Legal and Regulatory Update

Data protection with particular reference to the Internet

Michael Chissick and Jan Radler

Michael Chissick
is head of the IT and On-Line Law Group at Field Fisher Waterhouse. He advises clients ranging from IT consultants, to Internet service providers and companies providing IT systems and launching e-commerce sites.

Jan Radler
is a solicitor with Field Fisher Waterhouse with three years' post-qualification experience. He advises a number of large IT users and suppliers. His most recent experience involved advising on the implementation of a system delivering digital television on fibre-optic cables and assisting several companies setting up entirely Internet-based business.

Keywords: Data protection, accuracy, security, compliance

Introduction

The fast growth of electronic commerce gives rise to many privacy issues. Associated with e-commerce are new ways of paying for goods and services.¹ The common feature of all the electronic payment mechanisms is that the payer must disclose identifying data to the payee to establish commercial trust and satisfy regulatory and/or legal obligations of the payee to the clearing bank or credit institute involved in the payment transaction. The Data Protection Act 1998 applies to all these personal data obtained and processed over the Internet as it does to information obtained by more conventional sources for automatic processing.² The identification data consist of the name, card number, expiry date and real-world address for credit cards, and name and digital signature for digital cash. In the course of the transaction these personal data will be broadcast on the Internet.

By the time the EU Directive on Data Protection was adopted by the European Union on 24 October 1995, the whole computer and data-processing industry had been revolutionised by browser technology and hot-linking. Commentators have said that the legislation was unworkable and out of date before it had even been adopted. The USA, which prefers to leave regulation to industry, views the European Data Protection Directive as a classic demonstration of EU fondness for bureaucracy and regulatory overkill.

The Data Protection Act 1998 and the eight principles of data protection

The EU Directive³ on Data Protection and the UK Data Protection Act 1998 will govern the processing of all personal data in electronic transactions and are therefore likely to apply to every electronic transaction. The underlying principle of the legislation is, however, not to facilitate ease of passing on of data for securing and supporting electronic commerce. Instead it seeks to impose strict limitations on the use that may be made of personal data and the ability to transfer the personal data freely on the Internet.

The Data Protection Act 1998 (DPA) will implement the EU Data Protection Directive.⁴ It replaces the Data Protection Act 1984 in its entirety. Although many of its principles and provisions will be familiar from the former Act, it is bigger and more extensive, divided into six parts. New terminology replaces the terms used in the old Act, to reflect the increased powers and status of the Data Protection Registrar. Whilst the DPA sets out the overall legal framework, much of the detail will be contained in secondary legislation.

Michael Chissick,
IT and On-Line Law Group,
Field Fisher Waterhouse
Solicitors,
35 Vince Street, London
EC3N 2AA
Tel: +44 (0)171 481 4841
Fax: +44 (0)171 488 0084
E-mail: mpc@ffwlaw.com

Personal data

The 1998 Act defines 'data' as information which is or is intended to be processed electronically, or which forms or is intended to form part of a 'relevant filing system'.⁵ The definition of 'personal data' is 'data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller'.⁶ The definition of 'processing' would cover all forms of encryption, sending, decryption and verification of digital signatures or other forms of identification of a party to an electronic transaction.⁷ Applying these very wide definitions it is difficult to think of any scenario that would involve any sort of dealing with 'data' which would not constitute 'processing'. This ensures that the DPA will apply after the transitional period from the old Act to all dealings and use of data relating to an individual by someone other than the individual concerned.

Data controller

A 'data controller' is 'a person who (either alone or 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'.⁸ It is the 'data controller' who bears primary responsibility for compliance with the 1998 Act for any processing activity. In addition to notification requirements, data controllers have an automatic statutory duty to comply with the Data Protection Principles.⁹ New under the 1998 Act is that breach of the Principles may give rise to direct liability for damages to any adversely affected individual, regardless of whether there is any regulatory intervention.¹⁰

Fair and lawful processing

The First Data Protection Principle provides that '[p]ersonal data shall be processed fairly and lawfully'.¹¹ In order for processing to be considered fair and lawful certain information must be provided, or made readily available, to the individual concerned.¹² This information includes the identity of the data controller and any nominated representative, the purpose or purposes for which the data are intended to be processed, and 'any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair'.¹³ This would be consistent with the requirements of the Distance Selling Directive to provide the minimum information about the purchase conditions prior to entering into any transaction.¹⁴ However, the application of the First Data Protection Principle goes further, as it applies at the time of any data collection from the data subject¹⁵ whether or not a visitor to a virtual shop decides to purchase goods or services or not. The Data Protection Registrar in her 1998 Annual Report commented that '[w]hen information is input onto a form on a web site it is immediately capable of being processed as personal data. Notifications of the uses and disclosures of the data should therefore be given at the beginning of the form, so that the individual can decide, on

First Principle of Data Protection

the basis of full information, whether or not to proceed with the transaction.¹⁶

Moreover, personal data must not be processed unless one of a number of conditions is satisfied.¹⁷ The most relevant for electronic transactions are the consent of the data subject, or necessity for the performance of a contract to which the data subject is a party or for taking steps to enter into a contract, for compliance with a legal obligation (other than contractual). In addition, processing is justified for certain public sector purposes or if it is 'necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject'.¹⁸ It is difficult to assess where the balancing middle ground may lie. If interpreted broadly, it would justify many routine business data-processing activities. However, until such a time as guidance has been provided in secondary legislation or has been published by the Data Protection Commissioner, or the concept has been tested in the courts, it would not be prudent to rely heavily on this rather vague justification for processing data. If a data controller begins processing data in reliance on the balance of interests test and subsequently finds that the test has been failed, it may at that stage be very difficult to establish one of the other grounds for processing.¹⁹

Sensitive personal data

The 1998 Act introduces a new concept of sensitive personal data. 'Sensitive personal data' are defined as 'personal data consisting of information as to' a data subject's racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, membership of a trade union, physical or mental health or condition, sexual life, or commission or alleged commission or proceedings in relation to any offence.²⁰ Processing of sensitive data will be legitimate only if the data subject has given her or his 'explicit consent'; the processing is necessary in relation to an employment right or obligation; the processing is necessary to protect the vital interests of the data subject or another person in circumstances where consent is not obtainable; the processing is by a charitable body in relation to its members; the data subject has made the data public; the processing is necessary in relation to legal proceedings or advice; or the processing is for certain public sector purposes. In addition, processing of sensitive data may be legitimate in the public or private sectors where it is carried out for medical purposes by a health professional, or where it is carried out, with appropriate safeguards, for ethnic monitoring purposes to promote or maintain equality. The UK Secretary of State may specify other circumstances in which sensitive data may be processed.

The issue of processing 'sensitive personal data' may arise on the Internet much more readily than would be expected at first sight. Obvious examples are members' areas of websites of political parties, or commercial sites distributing sexually explicit material. In other cases,

the association may be more subtle or uncertain. For example, does the hosting by an online service provider of a discussion or chat forum relating to a particular medical condition or treatment constitute processing of sensitive personal data? What if an airline or Internet travel agency collected data via a website relating to the dietary requirements of passengers? Again, whether that would constitute processing of sensitive personal data might depend on the precise facts. For example, a request for a vegetarian meal on a flight would probably not be sensitive personal data, whereas a request for a kosher or diabetic meal on a flight might be.²¹

Second Principle of Data Protection

Specified and lawful purposes

Pursuant to the Second Data Protection Principle, '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'.²² Previously, under the 1984 Act, it was sufficient to specify the purposes with the Data Protection Registrar at the time of registering. The new Act states that the purpose or purposes for which data are obtained may be specified in a notice given to the data subject or in a notification to the Commissioner.²³ This emphasises the obligation on the data controller to provide full information to the data subject before collection of the information, and may result in restricting the right to process the 'personal data' to the purposes actually notified to the data subject.

Third Principle of Data Protection

Adequate, relevant and not excessive

'Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed' under the Third Data Protection Principle.²⁴ This has important implications for the use made of an Internet website. Many websites are still primarily used as world showcases for companies. Often separate member areas are only accessible to the visitor after registering with the operator. The operator often trades additional valuable information or certain services for access to the private details of his/her visitors. The measure of what information may be requested from such visitors and be considered adequate, relevant and not excessive will in part be determined on the existing data protection registration and the advance notice provided by the operator before making the enquiries. The operator should make it clear precisely why any non-essential questions are being asked and whether a response is optional.

Fourth Principle of Data Protection

Accurate and up to date

'Personal data shall be accurate and, where necessary, kept up to date.'²⁵ The interpretation provisions state that this Principle will not be contravened where data obtained from the data subject or a third party are inaccurate provided that 'the data controller has taken reasonable steps to ensure the accuracy of the data' and the data record any view which the data subject may have expressed to the controller as to their inaccuracy. The reasonableness of any verification steps is to be judged

in the light of the purposes for which the data were obtained or further processed.²⁶ Compliance with this Principle may not pose serious difficulties where the operator of a website collects the personal data from the data subject direct, for example just before a sale-of-goods transaction. More problematic may be the scenario where the operator collects personal data from other sources on the Internet which are not readily verifiable, for example collection of details of access to news items prior to launching a news service on the Internet.

Fifth Principle of Data Protection

Timeliness

‘Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.’²⁷ This may prove to be particularly burdensome where it would demand that the operator of a virtual shop filter out all electronic records of visitors who did not purchase any goods and services, so as to limit the statutory record-keeping obligations to those to which the statutory obligations apply, namely concluded transactions.

Sixth Principle of Data Protection

Compliance with individuals rights

The Sixth Data Protection Principle requires data controllers to process personal data ‘in accordance with the rights of data subjects under this Act’.²⁸ An interpretation provision states that a person will be regarded as contravening this Principle only if he fails to provide access to data as required, fails to comply with a notice from a data subject requiring him to stop processing data for certain purposes, or fails to comply with the procedures relating to automated decision making.²⁹ This restrictive statement should, however, be read in conjunction with the general right which an individual has under s. 13 of the Act to compensation where he has suffered damage as a result of contravention by a data controller of any of the requirements of the Act. The difference between these two provisions is that a breach of the Sixth Principle may trigger the service on the data controller by the Data Protection Commissioner of an enforcement notice, whereas breach of s. 13 may form the basis for a civil claim for compensation for damage and, possibly, distress.

Seventh Principle of Data Protection

Security

The Seventh Data Protection Principle provides that ‘[a]ppropriate 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’.³⁰ Given the degree of public concern regarding the security, or otherwise, of communications and transactions via the Internet, this Principle needs to be considered carefully, notwithstanding that public concerns may be vastly overstated.

The 1998 Act contains some interpretation of this Principle from which a number of practical conclusions can be drawn. The first is that what constitutes ‘appropriate’ security will vary widely depending on the circumstances. Relevant factors include the nature of the data to be protected, an assessment of the harm that might result from

unauthorised or unlawful processing or accidental loss, destruction or damage, the state of technological development and the cost of any security measures.³¹ This suggests, for example, that whereas publication on a website of information which is already in the public domain might require little or no security cover, the collection via e-mail or the Web of medical or other sensitive data might necessitate adoption of rigorous security measures.

Secondly, data controllers are required to 'take reasonable steps to ensure the reliability of any employees who have access to the personal data'.³² Again, the use of the word 'reasonable' suggests different measures may be appropriate depending on the circumstances, ranging from minimal supervision to positive vetting.

Thirdly, where a data controller uses a data processor, the controller will automatically be in breach of the Seventh Principle unless both of the following criteria are satisfied:

- the processor provides 'sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out' and the controller takes 'reasonable steps to ensure compliance with those measures'.³³
- the processing is governed by a written contract requiring the processor to act only as instructed by the controller and to comply with security obligations equivalent to those imposed on the controller.³⁴

In the Internet context, data controllers will need to ensure that they have appropriate, and properly documented, contractual arrangements in place with any ISPs or other third parties which process data on their behalf, for example by hosting websites.

Eighth Principle of Data Protection

Transborder flow of personal data

The Eighth Data Protection Principle provides that '[p]ersonal 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'.³⁵ The concept of 'adequacy' is complex and may be more flexible than it appears at first sight.

Nevertheless, there are likely to be many instances where it cannot be demonstrated that a destination country ensures an adequate level of protection. To overcome the Eighth Principle's prohibition on transfer in such cases it will be necessary to rely on one or more of the exemptions listed in Schedule 4 to the 1998 Act. There are nine exemptions, the first seven of which apply 'automatically', in the sense that no prior regulatory approval is needed. The remaining two exemptions are not automatic and require the prior approval of the Data Protection Commissioner.

Probably the most straightforward automatic exemption is that the data subject has consented to the transfer.³⁶ Although the Internet is perceived by some as a threat to privacy, it may in fact prove to be a particularly effective medium for obtaining data protection consents.

An individual can be provided, by e-mail or via a Web page, with the requisite information to make an informed decision about an international transfer. The consent of that individual can then be captured via a return e-mail or a 'click-through' on a website.

The second and third automatic exceptions to the prohibition on transfer relate to contracts which a data controller might enter into with or for the benefit of a data subject, as well as preparatory steps in relation to such contracts.³⁷ Again, there may be many instances in the Internet context where one of these exemptions will justify the transfer of personal data to inadequate countries. Obvious examples would be the various transfers necessary to set up and complete an electronic commerce transaction. These might include payment arrangements with credit card issuers and fulfilment arrangements with suppliers and shippers.

The remaining automatic exemptions³⁸ are likely to be of much more limited relevance in the Internet context. The fourth covers transfers that are necessary for reasons of substantial public interest. The fifth applies to transfers that are necessary in connection with legal proceedings, legal advice or for establishing, exercising or defending legal rights. The sixth is available where the transfer is 'necessary to protect the vital interests of the data subject', and the seventh covers transfers of personal data from a public register.

This leaves the two non-automatic exemptions to the prohibition on transfers. These are the only other grounds on which personal data may lawfully be transferred to a non-EEA country which fails to ensure adequate protection for data subjects. The first covers transfers which are 'made on terms of a kind approved by the Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects'.³⁹ The second covers transfers which have been 'authorised by the Commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects'.⁴⁰

In the UK, detailed guidance is awaited from the Data Protection Commissioner on how these exemptions will be handled in practice. She has already stated that she 'intends to take a pragmatic approach to the issue of transferring personal data to third countries'. To a significant extent, however, her flexibility may be constrained by the European Commission, by the other EU national data protection regulators and, ultimately, by the EU Council of Ministers.

Some important guidance has already been published by the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data (the 'Working Party').⁴¹ The views of this Working Party are strongly indicative of likely regulatory practice across the EEA as the Working Party is comprised of the various national data protection regulators in the EEA. So far, the Working Party seems determined to adopt a strict approach to assessing both adequacy and special exceptions to the prohibition on transfer to non-adequate countries. This is consistent with the EU Directive, in which a discussion in the preamble regarding transborder data flows concludes with the simple statement that 'in any event, transfers to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to this Directive'.⁴²

Even that may not be the end of the story, however. Article 31 of the EU Directive has established a further committee, comprising representatives of the member states. The European Commission is required to submit to this committee drafts of any measures to be taken in relation to special international transfer authorisations. The committee may disagree with the Commission's approach, resulting in suspension of the relevant 'measures' and referral to the EU Council of Ministers, who may ultimately 'take a different decision'.⁴³

The transborder data flow rules in the EU Directive and the 1998 Act seem to be based on a presumption that international data traffic always follows precise and predictable routings. This assumption is fundamentally at odds with the way in which information is in fact conveyed via the Internet for at least two reasons. First, the Internet, which is a vast and dynamically configured network of networks, has a so-called 'self-healing' architecture. Messages, or data representing information of any other kind, are split into 'packets' which are sent via the most efficient routing at any given instant. A technical obstacle to the transmission of particular packets will be bypassed automatically and the packets concerned will be forwarded via a different route. Transfers are thus not predictable in geographical terms.

Secondly, because Internet e-mail can be downloaded and Web pages can be viewed from anywhere on the planet where an individual or organisation has a connection to an Internet service provider, the sender of a message or operator of a website has no effective control over where a particular message will be downloaded or Web page viewed. Even where, for example, there are rigorous access controls on a particular website, even if the website operator can conclusively verify the identity of a particular visitor to that site, it is difficult to see how the operator can be sure of the physical location of that visitor. Consequently it must be assumed that data contained in Internet e-mail messages and Web pages potentially may be transferred to any country in the world, without regard to the adequacy or otherwise of the local data protection safeguards, if any.

Moreover the sheer volume of personal data which is conveyed via the Internet and the vast number of data transfers make it inconceivable that even a significant minority of transfers can be regulated in any meaningful way under the cumbersome rules established by the EU Directive and the 1998 Act.

Jurisdictional data protection issues

The 1998 Act applies to data controllers in respect of particular data only if the controller is either established in the UK and the data are processed in the context of that establishment, or the controller is established outside the EEA 'but uses equipment in the United Kingdom for processing the data otherwise than for the purposes of transit through the United Kingdom'.⁴⁴ A data controller who falls into the second category must nominate a representative in the UK in relation to their obligations under the 1998 Act.

This apparently straightforward statement of territorial scope is fraught with difficulty in the Internet and online services context.

For one thing, due to the breadth of the establishment concept in the 1998 Act, it is possible that an Internet service provider will be established in multiple states within the EEA. Similarly, a commercial organisation may find that it is subject to multiple, and in certain respects inconsistent, national rules in relation to its internal cross-border intranet. Even where a data controller is not established in multiple EEA states, they may at least use equipment in multiple states. The EU Directive makes it clear⁴⁵ that 'when the controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable'.

The second problematic aspect of the territoriality provision in the 1998 Act is the exception for the processing of data using equipment in the UK which is merely 'for the purposes of transit through the United Kingdom'.⁴⁶ What if, for example, a website on a server in the USA is 'mirrored' by a UK-based ISP on a server in the UK to facilitate access to that site by UK-based customers of the ISP? Will the ISP in the UK become a data controller in relation to any personal data contained in that website? Will the ISP in the USA be treated as established in the UK merely because an ISP in the UK has chosen to make a copy of the site (quite possibly without the site controller's knowledge)? What if a website on a server in the USA plants a 'cookie' on the PC of a UK-based visitor to the site and subsequently interrogates that cookie remotely each time the visitor returns to the site? Is the data controller in the USA using equipment in the UK (ie the visitor's PC) to process data about that visitor? Given that 'processing' includes 'obtaining, recording or holding ... information or data', such a construction is possible. This would, however, be an absurd result as the website operator in the USA would presumably have to appoint the UK visitor as its representative for the purposes of compliance with the 1998 Act!

Privacy enhanced technologies

There are new technological solutions which may provide alternatives to the current requirements of disclosing personal data in electronic transactions. These are being given strong support by the European Data Protection Commissioner. Under the 1998 Act data which do not identify the individuals directly will only be 'personal data' in the hands of a data controller if that data controller has, or is likely to obtain, possession of any database or other data necessary to match up the data records with particular individuals.

The use of such anonymous payment mechanisms as digital cash sets out alternatives to the present payment systems with credit cards. A balance may be more readily found between the competing interests of secure electronic transactions and the protection of the privacy of personal data.

The UNCITRAL Model Law seeks to establish reliability for methods of signature of electronic documents.⁴⁷ It provides that form requirements relating to signatures may be met in relation to data messages where a method is used that identifies the person and

indicates that person's approval of the contents of the data message. The draft guide to the UNCITRAL Model Law does indicate that it may be useful to develop functional equivalents for the various types and levels of signature requirements in existence. The UNCITRAL Model Law further treats signature requirements in the context of the evidential weight of data messages based upon the reliability of the manner in which the data message was generated, stored, communicated and maintained in general.

The underlying policies articulated and promoted in the UNCITRAL Model Law and the GUIDEC, seen as vital to address the security aspects and trust in electronic business environments, are:

- to enhance the ability of the international business community to execute secure digital transactions;
- to establish legal principles that promote trustworthy and reliable digital ensuring and certification practices;
- to encourage the development of trustworthy ensuring and certification systems;
- to protect users of the digital information infrastructure from fraud and errors;
- to balance ensuring and certification technologies with existing policies, laws, customs and practices;
- to define and clarify the duties of participants in the emerging ensuring and certification system;
- to foster global awareness of developments in ensuring and certification technology and its relationship to secure electronic commerce.

Conclusion

There is much in the 1998 Act of relevance to businesses carrying out activities via the Internet. It will, however, be some time before it is possible to ascertain the precise impact of the 1998 Act on Internet-related activities. A substantial amount of detailed regulation will be established via secondary legislation that has not yet been published. Moreover, it is likely to be several years before anything approaching the full implications of the 1998 Act can be discerned via a combination of guidance from the Commissioner, decisions of the Data Protection Tribunal and decisions of the courts.

It could be argued that the 1998 Act, and similar laws in other jurisdictions which implement the EU Directive, will facilitate the development of the Internet. It is indeed possible that e-commerce will not flourish to the full extent possible in the absence of a sufficient degree of public confidence in the legal protection of privacy and security. Unfortunately, however, the restrictive and inflexible nature of many of the specific rules in the EU Directive and the 1998 Act may, if enforced strictly, stifle online innovation. The costs of e-commerce may be raised significantly without there being much to show in terms of enhanced protection for consumers and other data subjects. Moreover, certain requirements of the 1998 Act and the EU Directive may turn out

to be completely unworkable. In particular, the new transborder data flow regime may prove to be fundamentally incompatible with the 'any to any' network architecture of the Internet. National data protection regulators, and the European Commission, may quickly discover that it is futile to try to superimpose virtual border controls, based on terrestrial jurisdictional boundaries, on data traffic in cyberspace.

References

1. 'Towards a European Framework for Digital Signatures and Encryption', COM (1997) 503.
2. The 14th Annual Report of the Data Protection Registrar, published 14 July 1998.
3. European Directive 95/46 EC.
4. *Ibid.*
5. Section 1(1) DPA 1998.
6. *Ibid.*
7. *Ibid.*
8. *Ibid.*
9. Section 4(4) DPA 1998.
10. Section 13 DPA 1998.
11. Schedule 1, Part I, para 1 DPA 1998.
12. Schedule 1, Part II, para 2(1) DPA 1998.
13. Section 2(3) DPA 1998.
14. Distance Selling Directive 97/7 EC, Articles 4 and 5.
15. Section 2(2) DPA 1998.
16. The 14th Annual Report of the Data Protection Registrar (London: The Stationery Office, 1997) at p 60.
17. Schedule 2 DPA 1998.
18. *Ibid.*
19. Christopher Millard, (1999) *Society for Computers and Law*, February/March, Vol 9, Issue 6.
20. Section 2 DPA 1998.
21. Millard, ref. 19 above.
22. Schedule 1, Part I, para 2 DPA 1998.
23. Schedule 1, Part II, para 5 DPA 1998.
24. Schedule 1, Part I, para 3 DPA 1998.
25. Schedule 1, Part I, para 4 DPA 1998.
26. Schedule 1, Part II, para 7 DPA 1998
27. Schedule 1, Part I para 5 DPA 1998.
28. Schedule 1, Part I, para 6 DPA 1998.
29. Schedule 1, Part II, para 8 DPA 1998.
30. Schedule 1, Part I, para 7 DPA 1998.
31. Schedule 1, Part II, para 9 DPA 1998.
32. Schedule 1, Part II, para 10 DPA 1998.
33. Schedule 1, Part II, para 11 DPA 1998.

- 34. Schedule 1, Part II, para 12 DPA 1998.
- 35. Schedule 1, Part I, para 8 DPA 1998
- 36. Schedule 4, para 1 DPA 1998.
- 37. Schedule 4, paras 2 and 3 DPA 1998.
- 38. Schedule 4, paras 4 to 7 DPA 1998.
- 39. Schedule 4, para 8 DPA 1998.
- 40. Schedule 4, para 9 DPA 1998.
- 41. See in particular the Working Party's working document entitled 'Transfers of personal data to third countries — applying Arts 25 and 25 of the EU Data Protection Directive, adopted on 24 July 1998' (DG XV D/5025/98/final, WP12).
- 42. EU Directive on Data Protection, 95/46 EC, Recital 60.
- 43. EU Directive on Data Protection, 95/46 EC, Article 31.
- 44. Section 5(1) DPA 1998.
- 45. EU Directive on Data Protection, 95/46 EC, Article 4(1)(a).
- 46. Section 5(1)(b) DPA 1998.
- 47. UNCITRAL Model Law, Article 6.