

LEGISLATION IN BRIEF

Data Protection Act

In the UK, the collection and use of personal data is primarily governed by the Data Protection Act 1988. The DPA applies to the “processing” of “personal data”. Both these concepts are, under the legislation, very widely defined; the effect of this is that virtually every business operating in the UK (including foreign companies with UK branch offices) which holds information about individuals – whether employees, customers or anyone else – is affected by the DPA. Breach of the DPA can result in adverse publicity for organisations and, ultimately, criminal liability for its officers.

The following is a summary of the main provisions:

Notification

- Unless falling within one of the DPA’s narrow exemptions, every data controller who is processing personal information must notify the Information Commissioner’s Office.
- Notification must be renewed annually. Failure to notify is a criminal offence.

Data Protection Principles

- The DPA sets out a series of eight enforceable principles which require that data must be: (i) fairly and lawfully processed; (ii) processed for limited purposes; (iii) adequate, relevant and not excessive; (iv) accurate and up to date; (v) not kept longer than necessary; (vi) processed in accordance with the individual’s rights; (vii) secure; and (viii) not transferred to countries outside the EEA unless the destination country has adequate protection for the individual whose data is being transferred.
- Breach of any of these principles can lead to service of an information, special information or enforcement notice. Failure to comply with any of these constitutes a criminal offence. In practice, however, many organisations have found it difficult to apply all eight principles.

- Fair and lawful processing is probably the most important of all the principles. Processing will not be lawful if it relates, for example, to stolen information. It will not be fair if the individual is misled, if pressure or inducements are applied when collecting the data or if the subject is not given information about the data controller or the purposes for which his data is being collected. Additional rules apply in respect of direct marketing.
- The DPA applies to all information contained in a “relevant filing system”. This applies to data stored electronically but may also extend to paper files, microfiche and card indexes if sufficiently sophisticated.

Sensitive Personal Data

- Sensitive personal data includes information relating to race, sexual orientation, political opinions, health, religious and other beliefs and criminal records.
- It may only be processed fairly and lawfully if the individual has given his explicit consent to the processing or it falls within one of the limited exemptions (such as the processing is necessary for medical purposes, for the purpose of legal proceedings or the data relates to race or ethnic origin and is processed in the context of diversity monitoring).
- The rules on sensitive personal data may arise in situations which are not always obvious. For example, information relating to dietary requirements may indicate ethnic origin or religious beliefs and so would constitute sensitive personal data.

Rights of Individuals

- *Right of Access.* On application to the data controller, the data subject has the right to be told whether personal data relating to him is being processed. If so, he has a right to a description of the personal data held, the purpose for which it is being held, any person to whom it may have been disclosed and any information as to the source of the data.
- In order to satisfy these obligations, the data controller must supply a copy of the data in permanent form (for example in hard copy or on disk).
- *Right to Object to Processing.* Individuals have limited rights to require data controllers to refrain from processing their personal data in circumstances where such processing causes or is likely to cause unwarranted substantial damage or distress or where such processing is used for direct marketing.

Emergent Technologies

- Recently, the Data Protection Working Party has considered the practicalities of bringing new technologies within the ambit of the DPA.
- Certain retailers have proposed using tracking technology (Radio Frequency Identification) to track goods and prevent theft. Such tracking information could potentially provide highly valuable information about the shopping habits of individuals. The DPA could apply, even if the data controller is not able to identify the shopper by name or address.

- Similarly, in the area of biometrics, businesses which use voice/iris/fingerprint or other automatic identification or verification technology could find themselves having to apply the DPA principles to such methods of data capture.
- Businesses wishing to utilise new technology which also acts as a collector of data (whether as a main purpose or as a by-product) should seek advice to ensure that they are not inadvertently breaching the DPA.

Useful URLs

Information Commissioner's Office – www.ico.gov.uk

To learn more about data protection and how you can protect your business, email Andy Moseby at Kemp Little LLP at andy.moseby@kemplittle.com