

## DATA EXCHANGE – THE LEGAL IMPLICATIONS

1. Exchanges of data must have a lawful basis, and must also take place within the constraints of all the relevant legislation, essentially the common law duty of confidence, the Data Protection Act 1998, the Human Rights Act 1998 and various statutory provisions for exchange or prohibitions on disclosure.
2. These pages outline the main principles behind data exchange<sup>1</sup>.

### Common Law

3. Common law jurisdictions have established torts to protect individuals' rights to privacy. Torts are essentially civil wrongs that provide individuals with a cause of action for damages in respect of the breach of a legal duty. A number of common law torts afford protection to individuals' private interests and their confidential information. With regard to the use and disclosure of personal information, the tort of breach of confidence is clearly the most relevant.
4. The common law tort of breach of confidence deals with unauthorised use or disclosure of certain types of confidential information and may protect such information on the basis of actual or deemed agreement to keep such information secret.

### Breach of Confidence

5. A common law of breach of confidence action may arise where information carrying the necessary quality of confidence is communicated in circumstances entailing an obligation of confidence and the information is later used in an unauthorised way.
6. Public authorities must be mindful of the extent of the duty of confidence they owe in considering whether to take part in data-sharing exercises or whether they are precluded from so doing.
7. The courts have generally recognised that a public authority may ignore the duty of confidence it owes with regard to a particular information item:

---

<sup>1</sup> This document contains material taken from the Annex of a draft Report on Privacy and Personal Data by the Cabinet Office. The Report sets out a strategy for better delivery of essential public services through better use of personal data, and describes the safeguards that will need to be put in place to inspire public confidence in the public sector's handling of personal data. The Annex gives a background to the main legal principles to be considered.

- Where there is legal requirement (either under statute or a court order) to disclose the information (for instance, notification of certain diseases to public health authorities);
  - Where there is an overriding duty to the public (for instance, the information concerns the commission of a criminal offence or relates to life-threatening circumstances); or
  - Where the individual to whom the information relates has consented to the disclosure.
8. Furthermore, while there is an obligation on the part of the recipient of the information “not to take unfair advantage of it”, the purpose for which the information may be used need not necessarily be that for which it was provided. A breach of confidence will only occur where the disclosure of information is an abuse or unconscionable to a reasonable man.
  9. However, it is clear that the action for breach of confidence has a broad application to personal information provided to public authorities. Public authorities must be mindful of the extent of the duty they owe in considering whether to take part in data-sharing exercises or whether they are precluded from so doing.
  10. Breach of confidence will depend of a range of circumstances.
  11. There are certain cases in which doctors could disclose confidential personal information without the patient’s consent because the greater benefit might outweigh the duty of confidence.
  12. The case studies under the Data Protection section and Human Rights section below are also relevant.

## **Data Protection**

13. The Data Protection Act 1998 (“DPA”), which updated the Data Protection Act 1984, regulates the processing and handling of personal data which has been lawfully obtained. The Act provides for a framework of notification by data controllers with an independent supervisory authority – the Data Protection Commissioner (“DPC”).

### **The Data Protection Principles**

14. The DPA sets out 8 Data Protection Principles. The basic purpose of the Principles is to enshrine broad formulations of acceptable processing practice. Under Schedule 1 personal data must be:

1. fairly and lawfully processed [and in accordance with one of the conditions for fair processing set forth in Schedule 2 and with regard to sensitive personal data one of the conditions set forth in Schedule 2 as well as one set forth in Schedule 3];
  2. data must not be further processed in a manner incompatible with the purpose for which they were obtained;
  3. adequate, relevant and not excessive;
  4. accurate;
  5. not kept longer than necessary;
  6. processed in accordance with the data subject's rights;
  7. secure; and
  8. not transferred to countries without adequate protection.
15. The first and second data protection principles contain and require the compliance with significant conditions. The data protection principles apply to all personal data processed by data controllers, unless one of the exemptions of the Act applies, which provide limited relief.

### **The First Principle**

16. Under the First Data Protection Principle, personal data is required to be processed not only “lawfully” in accordance with applicable law and the provisions of the Act, but also “fairly”. On each occasion that personal data are processed, the data controller must, as a requisite of fair and lawful processing, have legitimate grounds for doing so in accordance with Schedule 2 of the Act (and with respect to sensitive personal data, Schedule 3 of the Act).
17. Schedule 2 sets out the following possible grounds for these purposes:
1. Processing with the consent of the data subject;
  2. Processing necessary for the performance of a contract to which the data subject is a party or which is necessary for entering into a contract;
  3. Processing which is necessary for compliance with a legal obligation other than one imposed by contract;
  4. Processing which is necessary in order to protect the vital interests<sup>2</sup> of the data subject;
  5. Processing which is necessary for the administration of justice, the exercise of any functions conferred by or under any enactment, the exercise of any functions of the Crown, a Minister of the Crown, or a government department, or the exercise of any other function of a public nature exercised in the public interest;
  6. Processing which is necessary for the purposes of the legitimate interests of the data controller or a third party to whom the data are disclosed, providing that these are not outweighed by the interests of the data subject.

---

<sup>2</sup> The approach adopted by the DPC is that reliance on this condition may only be claimed where the processing is necessary for matters of life and death

17. When processing sensitive personal data it is necessary to satisfy both a condition from Schedule 2 and at least one from Schedule 3. The Schedule 3 conditions are:

1. Processing with the explicit consent of the data subject;
2. Processing necessary for the purpose of exercising or performing a legal right or obligation in the context of employment;
3. Processing necessary to protect the vital interests of the data subject or another in cases where consent cannot be obtained;
4. Processing of political, philosophical, religious or trade union data in connection with its legitimate interests by any non profit bodies;
5. Processing of information made public as a result of steps deliberately taken by the data subject;
6. Processing necessary in connection with legal proceedings or the seeking of legal advice;
7. Processing necessary for the administration of justice, the performance of statutory functions, exercise of function of the Crown, Ministers or government departments;
8. Processing of medical data by medical professionals or others owing an obligation of confidence to the data subject; and
9. Ethnic monitoring.

18. Public authorities will normally be able to establish the legitimacy of their processing by reference to their statutory or public functions. In some cases they may need to rely upon the final condition, i.e. the pursuit of a legitimate interest not outweighed by the interests of the data subject. In addition, there are further conditions created by order of the Secretary of State that allow public authorities to process sensitive personal data for certain purposes. These fall into a number of broad categories:

- Crime prevention, policing, and regulatory functions (subject to a substantial public interest test)
- Insurance
- Equality monitoring in the area of disability and religious or other beliefs
- Research

19. Legitimate aims of public authorities are thus recognised in the grounds for fair and lawful processing, again reflecting the balance that is to be struck in protecting personal data while allowing the performance of certain functions that are necessary in a democratic society.

## **Regulation and Enforcement of the Act**

### Rights Given to Data Subjects

20. The DPA provides individuals with rights by which they can take practical steps to protect their personal data from being unlawfully or unfairly processed:

- **The right of subject access:** individuals are entitled to be informed by data controllers whether they are processing (directly or indirectly) personal data relating to them. If so, individuals have a right to be given a

description of the personal data, the purposes for which it is being processed, the source of the data and those (if any) to whom such data may be disclosed. Individuals also have the right, with some exceptions, to be given a copy of the information constituting the data held about them. A fee may be charged and the data controller should comply with the request promptly and in any case within 40 days.

- **The right to prevent processing likely to cause damage or distress:** data subjects are entitled to serve a written “data subject notice” on data controllers requiring them not to begin or to cease processing personal data relating to them, where such processing is causing or is likely to cause unwarranted substantial damage or distress to them or another. In case of dispute, upon application by the data subject, the court will consider the matter and, if satisfied, will order the data controller to take such steps as are necessary to comply with the notice.
- **The right to prevent processing for the purpose of direct marketing:** data subjects may by written notice require data controllers to refrain from processing personal data relating to them for the purpose of direct marketing.
- **Rights in relation to automated decision-taking:** data subjects are entitled to require a data controller to ensure that no decision which significantly affects them is based solely on the processing of their personal data by automatic means. Data subjects also have the right to be informed of the logic of any automated decision process taken concerning them.
- **Rights to compensation in the event an individual suffers damage as a result of processing by a data controller in contravention of the Act** where the data controller is unable to prove that it has taken such care as is reasonable in all the circumstances to comply with the relevant requirement.
- **Rights to take action to rectify, block, erase or destroy data** relating to them which is inaccurate (incorrect or misleading as to any matter of fact) or contains an expression of opinion which the court finds is based on the inaccurate data.
- **Right to request an Assessment by the Commissioner** as to whether or not personal data has been or is being processed in accordance with the Act.

### Role of the Data Protection Commissioner

21. The first duty of the Data Protection Commissioner – now the Information Commissioner (IC) - is to promote good practice. In addition, the DPC has the power to enforce compliance with the Data Protection Principles and to bring prosecutions for breaches of the criminal provisions in the Act. The Commissioner also has a duty to assess complaints from individuals.

22. The Act prohibits data controllers processing personal data unless they are notified to the DPC for the purpose of processing personal data - although there are exemptions in the Act that enable some data controllers to process data without notifying the Commissioner. In notifying they must inform the DPC of the purposes for which they hold, use and disclose personal data, details of any actual or proposed transfers of the data outside the European Economic Area and details of the security measures in place to protect the data. The DPC maintains a register of notifications.

23. In addition to maintaining this register the DPC exercises certain supervisory functions:

- **Section 42 Assessments:** As noted above, data subjects may request the DPC to carry out an assessment of whether any particular processing operation carried out by a data controller is likely to breach the provisions of the Act. The DPC is under a duty to make an assessment only when the request raises a matter of substance, so a detailed investigation of the data controller's actions may not be carried out in all cases. Where the DPC does carry out an assessment, the circumstances of the processing are considered and the data subject is informed of relevant exceptions which may justify the processing and any view formed or action taken by the DPC.
- **Information and Enforcement Notices:** data controllers are under a duty to provide information to the DPC to enable her to determine whether processing is lawful. To this end the DPC may serve an Information Notice on data controllers requiring the supply of relevant information concerning their processing actions. The DPC may also serve an Enforcement Notice. Failure to comply with an Enforcement Notice is an offence under the Act.
- The data controller has a right to appeal to the **Data Protection Tribunal** (now the Information Tribunal) concerning the service and extent of such notices. The Act also provides the DPC with limited powers of search and entry, upon application a circuit judge.

24. In practice, the application of these various measures will often be sequential; Enforcement Notices may, on appeal, be upheld, withdrawn or amended by the Tribunal.

### **Application of the Act to Data-Sharing**

25. The DPA regulates the use to which personal data is put each time it is processed. The Principles apply to all personal data processed by data controllers, unless the data controller is able to claim one of the exemptions listed in the Act. Controllers must comply with them, irrespective of whether they are required to notify and whether or not they are actually notified. Notwithstanding that personal data may legitimately have been collected and held by the data controller for a particular

processing purpose, if the data is subsequently processed in a manner which does not comply with the Data Protection Principles, that processing is prima facie unlawful.

26. Aside from general compliance with the Data Protection Principles, the Second Data Protection Principle 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”. The Third Principle requires that “Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed”. The guidance in Part II of Schedule 1 to the Act provides that:

“the purpose or purposes for which personal data are obtained may in particular be specified in a notice given for the purposes of paragraph 2 by the data controller to the data subject, or [in the data controller’s notification to the DPC].”

27. In this manner the data subject is given an effective right to know, at the time in which his/her personal data is provided to the data controller, the purposes for which that data may be processed. It is also clear that data-sharing – the disclosure of personal data to third parties by the data controller – falls within the broad definition of “processing”. Furthermore, the conditions of fair and lawful processing specified in Schedule 2 militate against data-sharing insofar as this entails dissemination of personal data for purposes beyond the immediate scope of the purpose for which it was collected.

28. Part II of Schedule 1 provides that:

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

29. The second principle must always be considered in the circumstances in which disclosure is required.

30. Unless the disclosure to third parties (data-sharing) can properly be considered to be compatible with the purpose for which the data were obtained, the Act effectively prohibits data-sharing. The Act contains limited exceptions to this rule of “non disclosure”. Section 29(3) provides that the non-disclosure rules will be disapplied where the application of the requirements of the Act would be likely to prejudice one of the matters listed below:

- the prevention or detection of crime,
- the apprehension or prosecution of offenders,
- the collection or assessment of any tax or duty.

31. Under section 35 of the Act – the so-called “gateways exemption” disclosures of personal data required by law or made in connection with

legal proceedings are similarly exempted from this non-disclosure requirement. Information disclosed for certain regulatory functions is also exempted from the non-disclosure requirement. In addition, the Secretary of State may make orders exempting from the non-disclosure provisions in the Act any disclosures of personal data made in circumstances specified in the order, "if he considers the exemption is necessary for the safeguarding of the interests of the data subject or the rights and freedoms of any other individual". These exemptions again recognise the broad balance to be struck between the protection of personal data and the necessity of certain actions in exercise of the legitimate functions of public authorities. In the absence of such a gateway, however, the disclosure of personal data by a data controller is likely to fall foul of the Act.

➤ *Case Studies*

32. To illustrate how the data protection principles should be considered before information is disclosed or transferred:-
33. Take for example, a partnership arrangement that may be aimed at addressing the problem of anti social behaviour by young people on a specific estate. It needs to be decided whose data needs to be shared, and how data sharing might help to tackle the problem, such as through referrals to provision of youth club facilities, reparation and mediation schemes, obtaining anti-social behaviour orders and referrals to youth offending teams.
34. There must be a lawful basis for processing data. It must be determined whether the type of processing to be carried out can satisfy at least one of the criteria in Schedule 2 of the first data protection principle, which requires that all processing has a legitimate basis. It must also be determined whether the processing will involve sensitive personal data, and therefore which ground in Schedule 3 will be satisfied.
35. The relevant authorities (namely chief police officers, police authorities, local authorities, probation committees or health authorities) may be able to rely on Section 115 of the Crime and Disorder Act as the grounds on which they can satisfy Schedule 2. Other authorities may be able to rely on this or they may have to look for other grounds on which to satisfy the conditions under Schedule 2. Each agency will also need to consider other legal obligations they might owe in relation to the personal data they hold, such as whether they hold it under a duty of confidence. In this case, it needs to be considered whether consent can or should be sought from an individual, and if consent cannot be obtained the authority concerned will need to consider whether there are any grounds on which the need for consent can be overridden.
36. With the young persons in this example, it may be sufficient that they are informed by the relevant authority, that this is a potential use of their

information. With other parties such as witnesses information should not normally be disclosed to other partners without their consent.

37. To satisfy the third principle partners will need to ascertain what categories of information need to be disclosed. Information must be adequate, relevant and not excessive for purpose. Information cannot be accessed or obtained by any person who is not an appropriate member of the initiative.
38. Appropriate security measures need to be taken to prevent unauthorised disclosure of or access to personal data. The means of making the referral to the initiative should ensure that the information cannot be accessed or obtained by any person who is not taking part in the initiative.
39. The data protection implications attached to the retention of data will need to be considered, including how the data collection will be notified, how data is to be recorded and how long kept, and how individuals will exercise their rights, for example by making a subject access request about their information. The partnership will need to have a mechanism by which subject access requests are considered to determine whether the source authority wishes to rely on a subject access exemption under the Data Protection Act.
40. Not all exchanges may be predictable or routine. The exemptions under Section 29 of the Data Protection Act should be used to allow the exchange of data, for example, in any case arising where the ability of law enforcers to prevent a crime or bring proceedings against an offender would otherwise be prejudiced.
41. Where non- or depersonalised data is used, for example for the mapping of incidences of particular types of offences, the provisions of the Data Protection Act should not apply providing the data does not include identifiable personal information.

## **Human Rights**

### **The European Convention on Human Rights**

42. The European Convention on Human Rights (“the Convention”) is a convention of the Council of Europe, which was adopted in 1950 and ratified by the United Kingdom in 1951. It was designed to give binding effect to the guarantee of various rights and freedoms in the United Nations Declaration on Human Rights, adopted in 1948. Article 8 of the Convention 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”.

43. The Convention thus enshrines a right to respect for individuals' private lives and prescribes the circumstances in which it is legitimate for a public authority to interfere with the enjoyment of this right. The Convention provides a qualified right - interference with the enjoyment of the right is expressly foreseen in certain circumstances. It is recognised that public authorities in pursuit of legitimate aims will have just cause in a democratic society for intervening in individuals' private spheres.

44. Since the adoption of the Convention, citizens of Council of Europe member states have had the right to present cases to the European Commission and Court of Human Rights (“commission” and “court”), established in Strasbourg. An international body of case law therefore exists which informs the extent to which the fundamental rights and freedoms enshrined in the Convention may find practical application. Applying general principles of international law, the Strasbourg court interprets the Convention in such a way as to give practical effect to its objects and purpose. Hence, in the case of Soering v UK the court noted:

“In interpreting the Convention regard must be had to its special character as a treaty for the collective enforcement of human rights and fundamental freedoms... Thus, the object and purpose of the Convention as an instrument for the protection of individual human beings require that its provisions be interpreted and applied so as to make its safeguards practical and effective.”

45. As well as interpreting the Convention in such a way as to give practical effects to its objects and purpose, the court also recognises that the Convention is “*a living instrument*” that should be interpreted in a dynamic manner. This notion means that the court is not bound by precedent and instead recognises that the conditions prevailing at the time a case is considered may properly affect the outcome of a particular decision. Hence the approach of the Strasbourg court particularly when considering cases touched on by societal mores (e.g. corporal punishment, legitimacy of offspring and the rights of transsexuals) has not remained fixed but rather has adapted to reflect prevailing conditions. With regard to Article 8 rights, developments in information and communication technologies have presented evolving challenges for judicial interpretation.

## **Restrictions of Rights**

46. Article 8(2) specifically envisages circumstances in which interference with the rights contained in Article 8(1) are permitted. However, such interference is subject to satisfaction of strict requirements to prevent abuse and compromise of personal rights. A number of principles have been adopted by the Strasbourg court when considering the extent of restrictions on the fundamental rights and freedoms set forth in the Convention.

47. **The principle of legality:** is relevant in this context since interference with the Article 8 right is expressly limited to that which is “in accordance with the law”. The Strasbourg court has elucidated three rules applicable to satisfying this principle:

- i. The legal basis for any restriction on Convention rights must be *identified* and *established*. In essence this is determined by reference to domestic law. Legislation, delegated legislation, the common law and even the rules of a professional body may suffice;
- ii. The law or rule must be *accessible* – i.e. persons likely to be affected must be able to find out what the law is that restricts their Convention right; and
- iii. The law or rule must be sufficiently certain that those likely to be affected must be able to understand its effect and thereby be able to order their conduct so as to avoid breaking the law.

48. The second key principle is **the principle of proportionality**. This principle is the mechanism by which the Strasbourg court seeks to determine whether a fair balance has been struck in the balance between the protection of the rights and freedoms of the individual and the interests of the community or society as a whole. In determining whether a restriction is *proportionate* the court will consider the following questions:

- Have “relevant and sufficient reasons” supporting the restriction been advanced;
- Is there a less restrictive alternative;
- Is the decision-making process procedurally fair;
- Are there any safeguards against abuse; and
- Does the restriction destroy the very essence of the Convention right in issue?

49. The principle of proportionality has been held by the Strasbourg court as being particularly relevant in determining whether or not a restriction under Article 8(2) is “necessary in a democratic society”. Thus the notion of *necessity* is not synonymous with “indispensability” but rather implies a “pressing social need”.

50. In determining the extent to which contracting states may be under a positive obligation to promote “respect for private... life”, the Strasbourg court has applied a wide “**margin of appreciation**”. This doctrine recognises that different contracting states have different cultural and societal standards. In view of this, the Strasbourg court considers that the

domestic authorities of those states are better placed than an international court to determine the propriety of particular measures.

## **Human Rights Act 1998**

51. The Human Rights Act 1998 (“HRA”) allows UK citizens to assert their rights under the Convention in UK courts and tribunals – although they may ultimately continue to take cases to Strasbourg. Furthermore, Section 3(1) of the HRA provides that “so far as possible to do so, primary legislation and subordinate legislation must be read and given effect in a way which is compatible with Convention rights”. Section 6 provides that “it is unlawful for a public authority to act in a way which is incompatible with a Convention right”. Accordingly, legislation is to be given effect and public authorities will be obliged to act in a way which is compatible with an individual’s right to respect for their private life. If individuals feel that public authorities have failed to do so they may challenge this through the Courts.

52. The HRA provides that “a court or tribunal in determining a decision which has arisen in connection with a Convention right must take into account the [Strasbourg jurisprudence]”.

## **Application of the HRA to data sharing by public authorities**

53. Whilst consideration should be given to the Convention as a whole, Article 8 is the most important in terms of data sharing. This article protects an individual’s right to privacy, family life, home and correspondence. Incorporated into UK law by the Human Rights Act, it has a fundamental impact on data sharing in this country.

54. In order to be compatible with Article 8 data sharing must be in accordance with the law, pursue a legitimate aim, and considered necessary in a democratic society.

55. Data sharing therefore requires a lawful basis (see the section on Administrative Law below) The exercise of any power must also be proportionate and should seek to balance the demands of the general interest of the community and the protection of the individual’s right to privacy. Data sharing will only be proportionate if:

- The objective is sufficiently important to justify infringing the right to privacy;
- The measures taken to meet the objective are rational and fair;
- The means used are no more than is necessary to accomplish the objective.

56. The proportionality requirement is of particular relevance to the issue of bulk data sharing or data matching exercises, which potentially involve “collateral intrusion” into the right of innocent people to their privacy.

57. Proportionate safeguards are contained in the principles of the Data Protection Act. These include the duty of fairness; regard to the method by which data is obtained; the principles that data is adequate for its purpose, relevant and not excessive; that it is accurate and up to date; that it is not held longer than necessary; and that it is held securely.

➤ *Case Studies*

58. One example of how human rights law affects the ability to exchange data is where this concerns information about victims. Applying Article 8, the victim will have a right to privacy, unless there is an overriding public interest in disclosing his or her information. A decision will, therefore, need to be made as to whether there is an overriding need which would justify setting aside the wishes and expectations of the victims in passing on their information. The nature and importance of the right to privacy together with the extent of the interference must be weighed against the nature and importance of the public interest the state seeks to justify.

59. The police duty of confidentiality is also a key factor in this example. A balance needs to be struck between the police's duty of confidentiality to victims, and their right to privacy, and the importance of other agencies being able to provide services to those victims. Any information subject to a duty of confidence cannot lawfully be disclosed unless it is in the public domain, the individual consents to the disclosure, there is statutory authority or some other specific overriding public interest justification requires disclosure.

60. To address human rights and common law duty of confidentiality issues, the victim must have a real opportunity to say if they do not want their details passed to say Victim Support, unless there is an overriding public interest in disclosure in a particular case.

61. Home Office guidance states that it is important that police officers should make it clear to victims that their details will normally be passed on to Victim Support unless the victim says they don't want this to happen. The opportunity for the victim to opt out of having their details referred needs to be a genuine one, and there must be mechanisms in place to ensure their wishes are respected. The arrangements for processing also need to be fully compliant with the data protection principles.

62. For more information about disclosing victims details see Home Office Circular 44/2001 or *Victims of Crime* leaflet which is given by the police to victims of reported crime.

63. Generally, there is a balance to be struck in deciding how someone's personal information is used. There might be arguments in the public interest for disclosing the information of victims or witnesses, but these

would have to be balanced against any potential resulting prejudice to the interests of the individuals concerned. Victims would normally be expected to receive greater protection over disclosure than offenders. For example, it might be agreed that information be shared between local authorities and police forces for the purpose of seeking evictions. If the numbers of call-outs to addresses are used, some of these may be because of domestic violence. If the number of call-outs is used as a ground for eviction, the spouse might be made homeless along with the alleged abusing partner. This might then prevent others suffering domestic violence from calling the police in future for fear that eviction might be a consequence. In this case, therefore, it would be important to decide whether to provide details of all call-outs, or to withhold information on those related to domestic violence.

64. It is clear that the protection of personal data is a fundamental aspect of respect for private life. The impact of human rights law can be felt in the realms of data protection and administrative law, and in common law.

## **Administrative Law**

### **An Introduction to Administrative Law**

65. Administrative Law is the law that governs the actions of public authorities. According to well-established rules of administrative law, a public authority must possess the power to carry out what it intends to do. If not, its action will be *ultra vires* - i.e. beyond its lawful powers. For public authorities considering the lawfulness of any data-sharing they propose to undertake, a key question is therefore whether they have the power or *vires* to process personal data.

66. Public bodies need to have a statutory basis for data-sharing. In addition to the necessity for a power to exist, it is also necessary that the power must be exercised for the purpose for which it was created.

67. As well as the specific powers provided to public authorities, it is clear that they may also undertake tasks “reasonably incidental” to the defined purpose.

### **Data gateways**

68. Without administrative powers, public bodies are precluded from sharing information for what they want to do. Statutory gateways can be established to permit disclosure of information as specified but actual disclosure or processing must be conducted within the framework provided by human rights and data protection law, other statutory restrictions and

the common law of confidence. The authority to carry out tasks can be provided by statute, Royal Prerogative, or in common law.

➤ *Case Studies*

69. One statutory data gateway is that provided by Section 115 of the Crime and Disorder Act 1998. The Toolkit goes into detail about how this operates. Section 115 provides the power for anyone involved in a Crime and Disorder strategy under the Act to disclose information to a relevant authority (namely the chief police officer, police authority, local authority, probation committee or health authority). This power does not override other legal obligations.
70. While Section 115 is permissive, Section 17 imposes a duty on all local and police authorities (and on joint National Parks and the Broads Authorities) to exercise their functions with regard to the effect on, and to do all that they reasonably can to prevent, crime and disorder in their area. This provision in the Crime and Disorder Act can potentially be used to direct the minds of those working in local authorities, making crime and disorder core business, encouraging greater multi-agency working, and lever agencies into action.
71. The example under Data Protection above outlines the data protection considerations to be addressed in sharing information about young people for the prevention of anti-social behaviour under a Crime and Disorder strategy. Under administrative law a public authority must have the administrative power to carry out what it intends to do. In the example, Section 115 of the Crime & Disorder Act 1998 contains the "gateway" providing the lawful basis for the exchange of information.
72. Similarly other partnerships looking at community safety issues may exchange data in order to implement local strategies for the reduction of crime and disorder. Where a clear need has been identified to implement a specific objective of a Crime and Disorder strategy, data sharing will normally be allowed, as long as there is no specific statutory or other restriction on disclosing the information. Formal agreement between the partners to the strategy is required, and data sharing protocols should be signed to make clear the responsibilities of each party to the data sharing arrangement.
73. Section 115 of the Crime and Disorder Act provides the legal power for exchange – this may involve disclosure to a relevant authority as defined by the act (see above), or disclosure to another partner regarded as acting on behalf of a relevant authority. Where it is not clear that the work of a partner is attached to a crime and disorder objective, Section 115 may not provide the necessary authority for exchange.

74. Section 115 can provide the legal authority for disclosure between the police and a local authority where in one example graffiti offenders are put onto a rehabilitation programme. The details of those who have been warned under the act and referred to a youth offending team – who will assess the offender to determine whether a rehabilitation programme aimed at preventing re-offending is appropriate - can be passed to the local authority if for participation in a programme which includes graffiti removal.
75. Questions have arisen over exchanging data in connection with social housing. A local authority is a relevant authority under the Act and there should not be any doubts about the ability to disclose data under a crime and disorder reduction initiative to the authority. Section 115 allows disclosure where it is necessary or expedient for the purposes of any provision of the act. This will include where disclosure is needed to support a Crime and Disorder Strategy.
76. The ability to disclose information to another organisation responsible for social housing stock, or to a registered social landlord, will depend on whether they are carrying out work to meet a specific objective under the local Crime and Disorder strategy. But will also depend on whether they are acting on behalf of the relevant authority (the local authority in this case) in doing so. This means in their capacity as persons selected by the relevant authority to formulate or implement the crime and disorder strategy, not simply in their capacity as private individuals or landlords.
77. A formal agreement should be in place to demonstrate that the partner requiring the information is working on behalf of the relevant authority to meet a clear crime reduction objective. This should be evidenced in an information sharing protocol, which should also set out the arrangements for the proper handling of the information. Disclosure must still comply with the principles enshrined in the Data Protection Act. The Toolkit provides advice on preparing protocols.
78. Specific gateway provisions apply in many statutory contexts.