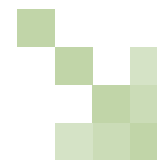


# UK (England and Wales)



Calum Murray and Chris Hawkins, Kemp Little LLP

[www.practicallaw.com/1-239-2996](http://www.practicallaw.com/1-239-2996)

## REGULATION

### 1. What national law(s) apply to the collection and use of personal data? If applicable, has Directive 95/46/EC on data protection (Data Protection Directive) been implemented?

The Data Protection Directive was implemented in the UK on 1 March 2000 through the Data Protection Act 1998 (DPA). The DPA is the primary legislation regulating the collection and use of personal data in the UK. Subsequent secondary legislation has been introduced to address specific issues involving personal data, such as the Privacy and Electronic Communications (EC Directive) Regulations 2003 (regarding the use of personal data for the purposes of unsolicited direct marketing and individual's rights in those circumstances).

In the UK, data protection, the DPA and related legislation and the protection of personal information is the responsibility of the Information Commissioner's Office (ICO) (*see box, The regulatory authority*). The ICO is an independent public body lead by the Information Commissioner, currently Richard Thomas.

The fundamental aims of the DPA are to give individuals rights over their personal information and to require anyone who handles personal information to comply with key principles when doing so. The DPA creates a framework within which all "processing" of "personal data" must be carried out. The scope of these terms is sufficiently wide that any UK entity obtaining personal information is likely to have to operate within the DPA framework.

### 2. To whom do the rules apply (EU: data controller)?

The DPA applies to "data controllers". Section 1 of the DPA defines a data controller as the person who either alone, jointly, or in common with other persons, determines the purposes for which and the manner in which any personal data are, or are to be, processed. In effect, the data controller is the party which decides what to do with personal data and how that activity is to be carried out. These decisions can be made with or at the same time as another data controller.

Where data controllers act together equally to determine the purpose and manner of any processing of personal data, each data controller acts as a joint data controller. Joint data controllers aim to achieve the same data processing outcome.

The status of common data controllers arises when two or more parties process the same collection of personal data, even though

for different reasons. Common data controllers aim to achieve varied data processing outcomes with the same personal data.

The role of data controller can be chosen or imposed by legislation. If personal data is processed only for purposes for which it is required by any enactment to be processed, the data controller is the person obliged to process the data by that enactment (*section 1(4), DPA*).

Data controllers do not need to hold the data or process it. It is sufficient to instruct a third party how to process the personal data to be deemed a data controller (*see Question 15*). This is more and more common as outsourced business models continue to spread.

### 3. What data is regulated (EU: personal data)?

The DPA identifies "data" as information which:

- Is processed automatically by equipment.
- Is recorded for the purpose of automatic equipment processing.
- Forms part of a relevant filing system.
- Does not fall into the first three bullets but amounts to an accessible record.

Such data is "personal data" and its use regulated by the DPA if both:

- It is data relating to a living individual.
- That individual can be identified:
  - from that data; or
  - from that data and other information which is in, or is likely to come into, the possession of the data controller.

Personal data can include:

- Names and dates of birth.
- Contact details such as addresses, e-mail addresses and telephone numbers.
- Expressions of opinions on living individuals.
- Indications of the intentions in respect of living individuals.

However, such information is only personal data if an individual can be identified from it directly, or using it in conjunction with other data.

The DPA does not address personal information about deceased people, although this may be protected as confidential at common law. Also, as its name suggests, the holding of “anonymous” data (such as retail transaction patterns for differing age groups) is not regulated by the DPA if the holder of the data cannot identify living individuals from such data. Further, to be personal data, information does not have to have a confidential nature.

In the ICO’s published views, whether or not data relates to a particular individual is a question of fact in each particular case. In *Michael John Durant v Financial Services Authority [2003] EWCA Civ 1746*, the Court of Appeal considered the degree of relationship required between the individual and the data. The Court held that information relates to an individual if it affects their privacy. In assessing the affect on privacy, the Court suggested that key considerations are whether the information:

- Is biographical.
- Has the individual as its focus.

Simply referring to a person’s name, where the name is not associated with any other personal information, is not usually personal data. This narrow approach may be more restrictive in practice than the definition of personal data in other EU member states.

#### 4. What acts are regulated (EU: processing)?

“Processing” of personal data is regulated under the DPA. This covers obtaining, recording, holding, organising, retrieving, disclosing in any way, aligning, destroying or deleting personal information.

A “catch-all” ending to the DPA definition of processing includes “carrying out any operation” on personal data as processing. This makes the combination of personal data and any activity with that data very likely to be regulated as processing.

#### 5. What is the jurisdictional scope of the rules?

The DPA applies to the following when they are “established” in the UK and if they process data as data controllers in the context of that establishment (*section 5, DPA*):

- Individuals ordinarily resident in the UK.
- Companies registered in the UK.
- Partnerships or other unincorporated associations formed in the UK.
- Persons with an office, branch or agency in the UK.

Data controllers established outside the European Economic Area (EEA) who process data using equipment in the UK are also subject to the DPA.

#### 6. What are the main exemptions (if any)?

The main exemptions to the DPA’s requirements are based on public policy considerations, where the public interest is deemed to require disclosure of personal data that would otherwise be in breach of the DPA. This includes disclosures for:

- The purposes of national security (*section 28, DPA*).
- The prevention or detection of crime and the apprehension or prosecution of offenders (*section 29, DPA*).
- The assessment or collection of any tax or duty or of any imposition of a similar nature (*section 29, DPA*).
- Health, education, social work and regulatory purposes (*sections 30 and 31, DPA*).
- Compliance with legislation or otherwise required by law (*sections 34 and 35, DPA*).

Processing personal data can also be exempt from most of the DPA (including the rights of data subjects), for artistic, literary or journalistic purposes. Again, the justification for such processing is founded on the public interest (*section 32, DPA*). In addition, the processing of personal data by individuals for their domestic purposes is specifically exempted (*section 36, DPA*).

Further specific exemptions from the DPA permitting data subjects’ access to their personal data (*see Question 13*) for disclosures include (*Schedule 7, DPA*):

- Confidential references given by the data controller.
- Information prejudicial to the combat effectiveness of the armed forces.
- Information relating to crown employment and crown, ministerial or judicial appointments and honours.
- Management forecasts, corporate finance and negotiations.
- Examination marks and examination scripts.
- Legal professional privilege.

#### 7. Is notification or registration required before processing data? If so, please provide brief details.

A prospective data controller must notify the ICO of its intention to process personal data before starting the processing (*section 18, DPA*).

The ICO uses notified details to make an entry describing the processing in the register of data controllers. This register is available to the public for inspection. Failure to notify is a criminal offence and it does not release a data controller from the ongoing obligation to comply with all other requirements of the DPA.

Notification can be done:

- Online, at the ICO’s website: <http://www.ico.gov.uk>.

- By telephone, on the notification helpline (+44 1625 545740).
- By completing a notification form in hard copy.

Every initial notification must be accompanied by a fee of GB£35 (about US\$69) and the period of notification lasts one year, after which an annual continuation fee of GB£35 must be paid.

Exceptions to the notification requirements exist for processing where the purpose is:

- The maintenance of a public register (*section 17(4), DPA*).
- Staff administration, advertising, marketing and public relations, accounts and record keeping.
- Operations carried out by non-profit making organisations.

Data controllers relying on an exception from the obligations to notify are still obliged to otherwise comply with the DPA at all times.

## MAIN DATA PROTECTION RULES AND PRINCIPLES

### 8. What are the main obligations imposed on data controllers to ensure that data is processed properly?

The main obligations imposed on data controllers by the DPA are set out in the eight data protection principles (Principles) (*Part I, Schedule 1, DPA*). Guidance on certain of the Principles is also provided in the DPA (*Part II, Schedule 1, DPA*).

Unless expressly exempt, the Principles apply to all personal data processing and require that personal data must:

- Be processed fairly and lawfully.
- Be obtained only for specified, lawful purposes and not be further processed in a manner incompatible with those purposes; data controllers cannot collect data without first deciding what they are going to do with it.
- Be adequate, relevant and not excessive to the purposes for which it is processed; data controllers cannot process vast sets of personal data if they do not need that data for their defined purposes.
- Be accurate and, where necessary, kept up to date; if recurrent processing is envisaged, data controllers require regular database overhauls.
- Not be kept for longer than is necessary for the purposes for which it is processed; data controllers must focus on what they have collected personal data for and if that task is completed, the data must be erased.
- Be processed in accordance with the rights of data subjects under the DPA (*see Questions 12 and 13*), other than as accepted individuals continue to have their rights in personal data.

- Be protected, through appropriate technical and organisational measures, from unlawful processing, accidental loss, destruction or damage. What is appropriate will depend on the nature of the personal data and the context of its processing.
- Not be transferred outside the EEA to any place that does not ensure an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. (*see Questions 16 to 19*).

While all the Principles must be complied with when processing personal data, the first Principle, that processing be fair and lawful, underpins the other Principles.

For processing of personal data to be fair, one of the fair processing conditions of Schedule 2 of the DPA must be satisfied (*see Question 10*). Where sensitive personal data is processed, there is an additional requirement that one of the conditions of Schedule 3 of the DPA be met (*see Question 11*).

In addition the first Principle requires that certain information is given to individuals before their data is processed (*see Question 12*). If the individual is deceived or misled about the purpose for which the personal data is to be processed, the processing is not fair.

In published guidance, the ICO says it is of primary importance to consider the consequences of the processing to the individual, then the purposes and nature of the processing when assessing fairness.

What constitutes lawful processing is not clarified in the DPA and so a general interpretation at law must be applied. This results in the data controller having to comply with all relevant rules of law when processing personal data, including all statute or common law rules, whether criminal or civil.

### 9. Is the consent of data subjects required before processing personal data? If so:

- What rules are there regarding the form and content of consent? Would online consent suffice?
- Are there any special rules regarding the giving of consent by minors?

If all other obligations are complied with, obtaining consent from data subjects before processing their personal data makes such processing fair and lawful. However, consent is not required, as there are other bases which justify processing an individual's personal data (*see Question 10*).

#### Form and content of consent

"Consent" is not defined in the DPA and so must be assessed from the facts. The Data Protection Directive, however, defines consent as an individual's freely given, specific and informed indication signifying agreement to the processing of their personal data.

Signifying agreement requires consent to be an active communication, but this need not be in writing. A common means of signifying consent is to set out the processing which will be undertaken and asking individuals to tick to signify their agreement to it. Consent cannot be obtained through acquiescence on the

individual's part nor can it be obtained under duress or by misleading the individual.

Consent provided online is sufficient for DPA purposes if the individual receives all necessary information about the proposed processing, and signifies consent to this processing as personal data is submitted. This consent is commonly captured by ticking an electronic box or clicking an "I agree" or similar icon.

### Consent by minors

Consent from minors is not covered in the DPA as a special category. The ICO recommended in a recent Issues Paper that it is good practice for parents to be consulted about important decisions affecting their children. However, the ICO also emphasises that the DPA confers rights on the individual, including minors. These rights should only be exercised by another on a minor's behalf if the minor is not capable of exercising them independently.

Against a backdrop of continued development of English case law regarding the independence of minors, the ICO is proposing to issue further guidance in the context of minors' data protection rights and obligations. The ICO is also preparing a framework code of practice to assist public sector organisations in setting up information sharing schemes regarding minors.

### 10. If there is no consent, on what other grounds (if any) can processing be justified?

In the absence of consent, personal data is processed fairly, as required by the first Principle (see *Question 8*), if the processing is necessary (*Schedule 2, DPA*):

- To perform a contract with the individual, or to comply with a request by the individual to contract.
- To comply with any non-contractual legal obligation of the data controller (for example, video surveillance in certain circumstances).
- To protect the life of the individual.
- For the administration of justice, to comply with a statute or for exercising functions of a public nature.
- For the legitimate interests of the data controller or a third party to whom the data is disclosed, except where it is unwarranted because it is prejudicial to the individual.

Additional criteria apply in relation to sensitive personal data (see *Question 11*).

### 11. Do special rules apply in the case of certain types of personal data, for example sensitive data? If so, please provide brief details.

Sensitive personal data include data relating to:

- Race or ethnic origin.
- Political opinions.

- Religious and other beliefs.
- Trade union membership.
- Health.
- Sex life.
- Criminal records.

Sensitive personal data is only processed fairly and lawfully, under the first Principle (see *Question 8*) if, in addition to one of the fair processing conditions in Schedule 2 of the DPA (see *Question 10*), at least one of the following conditions is also satisfied (*Schedule 3, DPA*):

- The individual gives explicit consent to the processing. This should be clear and should be consent to:
  - the detail of the processing;
  - the type of data to be processed;
  - the purposes of the processing; and
  - any special aspects of the processing, such as disclosures of the data.
- The processing is necessary to perform the data controller's employment law obligations.
- The processing is necessary to protect the life of the individual where consent cannot be given or cannot reasonably be obtained (or of a third party where the individual who the data relates to unreasonably withholds consent).
- The processing is carried out by certain non-profit organisations.
- The individual has made the data public.
- The processing is necessary for the purpose of legal proceedings, obtaining legal advice, establishing or defending legal rights, the administration of justice or exercising functions of a public nature.
- The processing is carried out by a health professional and is necessary for medical purposes.
- The data relates to racial or ethnic origin and is processed in the context of equal opportunity monitoring.

## RIGHTS OF INDIVIDUALS

### 12. What information should be provided to data subjects at the point of collection of the personal data?

The data controller must ensure that the individual is provided with:

- The name of the data controller (or its representative).
- The purposes for which the data is intended to be processed.

- Any other information necessary to ensure processing is fair (such as recipients of the data).

---

### 13. What other specific rights (such as a right of access to personal data or the right to object to processing) are granted to data subjects?

---

#### Rights of access

An individual can request information from a data controller. If the data controller is processing that individual's personal data, it must:

- Inform the individual.
- Describe the personal data.
- Give the purposes of the processing.
- Identify recipients of the data.
- Provide such data in permanent form.

Where a decision is made by fully automated means, the individual is entitled to be informed about the logic involved in the process.

#### Right to prevent processing

If an individual believes that a data controller processing their personal data is causing, or is likely to cause, substantial unnecessary damage or distress, the individual can send a notice to the data controller requiring that it stop the processing, within a reasonable time. This right does not apply where any of the conditions in paragraphs 1 to 4 of Schedule 2 of the DPA are met (see *Question 10*).

An individual can also, by written notice, require a data controller to cease, or not to begin, processing his personal data for direct marketing. In addition, the Privacy and Electronic Communications (EC Directive) Regulations 2003 generally require opt-in consent from individuals to receive direct marketing.

An individual can, by written notice, require that a data controller ensures that no decision significantly affecting him (such as work performance, creditworthiness, reliability or conduct) is based solely on processing his personal data by automatic means. This right does not apply where the decision is made in relation to the entry into, or performance of, a contract with the individual and either the effect of the decision is to grant a request of the individual (such as a loan application) or steps have been taken to safeguard the legitimate interests of the data subject (for example, allowing the individual to make representations).

#### Inaccurate data

An individual can apply for a court order requiring a data controller to rectify, block, erase or destroy inaccurate data relating to that individual (including an expression of opinion based on inaccurate data).

## SECURITY REQUIREMENTS

---

### 14. What security requirements are imposed in relation to personal data?

---

Data controllers must take appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing, damage or accidental loss or destruction. The DPA and the ICO do not provide details of what measures are appropriate, although BS7799, the British Standard for Information Security Management, is used as a reference point.

The ICO's view is that what is appropriate depends on the circumstances, particularly the harm that may result from the security breach, which in itself may depend on the nature of the data. The data controller needs to adopt a risk-based approach, taking into account the state of technological development at any time and the associated costs. Management and organisational measures are as important as technical ones.

In addition, the data controller must take reasonable steps to ensure the reliability of any employees who have access to personal data.

## PROCESSING BY THIRD PARTIES

---

### 15. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

---

The processing must be carried out under a written contract requiring the data processor to act only on the data controller's instructions and to comply with the security requirements under the seventh Principle (see *Question 8*). As processing is widely defined, it is easy for an organisation to fall within the category of a data processor. This requirement also applies to a data processor irrespective of the fact that it and the data controller are part of the same corporate group structure.

## INTERNATIONAL TRANSFER OF DATA

---

### 16. What rules govern the transfer of data outside your jurisdiction?

---

The DPA prohibits the transfer of personal data outside the EEA, unless the destination country ensures an adequate level of protection of the rights of the individual in relation to data processing. There are no special restrictions on the transfer of data within the EEA.

A transfer of data takes place only where some type of processing occurs. Simply passing through a country, for example, through a communications network, does not amount to a transfer.

The European Commission has made findings that the following countries offer an adequate level of protection:

- Argentina.
- Canada (subject to certain conditions).

- Guernsey.
- Isle of Man.
- Switzerland.
- US (where the US recipient is a signatory to the EU-US Safe Harbor Agreement 2000).

In other cases, the data controller must determine whether a country provides an adequate level of protection, taking into account Schedule 1, Part II, paragraph 12 of the DPA, which sets out that if the processing of personal data is done by a data processor on the data controller's behalf, it will not comply with the seventh Principle (requiring appropriate technical and organisational security (see *Question 8*)) unless it is done according to instructions in a written contract requiring, among other things, the data processor to comply with the seventh Principle.

Where a destination country is found or presumed not to satisfy the adequacy test, the transfer of data can still be permitted if it is:

- Done with the consent of the individual.
- Necessary to enter or perform a contract with the individual (such as an employment contract) or is necessary to perform or conclude a contract with another party that is in the interests of the individual.
- Necessary for reasons of substantial public interest (such as crime prevention or detection).
- Necessary for, or in connection with, any legal proceedings (including prospective legal proceedings), for obtaining legal advice or otherwise for establishing, exercising or defending legal rights.
- Necessary to protect the life of the individual.
- Made on terms approved by the ICO as ensuring adequate safeguards for the rights of the individual.
- Authorised by the ICO as being made in a way that ensures adequate safeguards for the rights of the individual.

Also, the use of European Commission authorised model clauses or binding corporate rules provide adequate safeguards for the rights of the individual (see *Question 17*).

### 17. Are data transfer agreements contemplated or in use? Have any standard forms or precedents been approved by national authorities?

The European Commission has approved three sets of model clauses as providing adequate protection to transfer individuals' personal information, covering transfers outside the EEA of data from a data controller to either another data controller or to a data processor. However, to rely on approval, the clauses cannot be amended in any way. A separate contract is not required, the terms can be included in any general contract between the parties.

## THE REGULATORY AUTHORITY

### The Information Commissioner's Office (ICO)

**Head.** Richard Thomas (Information Commissioner)

**Contact details.** The Information Commissioner's Office  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF  
**T** +44 1625 545 700 (switchboard)  
**F** +44 1625 524 510  
**E** [mail@ico.gsi.gov.uk](mailto:mail@ico.gsi.gov.uk)  
**W** [www.ico.gov.uk](http://www.ico.gov.uk)

**Main area of responsibility.** The ICO is an independent supervisory authority, which reports directly to the UK Parliament. It enforces and oversees the:

- Data Protection Act 1998.
- Freedom of Information Act 2000.
- Privacy and Electronic Communications 2003.
- Environmental Information Regulations 2004.

**Contact for queries.** In addition to the contact details above, there is an ICO Helpline for general enquires (08456 30 60 60 or 01625 54 57 45) and an e-mail address for enquiries regarding notification under the Data Protection Act ([notification@ico.gsi.gov.uk](mailto:notification@ico.gsi.gov.uk)). There is also an online enquiries form.

**Obtaining information.** To obtain information, go to the website or contact the main switchboard above.

There are some cases where a data controller may reasonably decide that there is adequate protection without carrying out a detailed test, for example where there is a contract in place requiring the data processor to have adequate security and act only on the data controller's instruction.

Corporate intra-group transfers of personal data from the UK outside the EEA can be carried out using binding corporate rules (BCRs) approved by the ICO. If a data controller wishes to use BCRs to export data out of the EEA from a number of different European jurisdictions, there is a co-operation procedure through which the data controller can propose a "lead authority" in one country who liaises with the other relevant authorities to have the BCRs approved by them all. The ICO only expects to authorise one-off arrangements in exceptional circumstances.

To date, only one UK company has had its BCRs approved by the ICO.

**18. Is a data transfer agreement sufficient to legitimise transfer, or must additional requirements (such as the need to obtain consent) be satisfied?**

Assuming all the Principles (*see Question 8*) are complied with, a data transfer agreement is sufficient to legitimise transfer.

**19. Does the relevant national regulator need to approve the data transfer agreement? If so, please provide brief details.**

Agreements do not need to be approved on an individual basis. The data controller is responsible for ensuring adequate protection exists.

## ENFORCEMENT AND SANCTIONS

**20. What are the enforcement powers of the national regulator?**

If the individual is unable to resolve an issue with the data controller, the individual can make a request for assessment to the ICO. Provided sufficient information is provided, the ICO must make an assessment as to whether the processing complies with the DPA and inform the individual that it has made an assessment. The ICO can serve an information notice on a data controller requesting information. The ICO's priority is to give the data controller advice and ask it to resolve the problem so that it handles personal information properly in the future. Therefore, if the organisation has corrected the mistake, it is unlikely that the ICO will take action.

In the most serious cases, the ICO can serve an enforcement notice, which is a legally binding document requiring the data controller to take steps or refrain from processing data (there are additional requirements in relation to journalistic, literary or artistic material). However, in most cases the ICO cannot punish an organisation or award compensation for a breach of the DPA.

Failure to comply with an enforcement notice, information notice or a special notice (relating to journalistic, literary or artistic material) is an offence unless the data controller can show that they exercised all due diligence to comply with the notice.

The ICO also has powers (subject to a court warrant) of entry, inspection, and seizure of documents.

**21. What are the sanctions and remedies for non-compliance with the data protection laws? To what extent are the laws actively enforced?**

As at 1 March 2007, offenders are liable to a fine of a maximum of GB£5,000 (about US\$9,800) if convicted summarily in a Magistrate's Court, and an unlimited fine if convicted on indictment in a Crown Court (*section 60, DPA*). However, to deter people from trading in personal data, the Government intends to amend section 60 of the DPA to allow for, in addition to the current fines:

- On summary conviction, up to six months imprisonment (increased to twelve months imprisonment in England and Wales when section 154 of the Criminal Justice Act 2003 comes into force).
- On conviction on indictment, up to two years imprisonment.

The Government plans to introduce this amendment when Parliamentary time allows.

Officers of a company which has committed an offence under the DPA can have separate personal liability for that offence under the DPA. This liability arises if the company committed the offence with the officer's consent or due to the officer's neglect.

An individual can claim for compensation through the courts for damage caused by a breach of the DPA by the data controller. Such claims can be made whether or not the ICO is involved.

Also, data controllers who fail to give a proper data protection notice could commit the new offence of failing to disclose information under the Fraud Act 2006.

From April 2005 to March 2006, the ICO prosecuted 16 cases under the DPA, up from 12 in the previous year.

**PLC** Employment   
Essential know-how

PRACTICAL LAW COMPANY

“Having such a comprehensive, high-quality resource no further than our keyboard and mouse saves us time and money.”

Robert MacKenzie, Group Legal Director, NTL Group Limited.

**PLC Employment** is the premium web service for employment lawyers. It keeps users up to date with all relevant developments by e-mail and gives them access to practical support via continuously updated practice notes and standard documents. [www.practicallaw.com/employment](http://www.practicallaw.com/employment)

# Kemp Little LLP

“Always ahead of the game”  
(Legal Business)

“Particularly well positioned to capitalise on convergence”  
(Legal 500, 2006)

...in 2006, we were shortlisted for the Legal Week TMT Team of the Year 2006 and received 'stand out' ranking in the Management Category of the inaugural 'FT Innovative Lawyers' survey...

...adding to our track record of 8 excellence and innovation achievement awards and nominations over the last 5 years.



Kemp Little LLP  
Cheapside House  
138 Cheapside  
London  
EC2V 6BJ

Tel: 020 7600 8080  
Fax: 020 7600 7878  
[www.kemplittle.com](http://www.kemplittle.com)

“The City’s outstanding technology focused law firm”  
(Legal 500, 2006)