An overview of UK data protection law
Contents

Introduction........................................................................................................................................... 01
Scope of the Act ...................................................................................................................................... 02
Notification ........................................................................................................................................... 02
The data protection principles ........................................................................................................... 02
Rights of data subjects .................................................................................................................... 03
Transfers of personal data outside the European Economic Area ................................................. 03
Why comply? ....................................................................................................................................... 04
Exemptions .......................................................................................................................................... 04
Achieving and maintaining compliance ......................................................................................... 05
Other relevant law ............................................................................................................................. 06
The Privacy and Electronic Communications (EC Directive) Amendment Regulations 2011 .................................................. 06
Summary of the data protection principles ...................................................................................... 07
Introduction

The use by businesses of information about individuals is subject to a complex array of data protection laws. This note provides a summary of the principal law regulating the use of personal information, the Data Protection Act 1998, in addition to including a brief overview of some of the other related UK laws a business will need to consider in order to avoid issues of legal liability, restrictions on the handling of data or damage to brand and reputation.

Essentially, the Data Protection Act 1998:

- sets out the rules and practices which must be followed when processing information about individuals;
- grants rights to those individuals in respect of their information; and
- creates an independent supervisory body to enforce these rules, rights and practices.

Background – European law

In 1995, the European Commission adopted the Data Protection Directive which aimed to harmonise data protection legislation throughout the European Union. Each member state was required to implement the Directive by 24 October 1998.

The Data Protection Act 1998 (referred to in the rest of this note simply as the “Act”) is the UK’s implementing legislation. It provides the framework for the UK’s data protection regime, with detail being filled in by means of specific items of legislation known as “statutory instruments” or “regulations.”

---

1 Member States have adopted the Directive in slightly different ways, so there are still some differences in national data protection law between them.
Scope of the Act

Key terminology

The Act regulates the processing of personal data. Personal data are data relating to living individuals (referred to in the Act as “data subjects”) who can be identified from those data, or from those data together with other information which is in, or is likely to come into, the possession of the entity who decides what the data will be used for (the “data controller” – see later). Personal data also include opinions and indications of intentions about the data subject.

The Act applies to:

- information that is processed automatically (i.e., computer-based records);
- information recorded on paper (but only if there is some structure to the paper records so that you can find specific information about an individual, for example, an indexed ring-binder of records);
- health records and certain public authority records.

The term “processing” has a very wide meaning under the Act. It is intended to cover any conceivable operation on data, ranging from collecting, recording, holding of them and the carrying out of any operation on those data, through to their subsequent disclosure and eventual destruction.

Data controllers and data processors

“Data controllers” are the entities (companies, firms, sole traders etc.) who, either independently, or jointly with others, decide how personal data will be used and what they are to be used for. “Data processors” are the entities who process personal data on behalf of data controllers. For example, if a business uses a payroll bureau to process its payslips and payments to staff, then that payroll bureau is acting as a data processor.

The Act only places obligations on data controllers, not on processors. However, if a controller uses the services of a processor, it must have a written agreement in place with the processor in which the processor is obliged to:

- do only what the controller instructs it to do with the personal data; and
- maintain appropriate security measures in place with respect to the personal data.

Notification

Generally speaking (there are some exemptions), before processing any personal data, it is necessary for data controllers to first notify the UK’s Information Commissioner of the intended processing activities.

Under the Act, notification must take place annually. A notification involves providing certain information to the Information Commissioner including the data controller’s name and address, a description of the personal data being processed, the purposes for which those data are processed and any recipients of the personal data, and a description of any intended destination countries. The details of the notification will then appear on a publicly accessible register.

The data protection principles

The Act is based on eight Data Protection Principles. The first Principle is particularly important; it requires that personal data are processed, i.e., obtained and subsequently used, “fairly and lawfully”. There are two aspects to this:

- making sure that the processing is legitimate by satisfying one or more specified preconditions; and
- providing individuals with certain information when collecting data from them (or, if data is not collected directly from them, then before undertaking any processing of their data).
Key preconditions include where the data subject has consented to the processing, where the processing is necessary for the performance of a contract and where the processing is necessary for the “legitimate interests” of the data controller (provided that those interests do not prejudice data subjects’ rights). If “sensitive personal data” (which is a special category of personal data including information about race, health, religion, politics, union membership or criminal offences) are being processed, then one or more further preconditions must be met.

As noted above, in addition to meeting one or more processing preconditions before personal data may be processed, data subjects must be provided with certain specified information either at the time the data are gathered, when the data is first processed, or as soon as possible afterwards. The specified information includes:

- the identity of the data controller(s) for the data;
- the intended uses for the data; and
- any other information which is necessary to enable the processing to be fair (for example, informing someone of their right to object to direct marketing).

The eight Data Protection Principles are summarised on page seven of this note. They must be observed, not only at collection, but throughout the subsequent processing of personal data.

Rights of data subjects

The Act confers a number of rights on individuals in respect of their personal data. For example, individuals:

- may make requests to those who process personal data about them (known as “subject access requests”) for information as to what data are stored, what it is used for, the recipients to whom it is or may be disclosed and the source of the personal data;
- have rights to prevent processing likely to cause substantial damage or substantial distress to them or to another;
- have the right to object to direct marketing;
- have the right to veto automated decisions which significantly affect them;
- may take action to get their personal data corrected or erased; and
- are entitled to compensation from data controllers for breaches of the Act.

Transfers of personal data outside the European Economic Area2 (“EEA”)  

Under the Act, transfers of personal data to countries outside the EEA are prohibited unless either:

- the destination country in question ensures an “adequate” level of data protection for individuals; or
- one or more preconditions which allow the transfer to take place applies.

In determining what makes a destination country adequate, it is possible to either rely on a published European Commission decision, or to make an assessment of adequacy based on a number of factors such as the nature of the data being transferred and the purposes for which they are being transferred, the law in the country in question and any security measures being taken. Very few countries outside of the EEA are deemed by the Commission to have adequate protection3. The United States has put in place an agreement with the Commission known as “safe harbour”, whereby US businesses who sign up to a set of privacy principles (similar to the Data Protection Principles under the Act) may be considered as offering adequate protection.

---

2 The EEA is composed of the 27 EU Member States together with Norway, Liechtenstein and Iceland
3 As at the date of this note, current decisions apply to Switzerland, Canada, Argentina, Guernsey, Jersey, Isle of Man, the Faroe Islands, Andorra and Israel each of which have been determined to be adequate. Certain conditions apply to the decision regarding Canada
If the destination country outside the EEA does not have adequate data protection laws in place, then the transfer will only be permitted where one or more specified preconditions (which are additional preconditions to the ones for general processing described above) can be met, such as where the data subject has consented, the transfer is necessary for the performance of a contract with the data subject or the rights of the data subject are protected by a contract based on the European-approved terms in place between the sender and the recipient of the data.

If a destination country has not been found to be adequate by the Commission (or, if the business receiving the data is in the US and it has not signed up to the safe harbour scheme,) then it is advisable to make sure the transfer meets one of the transfer preconditions, rather than to rely on a self-assessment of adequacy.

The restrictions on transfers also apply to transfers within a group of companies.

A further option for large multi-national groups is to put in place group-wide data handling policies (Binding Corporate Rules) and to have such policies recognised by national data protection regulators.

Obtaining approval for a set of Binding Corporate Rules is a potentially lengthy and costly process but it is seen as an alternative approach for multinationals with very complicated data transfer arrangements.

**Why comply?**

Many breaches of the Data Protection Act 1998 are criminal offences. Further, the directors or other officers of a company in breach may also be personally liable.

There are also other consequences. The level of awareness of individuals in the UK with respect to their data protection rights has increased over the last few years, and people will more readily complain to the Information Commissioner where an organisation is not complying with data protection legislation. The administrative costs of dealing with complaints and, ultimately, investigations by the Information Commissioner can be very high and the Information Commissioner will publicise complaints which are upheld or successful prosecutions.

To force compliance, the Information Commissioner may impose a fine of up to £500,000 on organisations that deliberately or recklessly commit serious breaches of the Act. The Information Commissioner may also serve enforcement, and information notices, the latter requiring a controller to provide information to assist the Commissioner in determining whether the data protection principles have been broken or he may, in the case of public bodies, demand to audit their compliance. Going even further, the Commissioner may in certain circumstances apply to the court for an entry and inspection warrant.

**Exemptions**

The Act contains a number of exemptions from some or all of the data protection principles and the other provisions such as:

- for processing concerning the detection of crime or the assessment of taxation;
- where information must be made public by law;
- where the disclosure is made in connection with legal proceedings, or pursuant to a court order;
- for the purposes of research, history and statistics; and
- for processing for purely domestic purposes.
There are also exemptions from the obligation to provide information in response to a subject information request (see above) in respect of (for example) confidential employment references, management forecasts, intentions with respect to negotiations, examination marks and scripts and legally privileged material.

Achieving and maintaining compliance

Being compliant means having an accurate notification in place and internal procedures to ensure that in practice the organisation processes personal data in accordance with its notification and with applicable data protection law.

General guidelines

Data controllers should audit (and revise where appropriate) their data processing activities on a regular basis. In particular:

- the data protection notification of each group company (if applicable) must reflect the data processing activities in practice from time to time;
- relevant staff should be trained to understand the impact of the Act on their particular area. For example, there are implications for human resources records and for the technical capabilities of the computer systems which are used to process personal data;
- suitable written contracts must be in place with third parties for whom personal data is processed, or to whom the processing of personal data is outsourced;
- measures must be taken to keep personal data secure at all times. In particular, staff should understand the importance of never transmitting personal data or carrying personal data on a portable device (such as a laptop or blackberry) which is not protected by passwords and/or strong encryption;
- the terms under which intra-group transfers of personal data are made need to be assessed;
- all transfers of personal data across borders must be examined, in particular those to outside of the European Economic Area; and
- internal procedures need to ensure continuing compliance with the above and the effective handling of enquiries and complaints by individuals.

Appointment of a data protection officer

Once established in the UK, although there is no current legal requirement under the Act, it is advisable to appoint a data protection officer to assist with compliance.

The primary duties of such an officer should be to:

- Keep the notification(s) up to date, including:
  - keeping track of the legal entities which carry out processing; and
  - keeping track of new data processing purposes.
- Assist with compliance issues, including:
  - dealing with subject information requests from the public; and
  - liaising with external advisers and the Office of the Information Commissioner.
- Liaise with the human resources department (if the officer is not a member of the HR department) to ensure that correct procedures are followed when employees join and leave, and when employees make subject information requests.
- Assist in training/awareness of staff.
Other relevant law

The Data Protection Act 1998 is just one UK statute which regulates the use of personal data. Recent years have seen a number of very significant items of legislation in this area. These laws have implications beyond the field of data protection but their implications relevant to data protection are summarised below.

**The Privacy and Electronic Communications (“EC Directive”) Regulations 2003**

These regulations contain provisions that govern (among other things) direct marketing by email and/or when using Short Message Services (“SMS” or “text messages”). The position set out in the regulations is that unsolicited direct marketing by electronic means (interpreted as covering both email and SMS) is subject to a requirement that the recipient has previously notified the sender that they consent to the email or SMS being sent (and that certain information about the sender—whose identity must be clear—has been provided to the recipient).

However, the need for prior consent will not apply where the individual’s details have been obtained by the business in the course of a sale or negotiations regarding a potential sale. In this case, it is permitted for the same business to send SMS or email communications to such a person provided that the marketing is in respect of its own similar products or services only and the recipient has been given a simple means of refusing the use of his details for marketing at the time those details were initially collected and with each subsequent email communication.

**The Privacy and Electronic Communications (EC Directive) Amendment Regulations 2011**

New law implementing a revised EU directive came into force from 26 May 2011 which obliges organisations using cookies (which includes equivalent technologies) only to place cookies on the machines of users who have given their consent. The only general exemption to this requirement is where the placing of the cookie is “strictly necessary” to provide a service requested by the subscriber or user. This exception is limited in scope but would cover situations, such as where a cookie is needed to underpin the operation of a shopping basket of goods selected by a user and may also apply to specific security cookies.

Businesses with a website, (or one which actively targets UK users) and which places cookies on users machines, need to identify the different cookies that are served, assess how intrusive these are and implement changes to get the consent of the user ahead of the cookie being served. Businesses must also provide clear information about how cookies are used throughout their website(s).

**Human Rights Act 1998 (“HRA”)**

The HRA states, among other things, that individuals have a right to respect for their private and family life, their home and their correspondence. Although the HRA is not directly enforceable against private organisations, the Act does require a court or tribunal to interpret any UK legislation in a way that is compatible with the rights set out in the HRA. This means that, where appropriate, courts and tribunals must consider individuals’ privacy rights.


RIPA regulates, among other matters, the interception of communications on a public or a private network. Monitoring is allowed only if the controller has obtained a warrant from a designated official, if both parties to the call/email consent or if the purpose of the monitoring falls within the Lawful Business Practice Regulations 2000. These set out the circumstances when monitoring or keeping a record of communications is lawful, for example in order to:

a) ascertain compliance with regulatory or self-regulatory practices or procedures which are acceptable to an employer in carrying on its business;

b) ascertain or demonstrate the standards which are achieved or ought to be achieved by persons using the system in the course of their duties; or

c) investigate or detect unauthorised use of the employer’s systems.
It is also permissible to monitor (but not to keep a record of) communications if the monitoring is to determine whether a communication is a business communication. However, these exceptions only apply to the extent that all reasonable efforts have been taken to inform staff that monitoring takes place.

**The Freedom of Information Act 2000 ("FOI Act")**

The FOI Act provides for general rights of access to “recorded” information held by public authorities (such as Government departments, local authorities, the NHS and educational bodies).

On receiving a request for information, the public authority is obliged to confirm within 20 working days whether it holds the information requested and if it does, to provide it.

Where the information requested is personal information, the requirements of the Data Protection Act 1998 must also be considered and, in particular, whether the disclosure of the requested information would infringe the Data Protection Act.

Organisations can also use the FOI Act to obtain information (such as information held about competitors). Businesses therefore need to consider carefully what information they supply to a public authority and whether this can be protected from disclosure in the event of an FOI Act request being made.

**Summary of the data protection principles**

- Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
  - at least one of a specified list of pre-conditions is met (for example, the data subject has given his consent or the processing is necessary for the performance of a contract to which the data subject is a party), and
  - in the case of sensitive personal data, at least one of an additional set of pre-conditions is also met (for example, the data subject has given his explicit consent or the processing is necessary for performing a legal obligation with respect to employment).
- 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.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under the Act.
- 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.
- 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.

This note provides general guidance only. If you have any specific queries with respect to data protection law issues, please raise them with us.
About Us

Taylor Wessing is a leading International law firm with a single-minded approach: to help our clients succeed.

What makes us different is our forward thinking approach to serving clients. We think creatively about business issues and are constantly looking for new and better ways to add value with truly innovative solutions that help to grow our clients’ businesses.

By keeping close to our clients we can proactively identify better ways to help them achieve their ambitions.

Today’s world is undergoing fundamental change and that creates the need for intelligent solutions.

Our aim is to be at the forefront of developing those solutions by serving clients in the sectors that we believe are the industries of tomorrow:

- Technology, Communications and Brands;
- Life Sciences and Healthcare;
- Real Estate and Infrastructure;
- Energy and Environment;
- Financial Institutions and Services.

With over 750 lawyers in the UK, Germany, France and Belgium, we are able to provide unrivalled support for commercial organisations doing business in Europe across a full range of legal practice areas. We are also strong in the Middle East, India, China and North America. We are driven by where the industries of tomorrow are growing the fastest.