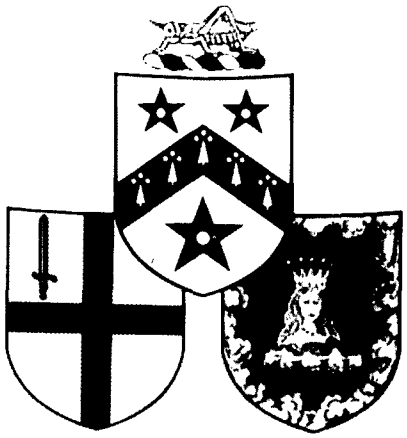
G R E S H A M

C O L L E G E



THE INTERNET AND ELECTRONIC COMMERCE

Lecture 5

ELECTRONIC COMMERCE: NEW DATA PROTECTION LAW

by

PROFESSOR GERALD WAKEFIELD BSc LLB DipLaws DipMet FRSA
Gresham Professor of Law

2 March 1999

GRESHAM COLLEGE

Policy & Objectives

An independently funded educational institution, Gresham College exists

- to continue the free public lectures which have been given for 400 years, and to reinterpret the 'new learning' of Sir Thomas Gresham's day in contemporary terms;

- to engage in study, teaching and research, particularly in those disciplines represented by the Gresham Professors;

- to foster academic consideration of contemporary problems;

- to challenge those who live or work in the City of London to engage in intellectual debate on those subjects in which the City has a proper concern; and to provide a window on the City for learned societies, both national and international.

Gresham College, Barnard's Inn Hall, Holborn, London EC1N 2HH
Tel: 0171 831 0575 Fax: 0171 831 5208
e-mail: enquiries@gresham.ac.uk

NEW DATA PROTECTION LAW FOR THE UK

IMPLEMENTING THE EU DATA PROTECTION DIRECTIVE

The Data Protection Act 1984 is 'an act to regulate the use of automatically processed information relating to individuals and the provision of services in respect of such information'. However, the Act has its origins in the Council of Europe Convention on Data Protection ('Treaty 108'), and through this in the Council of Europe Convention on Human Rights ('the European Human Rights Convention'). Article 1 of Treaty 108 sets ou the objective. 'The purpose of this convention is to secure...for every individual...respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him...'.

The EU Data Protection Directive (95/46/EC) was adopted on 24th October 1995. EU member states are required to have in place by 24th October 1998 national provisions giving effect to this Directive.

The new UK Data Protection Act ("the Act") 1998, which will implement the 1995 Data Protection Directive was given royal assent on 16 July 1998.

The Directive is in substance very similar to the Data Protection Act 1984, and at least 80 per cent of the compliance with the new act flows from complying with the Data Protection Act 1984. However the Directive goes further than the 1984 act .
Specifically, it:

- Re-defines some key concepts;
- Extends to certain manual records;
- Sets conditions for processing Personal Data;
- Sets tighter conditions for processing Sensitive Data;
- Requires specific exemptions for the media;
- Strengthens the rights of the individual;
- Strengthens the power of the regulatory authority;
- Sets new rules for Personal Data transfer outside the EU;
- Simplifies the existing registration scheme to one of *notification*.

It should be noted however that there is at least a three year transitional period (longer for existing manual records) during which time relief from certain obligations is given thus allowing time for commerce and industry to build up compliance into the new systems.

First, Some Definitions

"Personal Data" remains data relating to *living individuals* who can be identified from the data, or from those data and other information which is, or is likely to come into the possession of the **data controller**. It includes any expression of opinion about the individual and any indication of the intentions of the **data controller** or any other person in respect of the individual (section 1(1)).
This definition extends that of the 1984 Act by including information which is *in or likely to come into* the **data controller**'s possession, so that information held separately within an organisation where a **data controller** may have access to it, would be caught by the Act.

From an HR perspective, information held on personnel files as to an employer's intentions vis a vis an individual employee is now within the scope of the Act (was previously excluded), although there may be limitations on the **data subject**'s access rights to such information, as are expressions of opinion on the **Data Subject** (see **Data Subject** Rights below).

Although data which is not about living individuals but about companies, for example, is not explicitly covered, details about individuals held in the context of corporate mailing lists would be covered by being "processed" under the Act.

However, if an individual name is utilised only to enable a mailing to reach its intended goal within the recipient organisation, it is unlikely to be viewed by the Data Protection Commissioner as giving rise to cause for concern, unless in exceptional circumstances, and may in any event constitute Personal Data given some transitional relief as a 1984 Act exemption until October 2001

The new definition of "**Processing**" is much wider than the previous one and the previous restriction where processing had to take place "by reference to the **data subject**" has now gone. This distinction with the 1984 Act will be an important one in the new widened definition but its effect will not be felt immediately because "processing by reference to the **data subject**" will continue to apply as a restriction until October 2001 under the transitional relief provisions in Schedule 8.

"Processing" now covers *all* activities in relation to Personal Data, including any use of the data in correspondence, or by email. The previous exemption for the processing of Personal Data for preparing the text of documents has now gone. The significance of this is that subject access rights may now apply to all electronically held documents, emails and the like where the Personal Data can be electronically searched for. The **Data Subject** however has to be able to satisfy the **data controller** as to the location of the information sought (Section 7(3)) as well as complying with the other requirements for valid access requests.

Self-evidently a **Data controller** is by Section 1(1) 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.

Description of personal data (DATA CLASS);

Personal identifiers
Financial identifiers
Identifiers issued by public bodies
Personal details
Personality, character
Current marriage or partnership
Details of other family, household members
Other social contacts
Immigration status
Academic record
Qualifications and skills
Membership of professional bodies
Professional expertise
Publications
Current employment
Recruitment details
Termination details
Career history
Payments, deductions
Work management details

Work assessment details
Income, assets, investments
Pension details

http://www.dpr.gov.uk/sample.html

THE DATA PROTECTION ACT 1998

Processing of Personal Data

The Act ensures continuity with the Data Protection Act 1984 by incorporating and updating the eight Data Protection Principles. It should be noted that unlike in the 1984 Act, these Data Protection Principles may now be enforced even against unregistered users of Personal Data.

Schedule 1 sets out the **Data Protection Principles** as follows:

1. Personal Data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

   (a) At least one of the conditions in Schedule 2 is met.

   Schedule 2

   Conditions Relevant for Purposes of the First Principle: Processing of any Personal Data

   (i) The **data subject** has given his consent to the processing.

   (ii) The processing is necessary-

   (a) for the performance of a contract to which the **data subject** is a party, or

   (b) for the taking of steps at the request of the **data subject** with a view to entering into a contract.

   (iii) The processing is necessary for compliance with any legal obligation to which the **data controller** is subject, other than an obligation imposed by contract.

   (iv) The processing is necessary in order to protect the vital interest of the **data subject**.

   (v) The processing is necessary-

   (a) for the administration of justice;

   (b) for the exercise of any functions conferred on any person by or under any enactment;

   (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or

   (d) for the exercise of any other functions of a public nature exercised in the public interest by an person.

   (vi) The processing 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 an particular case by reason of prejudice to the rights and freedoms or legitimate interests of the **data subject**.

The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

(b) In the case of Sensitive Personal Data, at least one of the conditions in Schedule 3 (conditions relevant to processing of Sensitive Personal Data) is also met.

In this Act "sensitive personal data" means personal data consisting of information as to-

(a) the racial or ethnic origin of the data subject,

(b) his political opinions,

(c) his religious beliefs or other beliefs of a similar nature,

(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation Act 1992),

(e) his physical or mental health or condition,

(f) his sexual life,

(g) the commissions or alleged commission by him of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Schedule 3

Conditions Relevant for Purposes of the First Principle: Processing of Sensitive Personal Data

(i) The **data subject** has given his explicit consent to the processing of the personal data.

(ii) (1)The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the **data controller** in connection with employment.

(2)The Secretary of State may by order –

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

(iii) The processing is necessary-

(a) in order to protect the vital interests of the **data subject** or another person, in a case where-

(1) consent cannot be given by or on behalf of the **data subject**, or

(2) the **data controller** cannot reasonably be expected to obtain the consent of the **data subject**, or

(b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the **data subject** has been unreasonably withheld.

(iv) The processing-

(a) is carried out in the course of its legitimate activities by any body or association which-

(1) is not established or conducted for profit, and

(2) exists for political, philosophical, religious or trade-union purposes,

(b) is carried out with appropriate safeguards for the rights and freedoms of **data subject**s,

(c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and

(d) does not involve disclosure of the personal data to a third party without the consent of the **data subject**.

(v) The information contained in the personal data has been made public as a result of steps deliberately taken by the **data subject**.

(vi) The processing-

(a) is necessary for the purpose of , or in connection with, any legal proceedings,

(b) is necessary for the purpose of obtaining legal advice, or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

(vii) (1)The processing is necessary-

(a) for the administration of justice,

(b) for the exercise of any functions conferred on any person by or under an enactment, or

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

(2)The Secretary of State may by order-

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

(viii) (1)The processing is necessary for medical purposes and is undertaken by-

(a) a health professional, or

(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2)In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

(ix) (1)The processing-

(a) is of sensitive personal data consisting of information as to racial or ethnic origin,

(b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and

(c) is carried out with appropriate safeguards for the rights and freedoms of **data subject**s.

(2)The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of **data subject**s.

(x) The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph

Both these Schedules mean that fair and lawful processing is a higher obligation to fulfil than previously. Without the **Data Subject's** consent, the processing must comply with a Schedule 2 purpose. The issue of **Data Subject** consent will be an important one where the other conditions do not apply, for example where there is no contractual relationship with a **Data Subject** and the data is collected for direct marketing, or is supplied within a group of companies for such purposes.

Note also that there are now specific provisions for the treatment of Sensitive Data, which includes union membership, an individual's physical/mental condition, criminal record and ethnicity. A **Data Subject** has to give "explicit" consent before such data can be processed or at least one Schedule 3 specified purpose has to apply

2. Personal data shall be obtained only for one of more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose of purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or for those purposes.

6. Personal data shall be processed in accordance with the rights of **data subjects** under this Act.

7. Appropriate 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.

8. The Personal 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.

Schedule 4

Cases where the Eighth Principle does not apply

(i) The **data subject** has given his consent to the transfer.

(ii) The transfer is necessary-

(a) for the performance of a contract between the **data subject** and the **data controller**, or

(b) for he taking of steps at the request of the **data subject** with a view to his entering into a contract with the **data controller**.

(iii) The transfer is necessary-

(a) for the conclusion of a contract between the **data controller** and a person other than the **data subject** which-

(1) is entered into at the request of the **data subject**, or

(2) is in the interests of the **data subject**, or

(b) for the performance of such a contract.

What data constitutes Personal Data has been extended by the Act beyond information processed by computer and recorded with the intention that it should so be processed, to now include information recorded as part of a **"relevant filing system"**, the extension to **manual records**.

Although existing manual files will not need be covered by the Act until 2007, those created after 24 October 1998 will be subject to individual access rights.

A "**relevant filing system**" (section 1(1)) means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

This will include paper based files holding Personal Data where these are structured so as to allow ready access to particular information about individuals, but what will be caught as a "relevant filing system" is currently open to interpretation.

If the relevant filing system, such as a card index system, is structured as to the location of the personal information it is likely to fall within the Act, but a correspondence file albeit containing personal information, would not be so caught. The maintenance of existing manual files will eventually become subject to the Act and hence the Data Protection Principles. New manual files will need to be established and maintained in accordance with the requirements of the Act, or where practical to do so, set up in such a way as to fall outside the Act.

Technical measures for Data Security

The **Seventh Principle** requires that appropriate technical and organisational measures should be taken against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data.

New rules for the interpretation of the Seventh Principle are set out in Part II of Schedule 1.

'With regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to:

(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage, and

(b) the nature of the data to be protected.

The **data controller** must take reasonable steps to ensure the liability of any employees of his who have access to the Personal Data.'

Where processing of Personal Data is carried out by a **Data Processor** on behalf of a **data controller**, the **data controller** must in order to comply with the Seventh Principle:

(a) choose a **Data Processor** providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and

(b) take reasonable steps to ensure compliance with those measures.

Where processing of Personal Data is carried out by a **Data Processor** on behalf of a **Data Controller**, the **data controller** is not be regarded as complying with the Seventh Principle, unless:

(a) the processing is carried out under a contract which is made or evidenced in writing, and under which the **Data Processor** is to act only on instructions from the **data controller**, and

(b) the contract requires the **Data Processor** to comply with obligations equivalent to the imposed on the **data controller** by the Seventh Principle.

It is necessary therefore to enter into *formal contractual relationships* with **Data Processors** in the terms required, whether such entities are part of the same group of companies or not, and such contracts must provide that the **Data Processor** complies with the terms of the Seventh Principle in respect of the subject matter of the agreement. Note also that in the *choosing* of the **Data Processor**, steps should be taken to obtain the sufficient guarantees as to technical and organisational security measures that are required under the Seventh Principle.

Transferring Data to Third Countries

Principle 8 of the Data Protection Act deals with the issue of trans-border data flows. This is one of the most important and contentious issues. Interpretation of this Principle may be found in Part II of Schedule 1, which outlines points to consider when determining adequacy, but states that adequate protection of data may not be required where certain criteria, set out in Schedule 4, are satisfied.

Part II of Schedule 1, paragraph 13 states that *an adequate level of protection* is one which is adequate in all the circumstances of the case, having regard in particular to:

1. The nature of the Personal Data;
2. The country or territory of origin of the information contained in that data;
3. A country or territory or final destination of that information;
4. The purposes for which and period during which the data are intended to be processed;
5. The law in force in the country or territory in question;
6. The international obligations of that country or territory;
7. Any relevant codes of conduct or other rules which are enforced in that country or territory; and
8. Any security measures taken in respect of the data in that country or territory.

However if the criteria, as set out in Schedule 4, are satisfied the Principle does not apply.

Schedule 4 outlines cases where the 8 Principles do not apply. These include:

1. The **data subject** has given his consent to the transfer;
2. The transfer is necessary for contractual reasons;
3. The transfer is necessary for reasons of substantial public interest.
4. For the transfer of any legal proceedings or the purposes of obtaining legal advice.
5. The transfer is necessary in order to protect the vital interest of the **data subject**.
6. The transfer is part of Personal Data on a public register.
7. The transfer is approved by the Commissioner as ensuring adequate safeguards.
8. The transfer has been authorised by the Commissioner.

Manual Records

The 1984 Act did not cover manual records. However Article 2 of the Directive 95/46/EC states that *"Personal Data shall mean any information relating to an identified or identifiable natural person"*. However the Article 32(2) of the Directive allows a member state to provide that the processing of data *already* held in manual filing systems need not be brought into conformity with Articles 6, 7 and 8 until 2007. These articles set out the principles relating to data quality, criteria for making data processing legitimate, and the basis on which special categories of data may be processed. This is covered in the 1998 Act by Part II of Schedule 8.

Enforcement

A significant difference between the 1984 Act and the 1998 Act is that whilst the Registrar under the 1984 Act could not enforce the Data Protection Principles against those who are exempt from registration, the Commissioner under the 1998 Act will be able to enforce the Principles, which remain largely the same, against those who are exempt from notification.

Notification

Part III of the Act requires notification by **data controller**s and, subject to the general exemptions under the Act by section 17, it is an offence to process Personal Data without an entry in respect of the **data controller** included in the register maintained by the Commissioner of Data Protection (as the Registrar is now called).

The "**registrable particulars**" include a description of the Personal Data being, or to be processed, by or on behalf of the **data controller** and of the category, or categories, of **data subject** to which they relate, together with a description of their purpose or purposes for which the data are being or are to be processed. The particulars also include a description of any recipient or recipients to whom that **data controller** intends or may wish to disclose the data and the names or descriptions of any countries or territories outside the EEA to which the **data controller** directly or indirectly transfers, or intends or may wish directly or indirectly transfer, the data.

In addition, notification is required of a general description of measures to be taken for the purpose of complying with the Seventh Principle as to appropriate technical and organisational measures against unlawful or unauthorised use of Personal Data.

Under the transitional relief given by Schedule 8, manual records in existence and processed at 24 October 1998 will not require notification by way of registrable particulars.

By section 20, **data controller**s must continue to notify the Commissioner of any changes to the substance of their registration such that it remains up to date.

Media Exemptions

There are no exemptions for journalist, publishers and broadcasters, who are therefore under duties to obtain and process data fairly and lawfully, grant subject accesses and to comply with the other requirements of the 1998 Act. Article 9 of the EU Directive authorises exemptions for Personal Data processing for journalistic, artistic literary purposes so far as is

necessary to reconcile personal privacy with freedom of expression. But the new law will have to reflect the European Convention on Human Rights which the government plans to incorporate into UK law. If the right balance between respected private life and the right of freedom of expression is not achieved, the courts will be able to comment adversely on the new law either because there is too much privacy or because there is not enough.

The Act gives exemptions by Section 32 for processing for (a) the purposes of journalism, (b) artistic purposes and (c) literary purposes.

Data Subject Rights

Part II of the Act sets out the rights of **data subject**s and others which are expanded in some important respects.

As before, an individual is entitled to be informed by any **data controller** whether Personal Data of which that individual is the **data subject**, are being processed by or on behalf of that **data controller** and where this is the case, to be given a description of any Personal Data held, the purposes for which they are being or are to be processed, and the recipients to whom they are or may be disclosed.

More importantly for many organisations, an individual is entitled to have communicated to him in intelligible form the information constituting any of his Personal Data and any information available to the **data controller** as to the source of those data. This latter provision will mean putting in place a system whereby sources of data are either to be included or excluded at the time of compilations. If there is any source information held, it must be made available.

An individual is also entitled to be informed by the **data controller**, of the logic involved in any decision taking where the processing by automatic means of that individual Personal Data is for the purpose for evaluating matters relating to him, including performance at work and his reliability or conduct, and the processing has constituted or has likely to constitute the *sole* basis for any decision significantly affecting him. (Section 7(1)d). This provision will be particularly relevant to organisations utilising automated credit referencing. The extent of what constitutes "the logic" involved in such decision making is likely to require a general description only of how the automatic system might work. Trade secrets would not require such description.

There are detailed provisions in the Act for the making of the subject access requests and for requests which require disclosing information relating to another individual who can be identified from the information requested.

There are also detailed provisions whereby individuals can prevent certain processing of types of data if it is used in making automated decisions, used for direct marketing purposes or if it is likely to cause damage or distress.

Schedule 7

Miscellaneous Exemptions

(i) Confidential references given by the **data controller**.

(ii) Armed forces

(iii) Judicial appointments and honours

(iv) Crown employment and Crown or Ministerial appointments.

(v) Management forecasts etc.

(vi) Corporate finance

(vii) Negotiations

(viii) Examination marks

(ix) Examination scripts etc.

(x) Legal professional privilege

(xi) Self-incrimination

NEXT STEPS - AN ACTION PLAN TO COMPLY WITH THE NEW REQUIREMENTS

It is considered that individual organisations both large and small will be well advised to establish a data protection compliance programme. The plan following is a basic framework for setting up a relevant procedure.

1. Recognise the new data protection requirements, establish a procedure for creating manual files and if within the Act – a methodology for granting subject access rights.

2. Establish a senior executive post to oversee and progress a programme of compliance which informs relevant employees of the new law, the Data Protection Principles and their practical consequences.

3. Audit manual and computer database systems which store Personal Data.

4. Establish procedures for advising **data subject**s of the use of their data.

5. Amend terms and conditions on which data is obtained.

6. Amend terms and conditions on which data is processed by a third party.

7. Establish security arrangements.

8. Consider implications and permissibility of transborder data flow outside the UK.

Relevant papers

The following papers may be accessed via the Internet:

- Data Protection Act 1998 - http://www.parliament.the-stationery-office.co.uk
- Government's proposals - http://www.homeoffice.gov.uk
- EU Directive (95/46/EC) - http://www2.echo.lu/legal
- Data Protection Act 1984 - http://www.open.gov.uk

ICC GUIDELINES FOR COMMITMENTS ON PRIVACY PROTECTION BY ACCESS PROVIDERS AND WEBSITE OPERATORS

Undertakings of Access Providers and Website Operators

1. Collection Undertaking

An Access Provider or Website Operator will not gather personal data about an identifiable Customer, including information concerning the on-line activities of Customer, unless one of the following applies:

(i) the data is necessary to complete invoicing requirements; or,

(ii) the data is necessary to fulfil an obligation imposed by a law to which the Access Provider or Website Operator is subject; or,

(iii) the data is necessary to fulfil the Access Provider's obligations to its Customer as clearly articulated in their agreement for provision of service; or

(iv) the Access Provider or Website Operator clearly informs the Customer he may do so, explaining by what means and for what purpose he will do so, and clearly and unambiguously sets forth a means by which the Customer may, at no cost to himself, object to such collection, and the Customer has not so objected.

2. Data Quality Undertaking

Where an Access Provider or Website Operator gathers Customer-identified personal data, such data shall be relevant to the legally-required or otherwise consented purpose for which they are used, and, to the extent necessary for those purposes, will be accurate, complete and kept up-to-date.

3. Purpose Specification Undertaking

The Access Provider or Website Operator shall in all cases, even those where legally-required to gather personal data, specify the purposes for which data are collected, doing so not later than the time of collection. The Access Provider or Website Operator will limit subsequent use thereof to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use Limitation Undertaking

The Access Provider or Website Operator shall not disclose, make available or otherwise use personal data for purposes other than those it has previously specified, except with the consent of the Customer or as required by law.

5. Security Safeguards Undertaking

The access Provider or Website Operator will protect the personal data contained by them against risk of loss, unauthorised access, destruction, use, modification or disclosure.

6. Openness Undertaking

The Access Provider or Website Operator shall establish and communicate to a Customer on request its developments, practices, and policies with respect to personal data. The Access Provider or Website Operator will establish means for Customers and other s to determine the existence and nature of personal data in their control, the main purposes of their use, as well as the Access Provider's or Website Operator's identity and the physical location of their business premises.

7. Individual Participation Undertaking

Access Provider and Website Operator undertake that Consumers have the following rights:

(a) to be informed whether or not Access Provider or Website Operator has data relating to such Consumer;

(b) to obtain from Access Provider or Website Operator any data relating to such Consumer:

  (i) within a reasonable time;

  (ii) at no charge;

  (iii) in a reasonable manner, such as by e-mail;

  (iv) in a readily intelligible form;

(c) to be given reasons if a request lodged under a. or b. above is denied;

(d) to provide a Consumer a means of challenging such denial, such as by informing the Consumer of any available arbitration mechanism, internal company appeal mechanism, or self-regulatory body dispute settlement mechanism.

(e) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

8. Accountability Undertaking

Access Provider of Website Operator undertake to authorize periodic qualified third-party verification of its observance of the undertakings herein.

9. Consumer Empowerment Undertaking

Access Provider undertakes to provide its Customers from time-to-time with technological tools enabling them to control, limit, or deny access through the Customer's computer to categories of websites which Customers may select. Website Operator undertakes to include in its website those elements which enable such tools to operate effectively, or take such other steps as will enable Customers to exercise such control with respect to its website.

10. Transborder Data Transfer ndertaking

Access Provider and Website Operator undertake to incorporate the warranties and undertakings set out in the ICC Guidelines for Contractual Undertakings Regarding Transborder Data Flows when they are engaged in such activities.