not covered by the Act), when it will still be necessary to consider whether it is
  compatible with Article 8 of the ECHR.

---

35 See Stone v South East Coast Strategic Health Authority [2006] EWHC 1668 (Admin), at [60],
and R (Ellis) v Chief Constable of Essex Police [2003] EWHC 1321 (Admin), at [29].

36 See recitals 1, 10 and 11 of the Directive; the explanatory report to the Council of Europe
Convention; and the references to that convention in cases such as Z v Finland, App. No.
22009/93, paragraph 95; Amann v Switzerland, App. No. 27798/95, paragraph 65; Rotaru v
Romania, App. No. 28341/95, paragraph 43.
Section 6 - Common law and statutory restrictions on the disclosure of data

Breach of confidence

1. Data sharing will not be ‘lawful’ for the purposes of the first data protection principle (or ‘in accordance with the law’ for the purposes of Article 8 of the ECHR) if it involves a breach of confidence.

2. For the purposes of the law of confidence, different government departments are treated as separate legal persons. Consequently, information cannot be freely disclosed between them without taking into account the common law of breach of confidence.

3. Information about individuals held by a public authority will sometimes be given to it in confidence, or the individuals may have a reasonable expectation that the information will not be disclosed without their agreement. In such cases, the public authority is likely to have a duty of confidence to those individuals.

4. A duty of confidence arises whenever the party subject to the duty is in a situation where he either knew or ought to have known that the other person could reasonably expect his privacy to be protected. The disclosure of data may amount to a breach of confidence if all the following conditions are met:
   - 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). But there is no requirement for a prior relationship to exist between parties, and third parties can also be bound by the duty; and
   - There was an unauthorised disclosure of that material.

37 The DPA mimics this by providing in section 63 that each government department is to be treated as a separate data controller.

38 The classic statement of the law on confidence is Megarry J’s judgment in Coco v A.N.Clark Engineers Ltd [1969] RPC 41, at 47-48, but this is a developing area of law and up to date legal advice should be sought. See also Campbell v MGN Ltd [2004] UKHL 22, at [11]-[22] and [43]-[52].

39 Even where a public authority has received data which is subject to the common law duty of confidence, it may have to disclose it in response to a request under the Freedom of Information Act 2000. It will be able to refuse the request in reliance on the exemption for information provided
5. It is not always necessary for the person alleging breach to prove he suffered damage or detriment, nor is it necessary for him to prove dishonesty or negligence on the part of the person subject to the duty.

6. It is a defence to a claim for breach of confidence that disclosure is necessary in the public interest\(^\text{40}\) (for example, to disclose current or future medical hazards, the unreliability of equipment used to provide evidence for use at criminal trials, or conduct and misrepresentations which mislead the public). In some circumstances this defence is set out in statute.\(^\text{41}\)

**Statutory prohibitions**

7. There are various statutory provisions that prohibit the disclosure of certain types of information in certain circumstances. For example:

   - medical confidentiality (e.g. under section 2 of the Abortion Act 1967)
   - information supplied in connection with legal proceedings (various rules of court)
   - health and safety (sections 27 and 28 of the Health and Safety at Work Etc Act 1974)
   - information supplied to HMRC (section 182 of the Finance Act 1989)
   - 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)
   - Information relating to social security (section 123 Social Security Administration Act 1992)

8. When considering whether any of these provisions prevent the proposed data sharing, it is necessary to consider the provision in detail. Some statutory restrictions provide that any disclosure of certain information will constitute a criminal offence unless that disclosure falls within one of the statutory gateways in the relevant legislation. Other

\(^{40}\) See Attorney-General v Guardian Newspapers (No.2) [1990] 1 AC 109, at 282.

\(^{41}\) For instance, section 68 of the Serious Crime Act 2007. See also section 17 of the Anti-Terrorism, Crime and Security Act 2001, that permits disclosure where it is proportionate: if that is the case, it seems that any obligation of confidence would be overridden.
statutory prohibitions give public authorities a discretion whether to disclose in certain circumstances.
Section 7 – Practical Steps and other considerations

1. This section considers some of the practical steps public authorities should take before committing to data sharing.

Privacy Impact Assessments

2. It is now mandatory for all government departments to carry out Privacy Impact Assessments (PIAs) when introducing new policies or processes involving personal data.42 PIAs will clearly be required when data sharing is taking place. They enable departments to fully understand and evaluate the potential risks that will be posed to the data, and to reach an informed decision about whether to proceed with the sharing the data. Additionally, a PIA conducted at an early stage in a data sharing project may highlight potential problems which would be more costly to overcome if they were only discovered during or after implementation.

3. Each government department is responsible for implementing an appropriate process to undertake these assessments43, taking into account the nature of their business and existing procedures.

4. The Ministry of Justice has published guidance on PIAs for government departments. See also the ICO’s guidance on PIAs.

Data Sharing Agreements

5. For bulk sharing of personal data with other public bodies or organisations it is strongly advisable to have in place a Data Sharing Agreement or Memorandum of Understanding to formally define the project, ensure that relevant considerations have been considered, and record the respective obligations of the parties.44

6. Clauses that it may be appropriate to include in such an agreement are:

- **Shared data**: a description of the information to be shared.
- **Purpose(s)**: the purpose(s) for which the sharing is taking place and consideration of why the sharing is proportionate to the purpose(s).

---

42 This follows from the Data Handling Review the Government published in 2008 which outlines the mandatory minimum measures which government departments must apply to protect information, including personal data.

43 As well as any other relevant mandated assessments such as Human Rights Impact Assessments.

44 The absence of a written agreement underpinning such data sharing may be a breach of the seventh data protection principle.
• **Further use** of shared data: consideration should be given to what further use could be made of the data shared by those who receive it. Provisions may include preventing the recipient from processing the data for purposes other than those for which it is shared without the data controller’s consent or for purposes which are incompatible with the purposes for which it was shared.

• **Roles**: In most cases where public sector bodies share data, both the sending and receiving organisations will be using some or all of the data for their own purposes and both will therefore be data controllers of at least some of the data. The agreement should state which body is the controller of which data and how it will be shared and used. Where one body is a data controller and the other is a data processor in relation to all or part of the data, their respective roles should be defined. This approach will in part determine the responsibilities each party has under the DPA.

• **Legal basis** on which data is being shared: a description of the legal powers that both organisations rely upon in order to share the data.

• **Security** of shared data:

  - Data controllers are responsible for the security of the data they hold. This responsibility requires the sending organisation to ensure that the information is kept secure during the sharing process, and they must also take reasonable steps to ensure it will be kept secure by the recipient.\(^{45}\)

  - The agreement should set out an explanation of the security arrangements that will be in place in relation to the shared data such as any applicable security standard, permissible copies, confidentiality, means of access to the information, storage facilities and encryption of data.

  - Where data is sent to a data processor who will process data on the data controller’s behalf, there must be a written contract in place which provides for the 7th data protection principle to be observed by the data processor as well as requiring the data processor to act only on the instructions of the data controller. (As previously mentioned, such data processing transfers are not usually considered data sharing).

---

\(^{45}\) The recipient body, as an independent data controller, will have responsibility for the security of the data it receives. However, where sharing is ongoing, the sending body will not be absolved from responsibility and will be obliged to cease sharing data if the recipient has previously failed to meet appropriate standards of security and there are no reasonable grounds to believe that the additional data shared would be secure.
• **Integrity** of shared data: the obligations of the recipient of the data to preserve its integrity.

• **Freedom of Information**: where one or more of the parties to the data share are subject to the Freedom of Information Act or the Environmental Information Regulations the agreement should provide for the parties to assist each other in responding to requests, e.g. by providing information where appropriate if it is in their possession, and for the co-ordination of any responses to such requests to ensure consistency.

• **Inspection**: the data provider may want to retain oversight of how the data is being held and used.

• **Loss and unauthorised release**: the steps to be taken if data is lost or released without authorisation. They could include a requirement for the recipient to report any loss as soon as possible and an obligation to conduct an investigation. The agreement may require the recipient to indemnify the provider of the data for all financial liability that may arise as a result.

• **Actions at the end of the project**: what will happen to the data, e.g. arrangements for its destruction and the provision of written confirmation of the same.

**Use of Codes of Practice**

7. Codes of practice set out 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. The Information Commissioner has the power to prepare codes of practice when he considers it to be appropriate: see his [Framework Code of Practice for Sharing Personal Information](#). He has regard to such guidance when considering compliance with the DPA and enforcement action. Government departments can also issue their own codes where relevant. One example is the Department for Work and Pensions [Code of Practice on Obtaining Information under the Social Security Fraud Act 2001](#) (April 2002) which includes provisions about confidentiality, security and complaints procedures.
Useful contacts and websites

- The Ministry of Justice has responsibility for the DPA, the Human Rights Act 1998 and the Freedom of Information Act 2000 and publishes guidance on its website on topics relating to these statutes.
- The website of the Office of the Information Commissioner includes extensive legal and practical guidance on the DPA and the Freedom of Information Act.
- The Statute Law Database (maintained by the Office of Public Sector Information, part of the National Archives) contains the text of relevant legislation.
- European Court of Human Rights case law is published on the Hudoc database.
- BAILLI, the British and Irish Legal Information Institute website, publishes British and Irish case law and legislation, European Union case law, Law Commission reports, and other law-related British and Irish material.
- The Home Office has published guidance and practice advice on data sharing for crime prevention and reduction: see Information Sharing for Community Safety (March 2010)