3. The legal landscape

3.1 Sharing data across and between organisations can be a complex process. As there is no single source of law regulating the collection, use and sharing of personal information, these activities are governed by a range of express and implied statutory provisions and common-law rules. Yet despite, or more likely because of, this broad range of provisions, the legal basis setting out whether and how information can be shared in any given situation is often far from clear-cut.

3.2 For practitioners dealing with everyday questions about whether or not to share information, the picture is often confused. The absence of clear legal advice either specifically sanctioning or preventing information sharing typically results in one of two outcomes. People either make decisions based on what feels right to them as professionals, albeit with concerns that their approach may not accord exactly with the law. Or (and perhaps the greater temptation for many) they defer decisions altogether, for fear of making a mistake.

3.3 Below we set out the key components of the legal framework, which illustrates the complexity that practitioners face.

The European Directive

3.4 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (widely known as the ‘Data Protection Directive’) concerns the protection of individuals with regard to the processing and movement of personal data. It is a harmonising measure, which binds Member States who have an obligation to transpose it into domestic law. Breaches of the Directive can be challenged by the European Commission and are reviewable by the European Court of Justice.

3.5 The original objectives of the Directive focused broadly on protecting the right to privacy in the processing of personal data, while ensuring the free movement of such data within the European Union. Fuelled in part by technological, commercial and social developments since its adoption in 1995, voices in some quarters are increasingly questioning whether the Directive, and by inference the UK’s Data Protection Act, is still fit for purpose. Some are calling for the Directive to be reviewed. The UK’s Information Commissioner has recently awarded a contract to RAND Europe to conduct a review of EU data protection law. The European Commission itself is also now seeking tenders to conduct a comparative study on different approaches to new privacy challenges in the light of technological developments. The Commission’s aim is to ‘give guidance on whether the legal framework of the Directive provides appropriate protection or whether amendments should be considered in the light of best solutions identified’.

---

3.6 While evidence to this review criticised aspects of the Directive, the point was generally accepted that there is very limited scope for, or value in, a fundamental review of UK data protection law in isolation. Analysis of the Directive goes beyond our remit, but we are pleased that the recent reviews are now under way. Although neither constitutes an official EC review of the Directive, any changes to the EU Directive will eventually require changes to UK’s Data Protection Act. This may still be some years away, however, and the recommendations of this review are set in a UK context and are directed at a more immediate agenda.

3.7 However, it is extremely important that the UK Government engages actively in review and reform of the EU Directive. We therefore recommend in this report that the Government should participate actively and constructively in the current European reviews and lead Member State and wider debate about reform. This will shake off any impression that successive governments have been lukewarm about data protection. More importantly, as data flows become ever more global, the Government has the opportunity to demonstrate its leadership by bringing forward practical international approaches to data protection, rather than simply responding to the proposals of others.

The Data Protection Act

3.8 The main piece of UK legislation governing data sharing is the Data Protection Act 1998\(^{21}\) (DPA). Replacing the Data Protection Act 1984, the DPA primarily transposes EC Directive 95/46/EC into UK law and regulates the collection, use, distribution, retention and destruction of personal data. Personal data are defined in Part 1 of the Act, but they broadly mean any data relating to a living individual who can be identified from those data. The DPA is built around the Directive’s principles of good practice for the handling of personal information, some of which are particularly relevant in the context of information sharing. For example, the principles require that any processing of personal information is necessary, and that any information processed is relevant, not excessive and securely kept. Processing is a wide concept covering collection, use and sharing. The principles are intended to provide a technology-neutral framework for balancing an organisation’s need to make the best use of the personal details it holds while safeguarding that information and respecting individuals’ private lives.

3.9 The DPA also establishes various rights for individuals (inappropriately described as ‘data subjects’), notably a right of access to information about themselves. It also requires almost all data controllers to notify a general description of their data-processing activities to the Information Commissioner, the independent statutory officer responsible to Parliament for regulating the DPA. The Commissioner has various functions – discharged through his office (ICO) - aimed at promoting good practice, providing guidance, resolving complaints and enforcing the law.

The Human Rights Act

3.10 The Human Rights Act 1998\(^\text{22}\) gave full effect in UK law to the rights contained in the European Convention on Human Rights (ECHR). It is unlawful for a public body to act in a way that is incompatible with ECHR rights (section 6).

3.11 Article 8 of the ECHR is particularly important when considering data sharing and privacy matters. This provides that a person has the right to respect for his or her private and family life, home and correspondence. A public body wishing to interfere with this right will need to prove that it is acting lawfully, and that its actions are in the pursuit of a legitimate aim that is necessary in a democratic society. To satisfy human rights requirements, compliance with the DPA and the common law of confidentiality is necessary, but not always sufficient by itself.

Common law

3.12 The power to collect, use, share or otherwise process information can be derived from common law, as can restrictions on these powers, such as the common-law duty of confidentiality. A breach of confidence can occur when information that one might expect to be confidential is communicated in circumstances entailing an obligation of confidence, but later used in an unauthorised way. Contractual agreements can also provide the basis for collecting, using and sharing personal information, and organisations and individual practitioners should also take into account any relevant professional guidance or industry code.

3.13 Government departments headed by a Minister of the Crown may be able to rely on common-law powers to share data where there is no express or implied statutory power to do so. The general position is that the Crown has ordinary common-law powers to do whatever a natural person may do (unless this power has been taken away by statute).

3.14 In addition to common-law powers, the Crown also has prerogative powers. Although there is no single accepted definition of the prerogative, these powers are often seen as the residual powers of the Crown, allowing the executive to exercise the historic powers of the Crown that are not specifically covered by statute. Residual powers may relate to foreign affairs, defence and mercy, for example. However, Parliament can override and replace prerogative powers with statutory provisions.

3.15 Public bodies which are established by statute (e.g. local authorities and HMRC) have only such powers as are conferred upon them by statute. This means that those bodies have no powers under the common law or the Crown prerogative and must rely solely on their express or implied statutory powers.

\(^{22}\) http://www.opsi.gov.uk/acts/acts1998/ukpga_19980042_en_1
Administrative law

3.16 Administrative - or public - law is the body of law governing the activities of government and other public bodies. Before a public body can engage in data sharing, it must first establish whether it has a legal power to share the data in question. Where a public body acts outside its powers, the activities can be challenged before the courts by way of a judicial review.

3.17 The nature of the public body and the rules governing its activities play a crucial part in determining the legal basis upon which it acts and whether its activities are lawful. If a public body does not have the power to collect, use, share or otherwise process data, it will be acting unlawfully; and the fact that an individual may have consented will not make the activity lawful.

Statutory powers

3.18 Non-ministerial departments or those created by statute cannot have prerogative or common law powers. Any data sharing by them must be based on statutory powers (express or implied), while statutory powers can also impose obligations on non-public bodies to share or disclose information. For example, section 52 of the Drug Trafficking Act 1994 makes it an offence to fail to report suspicion of drug money-laundering activities, thereby placing a statutory duty on people and organisations to share relevant personal information with the police.

Express statutory powers

3.19 Express statutory powers can be enacted to allow the disclosure of data for particular purposes. Such powers may be permissive or mandatory. A permissive statutory power describes legislation that gives an organisation the power to share data, for example, Section 115 of the Crime and Disorder Act 1998. A mandatory statutory power requires an organisation to share data when requested. An example of this is Section 17 of the Criminal Appeals Act 1995.

Implied statutory powers

3.20 Even where there is no express statutory power to share data, it may still be possible to imply such a power. To this end, where the actions or decisions of a public body are incidental to meeting the requirements of an expressed power or obligation, they can be considered to have an implied right or power to act.

3.21 Statutory bodies carry out many activities on the basis of implied statutory powers. This is particularly true of activities such as data collection and sharing, which are not always express statutory functions.

3.22 In order to imply a power to share data, the body in question must first of all be satisfied that it has the legal authority to carry out the core function to
which the sharing of data applies. Without the power to undertake the activity, there can be no implicit power to share data.

3.23 A public body sharing data under an implied power must also take account of any relevant conflicting statutory provisions that may prohibit the proposed sharing (either expressly or implicitly). Similar considerations should also apply to the collection of data. A body should consider whether collecting the data is reasonably incidental to existing statutory powers: i.e. whether it is fair to accept that this activity is reasonably associated with their existing powers.

Statutory bars

3.24 Legislation may also prohibit the disclosure of information or restrict disclosure to limited and defined circumstances. Section 18 of the Commissioners for Revenue and Customs Act 2005, for example, created a strict statutory duty for HMRC officials to maintain taxpayer confidentiality; and section 19 made any contravention of these provisions by such officials a criminal offence.