

DATA PROTECTION – THE NEW REGIME

The Data Protection Act 1998 (the “Act”) came into full force in the UK on 23rd October 2001.

The Act regulates the processing of all personal data by UK businesses. ‘Processing’ is defined in the Act as the obtaining, recording, or holding of information or data in order that the data can be organised, adapted, altered, retrieved, disclosed, transmitted, disseminated or otherwise made available to third parties, including the combining, blocking, erasure or destruction of information or data. Where such processing is carried out by a person who determines the purposes for which and the manner in which any personal data are or are to be processed, that person is known as a ‘data controller’.

Nearly every business in the UK is a data controller and is therefore be subject to the Act. Even merely reading data on a computer screen is processing! Businesses must take their responsibilities seriously - there are criminal penalties for not complying. Basically, all information from which a living individual can be identified is personal data and any processing of such must comply with the eight principles of the Act.

THE PRINCIPALS OF DATA PROTECTION

1. Personal data must be processed fairly and lawfully, and, in particular shall not be processed unless:
 - in the case of personal data, one of the conditions in Schedule 2 of the Act must have been complied with. These conditions generally make sure that the processing of the data is necessary or that the consent of the person involved has been obtained.
 - in the case of sensitive personal data, one of the conditions in Schedule 3 of the Act must have been complied with. These conditions are similar to the conditions in Schedule 2, but are more stringent. For example, the explicit consent of the person involved has to be obtained or the processing has to be necessary in order to fulfil certain restrictive purposes, like compliance with employment law. “Sensitive personal data” means data relating to person’s ethnic or racial origin, his political opinions or trade union involvement, religious beliefs or health.
2. Personal data must not be processed in any manner incompatible with any purpose other than the specified and lawful purposes for which the data was obtained.
3. Personal data must be adequate, relevant and not excessive in relation to the purpose for which the data is processed.
4. Personal data processed must be accurate and where appropriate updated.
5. Personal data processed for any purpose must not be held longer than is necessary.
6. Personal data must be processed in accordance with the rights of data subjects under the Act.
7. Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage, to personal data.
8. Personal data must not be transferred outside the European Economic Area (“EEA”) unless one of the exceptions shown below applies.

NOTIFICATION OF YOUR BUSINESS

All data controllers must, unless they are exempt, notify the Office of the Information Commissioner (“OIC”) that they are processing personal information and data. Such notification also needs to specify what steps the organisation is taking to comply with the above seven principles.

ACCESS TO DATA

Under the Act each individual ('data subject') has seven separate rights:

- Right of access to personal data.
- Prevention of processing likely to cause damage or distress.
- Prevention of processing for direct marketing.
- Prevention of automated decision making.
- Rectification, blocking, erasure, and destruction.
- Compensation.
- Request for assessment.

The most important of these is the data subject's right of access. A data subject has the right to obtain a copy of all personal data held about himself by any UK business by sending a written request.

This right can be an administrative nightmare for businesses. However, the business is entitled to charge a fee for access, up to a statutory maximum of £10 (in the case of some education and health data records, this maximum increases to £50). In return, the data controller must inform the person requesting the information of the personal data which is held about the individual, the purposes for which the data is being or to be processed and to whom the results are to be disclosed. Such information must be disclosed in an intelligible form, along with details of the source of the data obtained.

Research carried out by the OIC confirms that there has been a dramatic increase in the privacy awareness amongst the general public, which, not surprisingly, has led to a corresponding number of complaints to the OIC. It is worth noting that while the OIC knows that compliance with the Act causes considerable irritation and uses up the precious resources of a business, it is obliged to investigate all complaints made to it.

CONSENT

If personal data is obtained by a business from a third party without the knowledge of the data subject (e.g. by purchasing mailing lists) the data subject must, as a general rule, be told that there has been a sourcing of their personal information and the purpose for which the data has been sourced.

TRANSFERS OF PERSONAL DATA OVERSEAS

Personal data must not be sent to countries outside the EEA and any such transfer is unlawful. There are three exceptions to this. The first exception is where the data controller can show that the country to which the data is being sent has data protection legislation in place similar to or better than the UK. Currently, only Hungary and Switzerland fulfil this criteria. The second exception is where a data subject consents to their personal data being sent to the destination. The third exception is that personal data may be sent to the United States if the recipient has complied with the "safe harbour" rules negotiated between the EC and the US State Department of Commerce.

PAPER RECORDS

The biggest challenge for business will be complying with the application of the Act to paper records and notes. The government have recognised this difficulty and have allowed for there to be an additional period for compliance with this. Businesses have until 24th October 2007 to comply with the Act. However, this exception only applies to data held immediately before 24th October 1998. Any paper records held after the 24th October 1998 do not fall under this exception.

CONCLUSION

Most businesses, unless they are exempt, are likely to fall under the provisions of the Data Protection Act 1998 and are required to register with the OIC on an annual basis. Failure to register where your business is subject to the Act is a criminal offence and if you are in any doubt about whether the Act applies to you, you should register your business. When you are dealing with anyone's personal data, you should ensure that your business complies with the requirements of the Act.

MEDIA & TECHNOLOGY UNIT



Mark O'Halloran

office: 01293 643430

mobile: 07810 504556

email: mark.ohalloran@stevensdrake.com

sd.