BEIJING
CHICAGO
DALLAS
GENEVA
HONG KONG
LONDON
LOS ANGELES
NEW YORK
SAN FRANCISCO
SHANGHAI
SINGAPORE
TOKYO
WASHINGTON, DC

SIDLEY AUSTIN BROWN & WOOD
AND AFFILIATED PARTNERSHIPS

PRIVACY POLICIES

April 2003

ONLINE COLLECTION OF PERSONAL DATA

Most organisations that conduct their business online will collect data relating to individuals at some stage during their operations, whether in relation to customers, target clients, or even their own employees. Personal data can be collected on websites by a variety of means: registration pages, requests for details when goods or services are ordered, competitions and surveys, or by the use of various tracking devices such as cookies. Whenever personal data is collected, the organisation responsible for the use of such data (known as the 'data controller') will need to comply with various legal requirements, and may be advised to follow certain good practice guidelines, all of which are designed to protect the privacy of the individual whose data is being collected.

Compliance with these legal obligations and guidelines is greatly assisted by the use of a privacy policy, which is an increasingly common feature on commercial websites. A privacy policy is a statement of an organisation's policy on the use of personal information. At a minimum, it explains how personal information may be collected, what may happen to this information following collection, and details the associated rights of the individuals. So, a privacy policy is also valuable in terms of increasing the confidence of the users in the trustworthiness of the data controller and its practices.

In a recent study[1] carried out by the UK Information Commissioner in 2002, half of the sites surveyed contained carry either a privacy policy or a fair collection notice. There is also evidence[2] from the Organisation for Economic Co-operation and Development (OECD) that the number of websites posting privacy policies is growing rapidly.

This paper looks at the legal origins of privacy policies and how they can be used to aid compliance with data protection requirements. It then examines the key considerations when designing a privacy policy.

LEGAL ORIGINS OF PRIVACY POLICIES

There is no legal requirement either under EU or UK law to place a privacy policy on a website. Indeed, the term 'privacy policy' is somewhat of a misnomer, because there is not even any real law on privacy in the UK. However, there is a number of European legal provisions regulating various aspects of privacy and which impact upon the way in which personal information can be collected online.

In addition, the use of a privacy policy has been expressly recommended by various authoritative bodies at an international, EU and UK level. The OECD has provided detailed guidance on privacy and encourages the use of privacy policies. A Working Party set up under the Data Protection Directive has made express reference to privacy policies in its Recommendation[3], and in the UK the Information Commissioner specifically addresses privacy policies in his guidance on compliance with the Data Protection Act 1998[4].

[1] Study of Compliance with the Data Protection Act 1998 by UK based websites, dated May 2002
[2] The Report by the OECD Working Party on Information Security and Privacy, on compliance with, and enforcement of, privacy protection online, dated 21 January 2003
[3] Recommendation on the Collection of Personal Data by E-Commerce Companies by the Article 29 Working Party, adopted on 17 May 2001
[4] "Compliance Advice: Frequently Asked Questions", published on the Information Commission's website at www.dataprotection.gov.uk

In the UK the use of a privacy policy is a requirement of various voluntary codes of practice, which have been approved by the UK Information Commissioner, and of various guidelines published by privacy bodies.

EU DIRECTIVES

The most important EU law on privacy is laid down in the Data Protection Directive, which is supplemented by the Electronic Communications and Privacy Directive. In addition, the E-Commerce Directive and the Distance Selling Directive may be relevant to the creation of a privacy policy:

Data Protection Directive (95/46) (the "Data Protection Directive"): The Data Protection Directive sets out minimum standards which Member States must put in place to regulate the processing of personal information, to ensure that the rights of individuals are protected. The Data Protection Directive has been implemented in the UK by the Data Protection Act 1998 (the "DPA"). The DPA establishes the office of the Information Commissioner. As part of the Information Commissioner's duty to enforce and oversee the DPA, he is obliged to promote the following of good practice by data controllers. This is achieved in part by encouraging the use of codes of practice by data controllers.

Directive on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (2002/58): This Directive has been adopted by the European Parliament and is due to be implemented in the UK by the end of October 2003. This Directive applies to the processing of personal data of subscribers or users in connection with the provision of publicly available electronic communications services in public communications networks. In particular, it lays down various information requirements in relation to personal information which is collected electronically from the users' equipment.

E-Commerce Directive (2000/31)[5]*:* The E-Commerce Directive applies to "information society services", which means any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. This Directive requires service providers to make various information available to the recipients of the service.

Distance Selling Directive (1997/7)[6]*:* This Directive governs any contract concerning goods or services concluded between a supplier and a consumer under an organised distance sales or service provision scheme run by the supplier, who, for the purpose of the contract, makes exclusive use of one or more means of distance communication up to and including the moment at which the contract is concluded. A consumer means any natural person who, when entering into a distance contract, is acting for purposes outside his trade, business or profession. This Directive requires a minimum level of information to be provided to consumers before entering into a contract.

OECD

The OECD is an international organisation, comprising thirty member countries, with the aim of fostering good governance in public service and corporate activity. It discusses, develops and refines economic and social policies. As part of these activities the OECD may

[5] Implemented in the UK by the Electronic Commerce (EC Directive) Regulations 2002
[6] Implemented in the UK by the Consumer Protection (Distance Selling) Regulations 2000

set out guidelines in certain areas. These guidelines are not compulsory, but are widely recognised and followed. In 1980 the OECD published the Privacy Guidelines[7]. These established eight basic principles relating to international privacy protection, all of which have been enshrined in the Data Protection Directive.

The OECD has recently placed high priority on work on the global information society and electronic commerce. It set up a Working Party on Information Security and Privacy, which supports the use of privacy policies as a means of providing clear information to individuals on the use of their personal data. A "Privacy Statement Generator", produced by the OECD, aims to offer organisations a means of reviewing their privacy practices, and provides guidance on compliance with the OECD's Privacy Guidelines.

CODES OF PRACTICE

Codes of practice are not binding in the same way as legislation, but they play an important role in the framework surrounding the protection of individuals' privacy. The Data Protection Directive provides that Member States should encourage the establishment of codes of conduct intended to contribute to the proper implementation of the provisions of the Data Protection Directive. This is reflected in the DPA.

INFORMATION COMMISSIONER'S CODES OF PRACTICE

The Information Commissioner is charged with issuing codes of "good practice" to be followed by data controllers[8]. Although the codes may be obligatory or voluntary, it is generally in the best interests of businesses to adhere to such codes. This demonstrates to the Information Commissioner willingness to protect individuals' privacy, and to act in the best interests of consumers.

The Information Commissioner also has a duty to encourage trade associations to disseminate codes of practice to their members. Good practice is defined as "…such practice in the processing of personal data as appears to the Information Commissioner to be desirable having regard to the interests of data subjects and others, and includes (but is not limited to) compliance with the requirements of this Act."[9]. The following factors are relevant in considering the encouragement of good practice: transparency, fairness, purpose limitation, and security.

Whilst the Information Commissioner has not yet issued any codes of practice relating specifically to privacy policies, he has provided guidance on the drafting of privacy policies in the FAQs[10] and endorsed several industry codes of practice.

INDUSTRY CODES OF PRACTICE

Industry also produces its own codes of practice, such as the Business Banking Code (written by the British Bankers Association, the Building Societies Association and the Association for Payment Clearing Services), the Consumer Credit Trade Association Code of

[7] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data dated 23 September 1980
[8] Section 51 of the DPA
[9] Section 51(9) of the DPA
[10] "Compliance Advice: Frequently Asked Questions", published on the Information Commission's website at www.dataprotection.gov.uk

Practice and various relevant Advertising and Direct Marketing Codes issued by the Advertising Association and Advertising Standards Authority. Although industry codes of practice are voluntary, compliance with a trade association's code is often a condition of membership of that trade association. Membership is generally too valuable to jeopardise it by breaching the code. So in reality many industry codes of practice are subscribed to by the majority, if not all, organisations in that industry.

The Business Banking Code is a voluntary code, laying down general standards of good banking practice regarding the dealings of financial institutions with personal customers. In practice, around 120 banks and building societies have signed up to the Code, accounting for over 99% of the total market place. Section 11 of the Code addresses protection of customers' personal and business information: customers are assured that their personal information will be treated as private and confidential, and are notified of the limited circumstances in which their personal information will be disclosed to third parties. Customers will be notified of their right of access to personal records including any fee payable. They will also be informed if telephone conversations are to be recorded.

The Consumer Credit Trade Association (CCTA) Code of Practice sets out standards of good practice for the finance and leasing industry. It applies to all credit, hire or lease agreements and accounts operated by members, both with consumers and business customers. The Code does not in all cases lay down prescriptive rules but merely sets out principles which members are required to apply in the spirit of the Code. The principles of data protection are dealt with in very broad terms: members are required to comply with the data protection legislation when obtaining and processing customers' data and to explain to their customers that by virtue of this legislation they have the right of access to their personal records held on computer files.

The Direct Marketing Association (DMA) Code of Practice contains rules governing the use of personal information for direct marketing purposes. The Code provides that members must comply with all relevant data protection legislation. The Code lists general rules on the use of data, and special rules for data owners, data users, list brokers, list managers and data processors. The DMA is responsible for monitoring the Code and has the power to seek undertakings from a member not to repeat a breach, to issue a formal admonition, or to suspend or terminate membership. The DMA has also produced a Code of Practice for Electronic Commerce, which contains a section on privacy, stating the following: "Members must have in place an effective policy for protecting the privacy of all visitors to a website. The existence of such a policy must be made clear and a website must make available a click-through link to a statement of the privacy policy immediately prior to, or at the time that any personal information is collected." The Code continues to list minimum content requirements for a privacy policy and provides rules on use of information, security, access and transfers outside the European Economic Area (EEA).

PRIVACY GROUPS

A number of privacy groups have also set standards for compliance with data protection. These groups intend to provide a framework within which businesses can operate to ensure compliance with privacy laws and to establish a relationship of trust with consumers.

The most important example of a privacy group in the UK is TrustUK. This is a joint non-profit making venture between the Alliance for Electronic Business[11] and the Consumers' Association, which has been endorsed by the UK Government. Organisations can apply for accreditation by TrustUK, allowing them to display the TrustUK hallmark on their website. To become accredited, an organisation must have in place a mandatory code of practice for its members, which complies with core principles set down by TrustUK. These include the adoption and implementation of an effective policy for protecting visitors to the website, to which a clear click-through link is made available before or at the time any personal data is collected.

DESIGNING A PRIVACY POLICY

Given that a privacy policy is essentially a statement of an organisation's policy regarding personal data, the organisation needs to make sure that it does in fact have a policy in place. Initially, this involves conducting an audit of what personal data is collected online, how this is done, and how personal data is used once obtained. Most of the information will originate from the user registration page but data may be collected elsewhere, such as the 'Contact Us' page, the use of 'cookies' or e-mail correspondence. The organisation should then check what procedures it has in place to ensure the accuracy and security of personal information and to provide access on request to the users of this information.

In terms of location on a website, the privacy policy should be clearly accessible to users. The Recommendation[12] makes it clear that the various legal information requirements "should be shown directly on the screen before the collection to ensure the fair processing of data." Complete information on the privacy policy should be directly accessible on the home page of the website, and anywhere where personal data is collected. The link should explain clearly and specifically what it relates to, a suggested heading being, *"We are collecting and processing personal data relating to you. For further information, click here."* This suggests that the words "*Privacy Policy*" will not be sufficient on their own.

The policy should be written in language which is intelligible to the average user of the website. Websites that collect information from children may have to put more rigorous safeguards in place to ensure that the processing of such information is fair. It should be recognised that children generally have a lower level of understanding than adults, and notices explaining how data will be used should be worded accordingly.

Both the Recommendation and the FAQs provide detailed guidance on the contents of a privacy policy and the additional measures and procedures which should be put in place to support the privacy policy. A useful starting point for the wording of the privacy policy is the Privacy Statement Generator[13] published by the OECD. This poses a questionnaire which, when completed, generates a draft privacy statement from the responses given.

INFORMATION REQUIREMENTS

[11] Comprises the Confederation of British Industry, the Computing Services and Software Association, the DMA, e-centre UK and the Federation of the Electronics Industry

[12] Recommendation on the Collection of Personal Data by E-Commerce Companies by the Article 29 Working Party, adopted on 17 May 2001

[13] This can be found at www.oecd.org under 'OECD tools'

A privacy policy should contain the following "Fair Collection Information"[14]:The identity of the data controller and of its representative (if any). A representative will only be used if the data controller is located outside the EEA and uses equipment in the UK for processing personal data.

- The purposes for which the data may be processed. It should be noted that this requirement is self-limiting: individuals' permission to use of their personal data may be invalidated if the purpose for which such data is used is subsequently changed from the purposes disclosed prior to the collection of the data. If no purposes are stated, the purposes will be deemed to be those that are obvious from the nature of the transaction – data collected for non-obvious purposes will therefore be unlawfully collected. The Information Commissioner has added that as an aid to encouraging confidence, a privacy policy should describe not only what an organisation does with personal data but also what it does not do.

- Any other information in so far as it is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing. The Data Protection Directive suggests that this information could include details of recipients of the personal data, guidance on whether information requested is mandatory, and the rights of the individual in relation to his personal data. There are therefore some schools of thought that this information should make reference to any non-obvious data processing activities. So, on this basis, it is likely that data will not be treated as having been 'fairly' obtained on a website unless users of the site have been informed of the use of cookies on the site or of the potential use of the user's information for marketing purposes.

The Recommendation states that the following additional information should be provided:

- Guidance on whether replies to information requested are obligatory or optional. It is suggested that obligatory information can be indicated by the use of a star next to the question.

- The physical and electronic address of the data controller.

- The existence of, and conditions for exercising, the individuals' rights in relation to their personal data, namely the right to consent or object to the processing of personal data, the right to access personal data, and the right to have such data rectified or deleted.

- The recipients or categories of recipients to whom the collected information may be disclosed, such as business partners and subsidiaries, together with the reason why such data may be disclosed. Such an explanation is required if the data is to be used for purposes other than providing the requested service or if it is to be used for direct marketing.

- Information on any transfers of personal data to countries outside the EEA, including whether the country in question provides adequate protection of individuals with regard to the processing of their personal data.

[14] DPA Schedule 1 Part II paragraph 2(3) which implements Article 10 of the Data Protection Directive

- Contact details for any queries.

- The existence of any automatic data collection procedures, such as the use of cookies. This information must be provided before using such a method to collect data. Furthermore, users should also be informed of the domain name of the site server transmitting the automatic collection procedures, the purpose of these procedures, their period of validity, whether or not acceptance of such procedures is necessary to visit the site and the option available to object to their use, as well as the consequences of de-activating such procedures. However, the Information Commissioner states that a privacy policy should not be relied on exclusively to notify users of automatic data collection procedures – there should at least be some reference to the use of tracking technology clearly displayed to all visitors to the website.

- Information on security measures used.

CONSENT

Privacy policies are generally accessible on websites on a non-compulsory click-through basis. However, this means of access should never be used to obtain consent to the use of data from users on an opt-out basis (for example, for direct marketing): such an approach would be inadequate at both an EU and a UK level. A non-compulsory click-through privacy policy may be an effective means of obtaining consent on an opt-in basis, but the legal position is unclear and this approach should not be regarded as 'best practice'.

TECHNIQUES FOR INCREASING CONSUMER CONFIDENCE

The Information Commissioner's padlock symbol, launched in March 2000, alerts individuals to the fact that their personal information is being collected, and draws their attention to the explanation of how it is to be used. All data controllers may use the padlock symbol and it should be clearly positioned at any point where information is requested. Use of the symbol is not compulsory and it has not been widely used to date.

Seals of approval from organisations such as TrustUK can be used to reassure individuals that their personal information will be processed in accordance with data protection requirements.

Users may be assured that a website is secure is by the adoption of a Verisign certificate. The Verisign Secure Site seal indicates to customers that the website is authentic and that all transactions are secured by SSL encryption. The certificate can be obtained by application to Verisign.

COLLECTION LIMITATION

Personal data collected on a website should be relevant to the purposes stated in the privacy policy, and the purposes stated should be wide enough to justify the extent of the data collected. This is to ensure compliance with the third principle of the DPA which states that "personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed". The FAQs emphasise that website operators must not mislead users, and if information is not strictly necessary for the supply of a product or service, it should be made clear why the information is being requested and the provision of such information should be optional.

SECURITY

The seventh data protection principle under the DPA states that "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." In practice, this means that organisations have an obligation to ensure that personal data are collected online, and subsequently stored and/or processed, in a secure environment. The Recommendation states that users should be informed of the security measures "guaranteeing the authenticity of the site, the integrity and confidentiality of the information transmitted over the network taken in application of the national legislation applicable". The measures to be taken will depend on the harm that might result from unauthorised processing or accidental loss or destruction and the nature of the data to be protected. Technical measures might include use of passwords to authenticate employee users of customer data systems, encryption to prevent hackers or firewalls and virus detecting software. The FAQs question whether sufficient security can be achieved without the use of an encryption-based transmission system if the personal data are in any way sensitive, for example if they include credit card numbers.

CHANGES TO USE OF DATA

If an organisation wishes to change the nature of its use of personal data, it cannot simply change the statement of use in the privacy policy. Changing the privacy policy will only apply to personal data obtained after the date of the change. In respect of personal data collected before the change in the privacy policy, the Information Commissioner advises that the safest course of action is to obtain the user's consent to the new use. An opt-in approach is necessary if the data collected is to be used for a new purpose or to be disclosed either for the first time or to different organisations from those referred to in the privacy policy. If, however, the change in use does not amount to a new purpose, it is sufficient to advise users of the change and give them an opportunity to object.

MISUSE OF PERSONAL DATA COLLECTED ONLINE

An organisation which breaches the terms of its privacy policy may find itself in breach of the DPA, depending on which terms it has contravened. For example, if the organisation does not provide the user with information on the purpose(s) for which the data is being processed, the organisation would be in breach of the first principle of the DPA. This is not a criminal offence (whereas failure to notify the Information Commissioner that processing is taking place would be) but it may cause the Information Commissioner to take action against the website operator to enforce compliance.

If the Information Commissioner believes that a data controller has contravened any of the data protection principles, the Information Commissioner can serve an enforcement notice requiring the organisation to take specified steps, or to refrain from processing personal data. If the data controller does not comply with the notice, it is guilty of an offence, liable to a fine of up to £5,000 (or unlimited if in the Crown Court). If a company or other corporation commits a criminal offence under the DPA, any director, manager, secretary or similar officer is personally guilty of the offence.

The recent public criticisms of Amazon.com's "clarification" of its privacy policy have demonstrated the importance of putting in place a privacy policy which adequately states the purposes for which personal information may be used. In an early version of its privacy policy, Amazon stated that it did not disclose personal information to others, and specifically that it would in effect guarantee that this would never occur if customers requested Amazon not to sell that data to third parties by using "never@amazon.com". In September 2000 Amazon changed its privacy policy to acknowledge that customer data may be transferred to potential purchasers of the Amazon business without seeking additional consent from its customers. The change in the terms of the privacy policy prompted US consumer and privacy groups, Junkbusters Corp. and the Electronic Privacy Information Center, to ask the Federal Trade Commission (FTC) to investigate Amazon.com. The privacy groups claimed that the changes to the privacy policy constituted a breach of section 5 of the Federal Trade Commission Act in that Amazon had deceived its customers in its use of their personal data, on the grounds that Amazon could now disclose personal information about customers who previously selected "never@amazon.com". The FTC found that Amazon's revised privacy policy did not materially conflict with the representations Amazon had made in its previous policy. Despite the ambiguous nature of the revised privacy policy, Amazon had made assurances to the FTC that it would not disclose to third parties any personal information concerning consumers who previously selected "never@amazon.com". However, the FTC commented that if a material change was made to its stated privacy practices, Amazon should provide adequate notice to customers as well as a mechanism to obtain consumers' consent to the change with respect to information already collected from them.

APPENDIX
INFORMATION REQUIREMENTS FOR ONLINE COMMUNICATIONS

DATA PROTECTION DIRECTIVE 1995/46/EC

APPLICATION

The processing of personal data by automatic means or, if the personal data are to form part of a filing system, by alternative means.

INFORMATION TO BE GIVEN TO THE DATA SUBJECT IF PERSONAL DATA IS COLLECTED FROM HIM (ARTICLE 10)

Where the data controller collects the data from the data subject, it should provide the following information (unless the data subject already has it):

1. the identity of the data controller and of its representative (if any);

2. the purposes for which the personal data are being processed;

3. any further information such as the following, in so far as such information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing:

   (a) the recipients or classes of recipients of the personal data;

   (b) whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply;

   (c) the existence of the right of access to and the right to rectify the personal data.

INFORMATION TO BE GIVEN TO THE DATA SUBJECT IF PERSONAL DATA IS NOT COLLECTED DIRECTLY FROM HIM (ARTICLE 11)

Where the data controller does not collect the data from the data subject, the data controller should, subject to a limited exception, provide the data subject with the following information (unless the data subject already has it) at the time of receiving the personal data or, if a disclosure to a third party is envisaged, no later than when the personal data are first disclosed:

1. the identity of the data controller and of its representative (if any);

2. the purposes for which the personal data are being processed;

3. any further information such as the following, in so far as such information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing:

(a) the categories of data concerned;

(b) the recipients or classes of recipients of the personal data;

(c) the existence of the right of access to and the right to rectify the personal data.

E-COMMERCE DIRECTIVE 2002/31/EC

APPLICATION

Generally speaking, the provision of information society services.

GENERAL INFORMATION (ARTICLE 5)

Information to be made available by a service provider to recipients of the service and the competent authorities:

1. the name of service provider;
2. the geographic address at which the service provider is established;
3. the details of the service provider, including email address;
4. the details of the trade register (or equivalent) on which the service provider is entered, and his number, or equivalent means of identification in that register, if applicable;
5. the particulars of the relevant supervisory authority for the service, if applicable;
6. if the service provider conducts a regulated profession:
    (a) details of the body or similar institution;
    (b) the professional title and the member state where the title has been granted;
    (c) reference to the professional rules applicable to the service and the means to access them;
7. the VAT registration number of the service provider, if applicable.
8. any prices should be clearly and unambiguously indicated, indicating whether they include taxes and delivery costs.

COMMERCIAL COMMUNICATIONS (ARTICLES 6 AND 7)

All commercial communications (i.e. generally communications designed to promote the goods, services or image of any person pursuing a commercial, industrial or craft activity or exercising a regulated profession) should:

1. be clearly identifiable as commercial communications;
2. clearly identify the person on whose behalf the communication is made;
3. clearly identify any promotional offer and any related conditions;
4. clearly identify any promotional competition or game and any related conditions;

5. if the commercial communication is unsolicited and sent by e-mail, be clearly and unambiguously identifiable as such as soon as it is received.

CONTRACTS CONCLUDED BY ELECTRONIC MEANS (ARTICLE 9)

Except where the contract is concluded exclusively by e-mail (or the equivalent), the following information should be given to the recipient of the service prior to an order being placed (Note: parties who are not consumers may agree otherwise):

1. the different technical steps to follow to conclude to contract;

2. whether or not the concluded contract will be filed by the service provider and whether it will be accessible;

3. the technical means for identifying and correcting input errors prior to the placing of the order;

4. the languages offered for the conclusion of the contract

5. relevant codes of conduct to which the service provider subscribes and how those codes can be consulted electronically

Plus, terms and conditions applicable to the contract must be made available in such a way that the recipient can store and reproduce them

PLACING OF THE ORDER (ARTICLE 11)

If the recipient of the service places his order by technological means and the contract is not concluded exclusively by e-mail (or the equivalent), the service provider must acknowledge receipt of the order without undue delay and by electronic means. (Note: parties who are not consumers may agree otherwise.)

DISTANCE SELLING DIRECTIVE 2000/31/EC

APPLICATION

Distance contracts other than for financial services between consumers and suppliers.

INFORMATION PRIOR TO THE CONCLUSION OF THE DISTANCE CONTRACT (ARTICLE 4)

Information to be provided to the consumer in good time prior to execution of the contract:

1. the identity of the supplier and, where the contract requires payment in advance, the supplier's address;
2. the main characteristics of the goods or services;
3. the price of the goods or services including all taxes;
4. delivery costs, where appropriate;
5. the arrangements for payment, delivery and performance;
6. the existence of a right to cancellation, where applicable;
7. the cost of using the means of distance communication, where it is calculated other than at a basic rate;
8. the period for which the offer or the price remains valid;
9. the minimum duration of the contract in the case of contracts for the supply of goods or services to be performed permanently or recurrently, where appropriate;
10. [optional: the right of the supplier to substitute equivalent goods or services if it is unable to perform the contract within 30 days because the goods or services ordered are unavailable (Article 7).

WRITTEN CONFIRMATION OF INFORMATION (ARTICLE 5)

The consumer must receive confirmation in writing or another durable medium in good time during the performance of the contract and at the latest before delivery of goods to the consumer of the following if not already provided to the consumer in the stated medium prior to the conclusion of the contract:

1. the prior information requirements;
2. the conditions and procedures for withdrawal from the contract;
3. the geographical address of the place of business of the supplier to which any complaints may be sent;
4. details of any after-sales services and guarantees;

5. the conditions for exercising any contractual right to cancel the contract, where the contract is of an unspecified duration or a duration exceeding one year.

DISTANCE MARKETING OF FINANCIAL SERVICES DIRECTIVE 2002/65/EC

APPLICATION

Distance contracts for financial services between consumers and suppliers.

INFORMATION PRIOR TO THE CONCLUSION OF THE DISTANCE CONTRACT (ARTICLE 3)

Information to be provided to the consumer in good time before the execution of the distance contract. Such information must also be provided on paper or on another durable medium prior to the execution of the distance contract, or if not possible because of the means of distance communication requested by the consumer, immediately after the conclusion of the contract:

1. The supplier:

    (a) the identity and the main business of the supplier, the geographical address of its establishment and any other relevant geographical address;

    (b) the identity of the supplier's representative (if applicable) and relevant geographical address;

    (c) if the consumer is dealing with any professional other than the supplier, the identity of this professional, the capacity in which he is acting and his relevant geographical address;

    (d) if the supplier is registered in a trade or similar public register, the details of the trade register and the registration number of the supplier;

    (e) where the supplier's activity is subject to an authorisation scheme, the particulars of the relevant supervisory authority;

2. The financial service:

    (a) the main characteristics of the financial service;

    (b) the total price to be paid by the consumer for the financial service, including all related charges and taxes or, where an exact price cannot be indicated, the basis for the calculation of the price enabling the consumer to verify it;

    (c) where relevant, notice indicating that the financial service is related to instruments involving special risks related to their specific features or the operations to be executed or whose price depends on fluctuations in the financial markets outside the supplier's control and that historical performance are no indicators for future performance;

(d) notice of the possibility that other taxes and/or costs may exist that are not paid via the supplier or imposed by him;

(e) any limitations of the period for which the information provided is valid;

(f) the arrangements for payments and for performance;

(g) any specific additional cost for the consumer of using the means of distance communication, if such additional cost is charged;

3. The distance contract:

(a) the right of withdrawal exists, its duration and the conditions for exercising it, costs of exercising the right and consequences of non-exercise of that right, or a statement if the right of withdrawal does not exist;

(b) the minimum duration of the distance contract in the case of financial services to be performed permanently or recurrently;

(c) any rights the parties may have pursuant to the contract to terminate early or unilaterally and any associated penalties ;

(d) practical instructions for exercising the right of withdrawal indicating, *inter alia*, the address to which the notification of withdrawal should be sent;

(e) the Member State(s) whose laws are taken by the supplier as a basis for which the establishment of relations with the consumer prior to the conclusion of the distance contract;

(f) any contractual clause on applicable law and/or on competent court;

(g) the language(s) in which the contractual terms and conditions and the prior information are supplied, and the language(s) in which the supplier, with the agreement of the consumer, will communicate regarding the distance contract;

4. Redress:

(a) whether or not there is an out-of-court complaint and redress mechanism for the consumer and, if so, the methods for having access to it;

(b) the existence of certain guarantee funds or other compensation arrangements.

ELECTRONIC COMMUNICATIONS & PRIVACY DIRECTIVE 2002/58/EC

APPLICATION

The processing of personal data of subscribers or users in connection with the provision of publicly available electronic communications services in public communications networks.

TRAFFIC DATA (ARTICLE 6)

Information on processing for the purposes of subscriber billing and interconnection payment:

1. types of traffic data to be processed
2. purposes of the processing
3. duration of such processing

To obtain consent for processing for marketing or value added services:

1. types of traffic data to be processed
2. purposes of the processing
3. duration of such processing
4. subscriber's right not to give his consent
5. subscriber's right to withdraw his consent at any time

PROCESSING OF LOCATION DATA (ARTICLE 9)

Information on processing of location data:

1. types of location data to be processed,
2. purposes of the processing
3. duration of the processing
4. whether the data will be transmitted to a third party for the purpose of providing the value added service.
5. subscriber's right not to give his consent
6. subscriber's right to withdraw his consent at any time

CONTACT INFORMATION

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

Susan Atkinson, Associate, Tel +44 (0) 20 7778 1869

William Long, Associate, Tel +44 (0) 20 7778 1865

Sidley Austin Brown & Wood

1 Threadneedle Street

London EC2R 8AW

Tel: +44 (0) 20 7360 3600

Tel +44 (0) 20 7626 7937

WWW.SIDLEY.COM

ALL PARTNERS ARE EITHER SOLICITORS OR REGISTERED FOREIGN LAWYERS