SIDLEY AUSTIN BROWN & WOOD

London

THE DATA PROTECTION ACT 1998

The Data Protection Act 1998 (the "DPA"), which implements the European Data Protection Directive 95/46 EC (the "Directive"), came into force on 1 March 2000. The DPA allowed for two periods of transition, the first of which ended on 24 October 2001. The second transitional period ends on 23 October 2007, but only applies in limited circumstances to eligible manual data held immediately before 24 October 1998. Most businesses which are Processing data in the UK will now need to comply with the provisions of the DPA.

The DPA replaces the Data Protection Act 1984 (the "1984 Act"). Though the basic principles of the 1984 Act remain in place, the new data protection regime established by the DPA is much wider in scope and application.

1. Comparison of the DPA and the 1984 Act

In contrast to the 1984 Act, the DPA:

- increases the scope of the UK data protection regime - the DPA covers manual as well as automated filing systems, and ends certain exemptions available under the 1984 Act;
- introduces a number of pre-conditions before data can be processed "fairly and lawfully" (see section 3.1 below);
- introduces new and more onerous obligations for the Processing of "sensitive" Personal Data (see section 4 below);
- requires certain information to be provided to Data Subjects on collection of Personal Data and in response to Data Subject access requests (see Section 5 below);
- introduces new and enhanced Data Subject rights, and more extensive rights to compensation (see Sections 3.6 and 9 below);
- introduces a simplified notification procedure which replaces the registration requirements under the 1984 Act (see Section 9 below);
- introduces new restrictions on the transfer of Personal Data to third countries (see Section 3.8 below) and;
- places greater obligations on Data Controllers to maintain data security (see Section 3.7 below).

2. Application of the DPA and Definitions

The DPA covers the Processing of Personal Data by a Data Controller which is either:

- Established in the UK and the Personal Data are processed in the context of that establishment; or
- not Established in the UK (or any other EEA state) but uses equipment in the UK for Processing, unless that equipment is used for the mere transit of Personal Data through the UK.

All of these capitalised terms are defined below:

"Data Controller" is any person who determines the purposes for which and the manner in which any Personal Data is, or is to be, processed. A Data Controller may be an individual, such as a freelance consultant or a sole trader, a partnership or a company. A company operating a website through which it collects Personal Data is likely to be a Data Controller even when it uses another company to host the website.

The DPA distinguishes between Data Controllers and Data Processors. Please see 8 below for further details of Data Processors under the DPA.

"Data Subject" is an individual who is the subject of the Personal Data. This definition expressly excludes corporate entities.

"**Data Processor"** in relation to personal data, means any person (other than an employee of a data controller) who processes the data on behalf of the data controller.

"Established" is defined in the Directive rather than the DPA, and implies the "effective and real" exercise of activity through stable arrangements. This includes individuals resident in the UK, companies incorporated in the UK, partnerships formed under UK law, branches and subsidiaries.

"Personal Data" is data which relates to a living individual who can be identified from that data or from that data and other information which is in the possession or likely to come into the possession of the Data Controller. This data can include any expression or opinion or intention relating to that individual. An individual's name and address are Personal Data, as is an e-mail address of an individual if it contains enough information to identify him. However, a computerised list of company names and addresses would not be Personal Data (and therefore not covered by the DPA) if the list does not identify any individuals. If this list contained details of the company employees, it would be Personal Data.

"Processing" is widely defined in the DPA, and covers obtaining, recording, or holding information or carrying out any operation or set of operations on the information or data and includes any of the following: organisation, adaptation, alteration, retrieval, consultation, use, disclosure, transmission, dissemination, alignment, combination, blocking, erasure or destruction.

3. Notification

Subject to certain exemptions (see below), the DPA imposes an obligation on Data Controllers to notify the Information Commissioner of certain details relating to the Processing of Personal Data. The DPA makes it a criminal offence to process Personal Data without notification, unless the Data Controller has the benefit of one of the exemptions to notification.

These details will be recorded on a register which can be consulted by the public.

The DPA also requires that a Data Controller notifies the Office of the Information Commissioner of any changes to a register entry within 28 days of the change. Failure to keep a register entry up to date is a criminal offence, although the DPA provides a defence if the Data Controller can show that it exercised all due diligence to comply.

Notifications must be renewed every year. It is an offence for a Data Controller to continue Processing Personal Data if its notification has expired.

The DPA notification system is simpler than the registration system which existed under the 1984 Act. It is no longer necessary to provide detailed information about Processing activities – notification is intended to give an overall picture of the Processing. The Office of the Information Commissioner has produced a Guide to Notification, which is available on the Information Commissioner's website.[1]

Exemptions to Notification

Exemptions are only available in cases where Processing is unlikely adversely to affect the rights and freedoms of the Data Subjects.

The exemptions from notification provided in the DPA and the Notification Regulations made under the DPA include:

- "Relevant Filing Systems", which are defined as paper filing systems;
- Processing for the purposes of staff administration, provided such Personal Data is not disclosed to third parties (unless such disclosure is made with the consent of the staff, or is necessary for the purposes of staff administration);
- Processing for the purposes of advertising, marketing or public relations. Again, this exemption will be lost if the Personal Data is disclosed to third parties without the consent of the Data Subjects;
- Processing of Personal Data in respect of customers and suppliers for the purposes of keeping accounts and records;
- Processing for domestic purposes.

However, even if a Data Controller can enjoy the benefit of an exemption from notification, this does not mean that it is exempt from having to comply with the other provisions of the DPA.

[1] www.dataprotection.gov.uk

4. Data Processors

The DPA distinguishes between a Data Controller and a Data Processor. Data Processors are defined as anyone who processes Personal Data on behalf of the Data Controller, such as outside consultants or auditors.

The Data Processor itself will not have to comply with the obligations of the DPA, but the DPA does require Data Controllers to impose contractual obligations on their Data Processors to ensure the security of Personal Data. If the Data Controller does not ensure that adequate security provisions are in place, it will be in breach of the Seventh Data Protection Principle, which relates to security (see 3.7 above).

In order to comply with the Seventh Principle, the Data Controller must ensure there is a written contract between the Data Controller and Data Processor which requires that the Data Processor will only act on the Data Controller's instructions, and that the Data Processor will comply with the security obligations which the Seventh Principle of the DPA imposes on the Data Controller.

5. The Data Protection Principles

At the heart of the DPA lie eight data protection principles which are set out in Part 1 of Schedule 1 to the DPA. These principles set out the obligations imposed on Data Controllers in respect of the Processing of Personal Data. The DPA imposes a statutory obligation to comply with these principles, and failure to comply could result in enforcement action by the Information Commissioner and/or civil action for breach by the affected Data Subject.

The DPA lists certain exemptions to the various principles which Data Controllers can rely upon in limited circumstances.

The eight principles and permitted exemptions are discussed below:

5.1 The First Principle: Fair and lawful Processing

The first principle is the most important of the data protection principles. It places an obligation on the Data Controller to process Personal Data fairly and lawfully, and prohibits the Processing of any Personal Data unless the Data Controller can justify that Processing under one of the six conditions laid out in Schedule 2 of the DPA.

The six conditions upon which the Data Controller can justify the Processing of Personal Data are:

- the Data Subject has given his consent to Processing (e.g. through completing and returning an application form, or by clicking on an "I accept" box.
- the Processing is necessary for the performance of a contract to which the Data Subject is a party; or for the taking of steps at the request of the Data Subject with a view to entering into a contract (e.g. an application for credit);
- the Processing is necessary for compliance with any legal obligation to which the Data Controller is subject, other than an obligation imposed by a contract (e.g. health and safety matters or money laundering regulations);
- the Processing is necessary in order to protect the vital interests of the Data Subject (this would seem to only apply to life and death type situations);
- the Processing is necessary for the administration of justice, the exercise of statutory functions, government functions or public functions which are in the public interest;
- the Processing is necessary for the purposes of legitimate interests pursued by the Data Controller or by a third party to whom the Personal Data is disclosed except where unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the Data Subject.

Data Protection Notice

The DPA makes it clear that Processing will not be fair unless the Data Subject is also provided with certain information at the appropriate time. The information will usually be given by way of a data protection notice (the "Notice"). The DPA requires that the following information is included in the Notice:

- the identity of the Data Controller (if the Data Controller is a company, this would be its full legal name, not the trading name);
- the purposes for which the data are intended to be Processed;
- any further information which is necessary, such as a general description of the recipients of the data and the purposes for which they will use it, an opt-out of direct marketing, and a description of the Data

Subject's rights to access his Personal Data and correct any inaccuracies to this data.

In order for the Notice to be effective, it must be given at the appropriate time. Different rules apply to the timing of the Notice depending on whether the Personal Data is obtained directly from the Data Subject himself, or from a third party source. If the Personal Data is obtained directly from the Data Subject, the Notice should be provided at the time the Personal Data is obtained (e.g. the Notice can be given on the application form, or on a website through which the Personal Data is obtained). If the Personal Data is obtained by a third party, the Data Controller must ensure that the Notice is given either at the time the Personal Data is processed by the Data Controller, or within a "reasonable period" after the collection of the Personal Data.

Data Controllers may be exempt from the requirement to issue a Notice if the Personal Data has been obtained from a third party and the provision of a Notice would involve a disproportionate effort on the part of the Data Controller. The DPA does not define "disproportionate effort", and it is left to the Data Controller to determine depending on the circumstances. However, the exemption can only apply if the following conditions are satisfied:

- the Data Controller has not received any request for a Notice from the Data Subject;
- the reasons why it would be disproportionate for the Data Controller to give such a Notice have been recorded;
- the recording and disclosure of the Personal Data is necessary for the compliance with a legal obligation to which the Data Controller is subject.

This exemption cannot apply where the Data Controller has obtained the Personal Data directly from the Data Subject.

5.2 The Second Principle: Processing for specified and lawful purposes

The Second Principle states that Personal Data can only be obtained for one or more specified and lawful purposes, and must not be processed any further in a way which is incompatible with that purpose or those purposes.

The Data Controller's registration with the Information Commissioner and Notice will describe the purposes for which the Personal Data will be processed. If the Data Controller goes beyond these purposes, it may be in breach of this principle, and may also be in breach of the first principle as well. The Data Controller can only use the Personal Data for additional purposes if such additional uses would be totally obvious to the Data Subject.

5.3 The Third Principle: Personal Data must be adequate, relevant and not excessive

Personal Data must be adequate, relevant and not excessive for the purposes for which it is Processed. It is for the Data Controller to determine what is adequate, relevant or not excessive in relation to the Processing.

Data Controllers must also ensure that they hold enough Personal Data (without it being excessive) to meet their requirements. For example, if the Data Subject holds an account with the Data Controller, it will be necessary to hold enough Personal Data about the Data Subject in order to identify and verify his identity. Failure to hold sufficient Personal Data about the Data Subject in order to carry out identity checks could be a breach of the third principle in these types of circumstance, because the Personal Data held would not be "adequate". There could also be a breach of the Seventh Principle (see Section 3.7 below).

5.4 The Fourth Principle: Personal Data must be accurate and kept up-to-date

The Fourth Principle places an obligation on Data Controllers to ensure that Personal Data is accurate, and where necessary, kept up to date.

5.5 The Fifth Principle: Personal Data must not be kept for longer than necessary

The Fifth Principle requires that Personal Data processed for particular purposes is not kept for longer than is necessary for those purposes. The DPA does not impose specific time limits in relation to the holding of Personal Data – it is up to the Data Controller to determine how long it is necessary to hold the data. However, there is an exemption to this principle in relation to data held for the purposes of research, history or statistics, which can be

held indefinitely provided certain requirements laid out in the DPA are satisfied.

5.6 The Sixth Principle: Personal Data must be processed in accordance with the rights of Data Subjects

The Sixth Principle requires Personal Data to be processed in accordance with the rights of Data Subjects under the DPA. This principle relates to four specific rights, which the Data Controller will contravene if it fails to:

- provide information in response to a Data Subject access request;
- comply with a justified request to prevent Processing which is causing or will be likely to cause unwarranted damage or distress to the Data Subject or another person;
- comply with a notice to prevent Processing for the purposes of direct marketing;
- comply with a notice objecting to the taking of automated decisions.

The rights of Data Subjects under the DPA are considered further in Section 5 below.

5.7 The Seventh Principle: Measures must be taken against unauthorised or unlawful Processing of Personal Data

The Seventh Principle relates to the secure Processing of Personal Data, and requires that appropriate technical and organisational measures are taken by the Data Controller against unauthorised or unlawful Processing of Personal Data and against accidental loss or destruction of, or damage to, the Personal Data.

Technical measures which could be used include:

- using software controls to restrict access to particular users (i.e. using passwords);
- using technology to authorise and authenticate users;
- ensuring up-to-date virus checking software and firewalls are in place;
- the use of encryption to ensure the integrity and confidentiality of data.

Organisational measures which could be used include:

- restricting access to buildings, computer rooms, desks, equipment and other facilities;
- training staff on the care and handling of Personal Data;
- ensuring a business continuity plan is in place in order to maintain business functions in event of a disaster.

The technical and organisational measures which should be taken by the Data Controller in order to comply with the Seventh Principle need to be commensurate with the type of Personal Data which is being processed, the potential for disclosure, and the harm which would result from the breach of security. If the Personal Data is sensitive or confidential, a relatively higher level of technical or organisational measures will be required to safeguard the data.

The Seventh Principle also imposes obligations on Data Processors regarding the security of Personal Data, which are considered in Section 8 below.

5.8 The Eighth Principle: Transfers of Personal Data to a Country or Territory outside the EEA

The Eighth Principle prohibits the transfer of Personal Data to a country or territory outside of the EEA unless that country or territory ensures an adequate level of protection for the rights of Data Subjects in relation to the Processing of Personal Data.

The Eighth Principle will only apply to transfers of Personal Data to the non-EEA country where the Processing of the data will take place. It will not apply where Personal Data passes through a country in transit to the ultimate country where the Processing will take place.

It is the Data Controller's responsibility to determine the adequacy of the level of protection in a particular country or territory outside the EEA. The factors the Data Controller should consider in making this decision are:

- the nature of the Personal Data which is to be transferred;
- the country of origin;

- the country of final destination (certain countries and organisations outside the EEA will be deemed to provide an adequate level of protection);
- the purposes for which and period during which the Personal Data is intended to be Processed;
- the law in force in the country or territory in question;
- the international obligations of that country and territory;
- any relevant codes of conduct or other rules which are enforceable in that country or territory (such as the Safe Harbor Rules – see below); and
- any security measures taken in respect of the Personal Data in that country or territory.

The European Commission has adopted a decision which states that Switzerland, Hungary and Canada provide an adequate level of protection, and further countries are expected to be approved in the future. There will also be a presumption that an adequate level of protection is in place for the purposes of the Eighth Principle if the organisation in a non-EEA country subscribes to the "Safe Harbor" Rules. At the moment, these Rules only apply to a limited number of US entities, and a business transferring data to the US (which is deemed not to have laws which provide an adequate level of protection) will have to check whether the organisation to which the data will be transferred has subscribed to the Safe Harbor Rules.

Also, if appropriately drafted, contracts governing data transfers between two organisations may give rise to a presumption of adequacy. The European Commission has recently approved a set of standard contractual clauses for the transfer of Personal Data to third (i.e. non EEA) countries. If Personal Data is transferred under a contract which includes these standard clauses, and the parties comply with these clauses, the transfer will be adequately protected.

Exemptions to the Eighth Principle

The DPA contains a number of exemptions from the obligations of the Eighth Principle. If any of these exemptions apply, a Data Controller can transfer Personal Data to any country or territory in the world, irrespective of whether the country or territory to which the Personal Data is transferred provides an adequate level of protection. The exemptions apply if:

- the Data Subject has consented to the transfer. Guidance issued by the Office of the Information Commissioner (OIC) makes it clear that such consent must be freely given, specific and informed. The Data Subject must know and have understood what he is agreeing to. The reasons for the transfer and, as far as possible, the countries to which the Personal Data will transferred to should be specified. Any particular risks associated with the transfer should also be brought to the Data Subject's attention. A higher level of consent is required for the transfer of sensitive Personal Data (see Section 4 below);
- The transfer is necessary for the performance of the contract between the Data Subject and the Data Controller or for the taking of steps at the request of the Data Subject with the aim of entering into a contract with the Data Controller (e.g. the transfer of Personal Data abroad pursuant to an employment contract which entails service overseas); or
- The transfer is necessary for the conclusion of a contract between the Data Controller and a person other than the Data Subject which is entered into at the request of the Data Subject, or for the performance of such a contract; or
- The transfer is necessary for reasons of substantial public interest; or
- The transfer is necessary for the purpose of, or in connection with, any legal proceedings, including prospective legal proceedings; is necessary for the purpose of obtaining legal advice; or is otherwise necessary for the purposes of establishing, exercising of defending legal rights; or
- The transfer is necessary in order to protect the vital interests of the Data Subject; or
- The transfer is of part of the Personal Data on a public register and any conditions subject to which the register is open to inspection are complied with by any person to whom the Personal Data is or may be disclosed after the transfer; or
- The transfer is made on terms which are of a kind approved by the Information Commissioner as ensuring adequate safeguards of the rights and freedoms of Data Subjects; or

- The transfer has been authorised by the Information Commissioner as being made in such a manner as to ensure adequate safeguards of the rights and freedoms of Data Subjects.

For further discussion on the Eighth Principle see our briefing paper 'Regulation of Transborder Data Flows'.

6. **Sensitive Personal Data**

The DPA introduces stricter conditions which Data Controllers must comply with in order to process sensitive Personal Data.

Sensitive Personal Data is defined as Personal Data which consist of information as to the Data Subject's:

- racial or ethnic origin;
- political opinions;
- religious or spiritual beliefs;
- membership of a trade union;
- physical or mental health;
- sexual life;
- commission or alleged commission by him of any offence; and
- any proceedings for any offence committed or alleged to be committed by him, the disposal of such proceedings, or the sentence of any court in such proceedings.

If the Data Controller processes sensitive Personal Data, it must, in addition to the six conditions regarding the fair and lawful Processing of Personal Data laid out in Schedule 2 of the DPA justify the Processing of sensitive Personal Data on the basis of one or more of the further conditions laid out in Schedule 3 of the DPA These conditions are as follows:

- the Data Subject has given his explicit consent to the Processing of the sensitive Personal Data. The Information Commissioner has provided some guidance as to what "explicit" consent means, stating that such consent must be absolutely clear – i.e. the Data Subject must actively opt-in to the Processing to give consent. Simply providing an opt-out on a form or website will not be enough to obtain consent to lawfully process sensitive Personal Data. Also, to obtain explicit consent, the Data Controller will have to provide the Data Subject with a more detailed description of the Processing, the type of Personal Data which will be processed, and to whom the Personal Data will be disclosed;
- the Processing is necessary for the purposes of exercising or performing any right or obligation conferred or imposed by law on the Data Controller in connection with employment (e.g. the Processing of data regarding accidents or injuries at work which may be required under health and safety legislation);
- the Processing is necessary to protect the vital interests of the Data Subject;
- the Processing is carried out by a non-profit making body which exists for political, philosophical, religious or trade union purposes and relates only to members of that body (or those having regular contact with that body) and does not involve disclosure of the Personal Data to third parties without the Data Subject's consent;
- the information contained in the Personal Data has been made public as a result of actions taken by the Data Subject himself;
- the Processing is necessary for the purposes of actual or prospective legal proceedings, for the purposes of obtaining legal advice, or for the purposes of establishing, exercising or defending legal rights;
- the Processing is necessary for the administration of justice, the exercise of statutory functions, or the exercise of government functions;
- the Processing is necessary for medical purposes undertaken by a health professional or other person under an equivalent obligation of confidentiality;
- the Processing is necessary for the purpose of ensuring equality of treatment in respect of persons of different racial or ethnic origin, religious beliefs, or different physical or mental conditions, provided that such Processing is for the purpose of enabling such equality to be promoted or maintained.

In addition to the Schedule 3 conditions above, the Data Protection (Processing of Sensitive Data) Order 2000 provides further conditions which can be used to justify the Processing of sensitive Personal Data. They cover the Processing of sensitive Personal Data for the purposes of:

- preventing or detecting any unlawful act;

- discharging functions which protect members of the public from certain improper conduct, such as incompetence or mismanagement;
- providing confidential counselling, advice or support;
- carrying on insurance business or administering occupational pensions schemes;
- carrying on political activities by registered political parties;
- research, including statistical and historical purposes;
- exercising functions conferred on constables by law.

7. Data Subject Access Rights

The DPA has significantly increased the rights Data Subjects have in respect of the Processing of their Personal Data, particularly regarding their rights of access to their Personal Data. Compliance by the Data Controller with these rights of access is an obligation under the Sixth Data Protection Principle.

Under Section 7 of the DPA a Data Subject has the right to be informed by the Data Controller whether his Personal Data is being processed by or on behalf of that Data Controller. If the data is being Processed, the Data Subject has the right to be given a description of:

- the Personal Data which relates to him;
- the purposes for which the data is to be processed;
- the recipients or classes of recipients to whom this data is or may be disclosed.

The Data Subject also has the right to have communicated to him:

- the information constituting the Personal Data which relates to him: unless it would be a disproportionate effort for the Data Controller, or the Data Subject agrees otherwise, this information must be provided in a permanent form;
- any information available to the Data Controller as to the source of the data – although the Data Controller should not disclose the identity of another individual, unless this individual has consented or it is reasonable in all the circumstances to disclose the individual's identity without his consent.

This information should be communicated to the Data Subject in an intelligible form.

The Data Subject's access rights are not absolute, and are subject to a number of conditions and exemptions. There will be no obligation for the Data Controller to respond to an access request unless:

- the access request is made in writing (this can include email);
- the individual has paid a relevant fee, if any (which is subject to a maximum amount of £10);
- enough information has been supplied with the request to satisfy the Data Controller as to the identity of the person making the request. If these conditions are satisfied, the Data Controller must comply with the request within 40 days of its receipt.

8. Direct Marketing

Under Section 11 of the DPA a Data Subject has the right to prevent the Processing of his Personal Data for direct marketing purposes. Data Subjects have the right to give notice in writing to the Data Controller requiring the Data Controller to stop the Processing of Personal Data for such purposes.

"Direct Marketing" is defined as the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals. This definition includes telemarketing, mail shots, canvassing and emails, but would not include leaflets or letters which are not directed to particular named individuals.

There are no permissible exemptions to the provisions of Section 11 of the DPA.

9. Automated Decision-Making

Under Section 12 of the DPA a Data Subject has the right to require a Data Controller to ensure that no significant decision taken by the Data Controller will be based solely on the automated Processing of the Data Subject's Personal Data for the purposes of evaluating matters relating to him, such as his performance at work or creditworthiness.

There are a number of exemptions to this right, which apply when the decision to Process the Personal Data through solely automated means is:

- taken for the purposes of considering whether to enter into a contract with the Data Subject, or with a view to entering into such a contract, or in the course of performing such a contract;
- authorised or required by or under any enactment; or
- the effect of the decision is to grant a request of the Data Subject.

If any of these exemptions apply, the Data Subject will be prevented from objecting to the automated decision making.

If any of these exemptions do not apply, and the automated decision has already been taken, the Data Controller should inform the Data Subject of this fact. The Data Subject is then entitled to serve notice on the Data Controller within 21 days requiring it to reconsider the decision, or make a new decision on a non-automated basis. The Data Controller must respond to this notice within 21 days, informing the Data Subject of the steps it intends to take to comply with this notice. If the Data Controller believes the decision taken did not substantially affect the Data Subject, the Data Controller can decide not to comply with the notice.

If the automated decision has not yet been taken, the Data Controller has the discretion to decide whether the decision is likely to significantly affect the Data Subject, and whether the decision will be taken as the sole basis of evaluating the Data Subject. The Data Controller should then respond to the Data Subject's notice, informing him of the steps he intends to take in response to the request. If the Data Controller believes the Data Subject's request is not warranted, it should explain the reasons why it has reached this view.

If the Data Subject is unsatisfied with the action taken by the Data Controller pursuant to his request, he can ask the courts to make an order requiring the Data Controller to reconsider the decision, or make a new one which is not based solely on automated Processing.

In addition, Data Subjects also have the right to be informed by the Data Controller of the logic involved in any automated decision which affects them.

10. Enforcement and Sanctions

The Information Commissioner's powers of enforcement are wide, and can be exercised against any person who contravenes the DPA, irrespective of whether such a person is a Data Controller under the DPA.

The procedure for enforcement for breach of the DPA is as follows:

10.1 The Request for Assessment

Any person who believes himself to be affected directly by the Processing of Personal Data may make a request to the Information Commissioner for an assessment as to whether such Processing is being carried out in compliance with the DPA. This is therefore the way in which such a person could make a complaint to the Information Commissioner regarding the Processing of Personal Data which affects him.

The Information Commissioner is obliged to make an assessment if requested to do so.

10.2 The Information Notice

Following a request for assessment (or otherwise in order to check compliance with the DPA), the Information Commissioner may serve an Information Notice on the Data Controller. The Information Notice will require the Data Controller to provide specific information within a specified time and in a specified manner. A Data Controller does have a right of appeal to the Data Protection Tribunal against an Information Notice.

10.3 The Enforcement Notice

Following inspection of the information supplied by the Data Controller pursuant to the Information Notice, if the Information Commissioner is satisfied that the Data Controller is in contravention of any of the data protection principles, the Information Commissioner may serve an Enforcement Notice on the Data Controller which may require it to:

- take the steps laid out in the Enforcement Notice within any time period specified; and/or
- stop Processing any Personal Data for a particular purpose or in a particular manner within any time specified in the Enforcement Notice.

It is a criminal offence to fail to comply with the provisions of an Enforcement Notice.

A Data Controller does have the right of appeal to the Data Protection Tribunal if served with an Enforcement Notice. If an appeal is made, the Enforcement Notice will be suspended until the determination or withdrawal of the appeal.

10.4 Information Commissioner's Powers of Entry and Inspection

The DPA gives powers of entry and inspection to Officers of the Information Commissioner if the Information Commissioner believes that there are reasonable grounds for suspecting that:

- a Data Controller has contravened or is contravening any of the data protection principles; or
- an offence under the DPA has been or is being committed; and
- that evidence of the contravention or offence will be found on the premises of the Data Controller.

The Information Commissioner may apply for a search warrant if these conditions are met to enter the premises, search them, inspect, operate, examine and test any equipment on these premises which is used or intended to be used for the Processing of Personal Data, and to inspect and seize any documents which may be evidence of the contravention or offence.

11. Civil Actions for Non-Compliance with the DPA

In addition to the enforcement actions by the Information Commissioner, a Data Controller can face a civil action from an affected Data Subject if the Data Controller fails to comply with the data protection principles or any of the other requirements of the DPA. If the non-compliance causes damage to the Data Subject he will be entitled to compensation from the Data Controller. In addition, the DPA allows for compensation for distress caused by the non-compliance if accompanied by damage to the Data Subject. Other individuals such as the family members of a Data Subject who have been affected by the non-compliance may also be entitled to compensation.

If you would like to discuss any aspects of business or financial services regulation please contact:

- *John Casanova, Partner, Tel +44 (0) 20 7360 3739*
- *William Long, Associate, Tel +44 (0) 20 7778 1865*
- *Susan Atkinson, Associate, Tel +44 (0) 20 7778 1869*

Sidley Austin Brown & Wood
1 Threadneedle Street
London EC2R 8AW
Tel: +44 (0) 20 7360 3600
Fax: +44 (0) 20 7626 7937
www.sidley.com

ALL PARTNERS ARE EITHER SOLICITORS OR REGISTERED FOREIGN LAWYERS