

MACFARLANES

COMMERCIAL

BRIEFING

DATA PROTECTION - AN OVERVIEW

TO WHOM DOES THE DATA PROTECTION ACT APPLY?

The rules on data protection contained in the Data Protection Act 1998 ('the Act') apply to all 'data controllers'. A data controller is anybody (including a person, a company or a partnership) who, alone or with others, determines the purposes for (or the way in which) any personal data is held or used. 'Personal data' is any information which relates to identifiable living individuals.

The Act regulates the 'processing' of personal data. 'Processing' is defined very widely, and covers any sort of activity that can be conducted with data, including holding, using, transferring and destroying data.

A person or organisation will not be a 'data controller' if they process personal data only in accordance with a third party's instructions, but as soon as they have a say in how or why data is held or used, they will become a 'data controller'. Where an employee holds or uses personal data in the course of his/her employment, the 'data controller' is the employer, not the employee. Certain territorial restrictions apply to persons who will be data controllers under the Act - essentially, data controllers must be resident or incorporated in the UK, or use processing equipment in the UK which goes beyond simply transmitting data through the UK.

FIRST MAIN REQUIREMENT OF THE ACT - NOTIFICATION

Each data controller must notify certain details of its processing of personal data to the Information Commissioner unless all of its processing falls within an exemption. The exemptions include processing personal data solely in respect of: (a) past, present and prospective staff administration (matters such as staff appointment, removal, pay, discipline, superannuation and work management); (b) accounts and records (matters such as sales and purchases, and deciding whether to accept anyone as a customer or supplier); and (c) advertising and marketing the data controller's business and associated public relations activities. The exemptions are all narrowly construed, and most businesses will not be able to show that all of their processing falls within the exemptions. If in doubt, every data controller should notify. In addition, certain types of businesses (including those providing financial services) must notify.

The following details need to be notified:

- a. the data controller's name and address;
- b. the name and address of any representative (e.g. the 'data protection officer') which the data controller may have nominated for notification purposes;
- c. a description of the data processed and the category or categories of individuals to whom the data relates (the 'data subjects');
- d. a description of the purposes for which the data is being processed;
- e. a description of the intended recipients of the data; and
- f. the names (or a description) of any countries outside the EEA (that is, the Member States of the European Union plus Iceland, Liechtenstein and Norway) to which the data controller does or may transfer the data.

Notification is a relatively simple process. The Information Commissioner's website at www.informationcommissioner.gov.uk provides a step-by-step guide and online notification form. The fee for notification is currently £35 per year, unless the data controller has a turnover of £25.9m or over and 250 or more members of staff, or they are a public authority with 250 or more staff in which case the notification fee is £500.

Notification creates a public record, which any member of the public is entitled to access without charge online at www.ico.gov.uk/ESDWebPages/Search.asp.

SECOND MAIN REQUIREMENT OF THE ACT - THE DATA PROTECTION PRINCIPLES

Apart from notification, all data controllers must comply with the eight data protection principles whenever processing personal data (and ensure that the principles are followed by any third parties they ask to process personal data on their behalf). The eight principles are:

1. data must be processed fairly and lawfully, and only where certain conditions set out in the Act are met;
2. data must be obtained only for one or more specified and lawful purposes and used only in ways compatible with those purposes;

3. data must be adequate, relevant and not excessive (so a controller must be able to justify possession of all data it holds and uses);
4. data must be accurate and kept up-to-date;
5. data must not be kept longer than necessary;
6. data must be used in accordance with the data subject's rights (see below);
7. appropriate technical and organisational measures must be taken against unauthorised or unlawful use of data and against the accidental loss or destruction of, or damage to, data; and
8. data must not be transferred outside the EEA unless certain safeguards exist.

'FAIR AND LAWFUL USE' - CONSENT

In relation to the first principle (fair and lawful use), the processing will be deemed not to be fair and lawful unless at least one of a number of specified conditions are met. Two of such conditions are that the data subject has consented to the processing of the data, or that the processing is necessary in order to perform a contract to which the data subject is a party.

An alternative condition applies where the processing is in the data controller's legitimate interests and does not unfairly prejudice the individual's rights.

'Opt-In' and 'Opt-out' boxes are a recognised approach to obtaining such consent whereby a data subject is given an opportunity to opt in/out of having their data used in certain ways by ticking a box on a form which is returned to the data controller. A helpful practical test for consent is the 'surprise test'. The data controller should put himself in the place of a data subject and ask whether he would be surprised to find his data being used in a certain way. If he would, it is likely that consent has not been obtained properly. Separate rules govern the sending of electronic marketing (eg emails).

The Act recognises two kinds of data; normal personal data and sensitive personal data. For sensitive personal data, express consent is required (eg 'I consent to ...'). 'Sensitive personal data' covers information about a person's racial or ethnic origin; political opinions; religious or similar beliefs; trade union membership; physical or mental health or condition; sexual life; or details of their criminal offences. Normal personal data is all personal data that is not sensitive personal data.

TRANSFERRING PERSONAL DATA OVERSEAS

Under the eighth principle, personal data must not be transferred outside of the EEA unless certain safeguards exist (although please note that, even if the eighth principle allows the transfer, the other principles - especially the first principle - must still be complied with).

The European Commission has decided that transfer of data to Guernsey, Jersey, Isle of Man, Argentina, Canada (in relation to certain recipients only), Switzerland and to entities who have signed up to the US 'Safe Harbor' regime is permitted under the eighth principle, the Commission having decided that those jurisdictions have adequate data protection regimes. Transfer to any other jurisdiction should normally, in order to comply with the eighth principle, either have the express consent of the data subject or be conducted under a data transfer contract in a form approved by the EU, although other methods of complying with the eighth principle are possible.

DATA SUBJECT RIGHTS

Broadly speaking, data subjects have the right, on written request and payment of a fee (currently set at a maximum of £10), to be told what personal data relating to them is being processed by the data controller, the purposes for which it is being used for, who is receiving it and where it came from. This is known as a right to make a 'subject access request'. Following a series of decisions on this issue, notably the Court of Appeal decision in *Durant v Financial Services Authority* and *Andrew Ezsias v The Welsh Ministers*, a data controller will only be required, in general, to inform a data subject of all biographical information focussing on the data subject which the data controller holds in a system which is easily searchable, and to only carry out reasonable and proportionable searches to locate the data.

Data subjects also have the right to prevent use of their data where it would be likely to cause them substantial damage or distress, to refuse permission for their data to be used for direct marketing purposes, and to have their data corrected or destroyed where it is inaccurate.

OFFENCES UNDER THE ACT

Contravention of the Act may involve criminal penalties and potentially unlimited fines. Offences under the Act include processing personal data without an appropriate notification, and improperly disclosing or obtaining personal data.

The Act also provides for separate personal liability for directors or other officers in certain circumstances. The director or officer will be guilty of an offence where it is proved that the company

committed the offence with the consent or connivance of, or due to any neglect on the part of, the director or officer.

From 6 April 2010, the Information Commissioner will have the power to impose a monetary penalty of up to £500,000 on data controllers where there has been a serious contravention of any of the eight principles, the contravention was likely to cause substantial damage or distress and was deliberate or reckless.

KEY POINTS

- ◆ Companies should ensure they notify appropriate details of their processing of personal data to the Information Commissioner.
- ◆ All data controllers must comply with the data protection principles.
- ◆ Contravention of the Act may involve criminal penalties, including the possibility of an unlimited fine and personal liability for officers of the company. From 6 April 2010 the Information Commissioner may impose fines of up to £500,000 for serious breaches.
- ◆ Companies should either obtain the express consent of data subjects for transfers of data to countries outside of the EEA or ensure that appropriate safeguards are in place.

CONTACT DETAILS

If you would like further information or specific advice please contact your usual Macfarlanes contact or:

JEREMY COURTENAY-STAMP

DD: +44 (0)20 7849 2358

jcs@macfarlanes.com

RUPERT CASEY

DD: +44 (0)20 7849 2256

rupert.casey@macfarlanes.com

MACFARLANES LLP
20 CURSITOR STREET LONDON EC4A 1LT

T: +44 (0)20 7831 9222 F: +44 (0)20 7831 9607 DX 138 Chancery Lane www.macfarlanes.com

This note is intended to provide general information about some recent and anticipated developments which may be of interest. It is not intended to be comprehensive nor to provide any specific legal advice and should not be acted or relied upon as doing so. Professional advice appropriate to the specific situation should always be obtained.

Macfarlanes LLP is a limited liability partnership registered in England with number OC334406. Its registered office and principal place of business are at 20 Cursitor Street, London EC4A 1LT. The firm is not authorised under the Financial Services and Markets Act 2000, but is able in certain circumstances to offer a limited range of investment services to clients because it is regulated by the Solicitors Regulation Authority. It can provide these investment services if they are an incidental part of the professional services it has been engaged to provide. © Macfarlanes April 2010