SIDLEY AUSTIN BROWN & WOOD
AND AFFILIATED PARTNERSHIPS

THE EU'S DATA PROTECTION DIRECTIVE

On 23 September 1980, the Organisation for Economic Co-Operation and Development adopted a set of guidelines concerning data protection and transborder data flows. Following on from those guidelines, the EU enacted the Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data (the "Convention") in 1981. Within the EU, Member States had divergent laws on data protection and the EU took the view that it would be better to harmonise the laws of all Member States so that people could look to one standard when conducting Processing activity within the EU. At least, that was one of the aspirations. In 1995, after years of discussion the European Data Protection Directive 95/46 EC (the "Directive") was eventually adopted. Unfortunately, the Directive only sets out the minimum standard of data protection for Member States to implement. Member States are entitled to keep or to implement data protection rules which surpass the standard of the Directive. That, coupled with the fact that the Directive leaves Member States with some choices on the implementation of certain areas, means that complete harmonisation of data protection law throughout the EU has not occurred. As a result, businesses Processing data in more than one Member State need to be aware of the data protection legislation in each Member State. Nevertheless, the Directive sets out the minimum standard that all Member States are obliged to respect.

What is the Status of the EU Protection Directive 1995?

Like all EU Directives, this Directive does not automatically become law in any of the Member States; it needs to be implemented by means of national legislation. However, it does lay down the minimum requirements for the data protection laws of the Member States, so is useful in the interpretation of the national legislation.

What is the Scope of the EU Data Protection Directive 1995?

In the following description the capitalised terms are used as shorthand for the descriptions which follow immediately afterwards:

The Directive is intended to apply to the Processing of Personal Data wholly or partly by automatic means, and to the Processing otherwise than by automatic means of Personal Data which form part of a Filing System or are intended to form part of a Filing System. The Directive is not intended to apply to the Processing of Personal Data by an individual in the course of a purely personal or household activity. Moreover, the Processing must be either carried out in the context of an Establishment of the Controller within the jurisdiction of a Member State, or alternatively, carried out upon equipment located in the Member State other than for the sole purpose of transit through that Member State.

"Controller" means any person who alone or jointly determines the purposes for which Personal Data are Processed.

"**Data Subject"** means an individual who is the subject of personal data.

"Establishment" means a Controller is established in a Member State if it carries out the effective and real exercise of activity through stable arrangements in that Member State.

"Filing System" means any structured set of Personal Data which are accessible according to specific criteria whether centralised, or decentralised, such as a filing cabinet containing employee files organised according to their date of joining or their names.

"Personal Data" are data which relate to an individual who is identified or identifiable either directly or indirectly by reference to an identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. In practice, this is a broad definition including anything from someone's address or national insurance number to information about their taste in clothes.

"Processing" means any operation or set of operations performed upon Personal Data, such as collection, recording, organisation, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. This

definition is so broad that it covers practically any activity in relation to holding Personal Data.

What Obligations do Controllers have According to the Directive?

Notification

Each Member State is obliged to set up a national supervisory authority which Controllers must notify before commencing any wholly or partly automatic Processing operation(s). There are instances where the Member States can exempt Data Controllers from this requirement. For example, if the Controller has appointed a data protection officer who keeps an internal register of Processing activities, or if the Processing is unlikely to prejudice the individuals' rights and the Controller has specified the purposes of Processing along with certain other information to the supervisory authority.

Pre-Condition to Processing

Member States must provide that Controllers may only process Personal Data if they have satisfied one of six pre-conditions: (1) the individual in question has consented to the Processing, (2) the Processing is necessary to enter into or perform a contract with the individual in question, (3) the Processing is necessary for the pursuit of a legitimate interest of the Controller or a third party to whom the Personal Data are to be disclosed and the rights of the individual are not overridden, (4) the Processing is necessary to comply with a legal obligation, (5) that the Processing is necessary to protect the vital interests of the individual, or (6) the Processing is necessary for the administration of justice or carried out in fulfilment of a public interest function. Of these pre-conditions the first three will be most relevant to business.

Personal Data which relates to an individual's race or ethnicity, sexual or political life, trade union membership, religious or other similar beliefs, or health ("Sensitive Personal Data") can only be Processed in more narrowly defined circumstances. The circumstances which will be most relevant to a business would be where the individual has explicitly consented to the Processing (unless the Member State chooses to prohibit Processing even where consent has been given), or where the Processing is necessary for the Controller to fulfil obligations imposed by employment law.

Provision of Information

Certain information needs to be provided to individuals when Controllers collect Personal Data about them, unless and to the extent that the individuals already have that information. That information includes the identity of the Controller (or the Controller's representative), the purpose(s) of the Processing, and such further information as may be necessary to ensure that the Processing is fair (e.g. the categories of Personal Data, the categories of recipients, the existence of rights of individuals to access and rectify their Personal Data). In instances where the Personal Data are not collected by the Controller directly from the individual concerned, the Controller is expected to notify this information at the time it records the Personal Data, or where a disclosure is envisaged, at the time the Personal Data are first disclosed. Also, in cases of indirect collection, it is possible to avoid this requirement of information provision if to do so would be impossible or involve a disproportionate effort, or if the collection is intended for scientific or historical research or is collection that is mandated by law.

Treatment of Personal Data

In addition to notification, Member States must provide that Controllers Process fairly and lawfully, collect Personal Data for clear and legitimate purposes, ensure that Personal Data are adequate, relevant and not excessive for the purposes for which they were collected, and keep the Personal Data accurate, up to date, and in a form which permits identification of the individual for no longer than is necessary.

Security

The Controller will be responsible for ensuring that appropriate technical and organisational measures are in place to protect the Personal Data. Controllers must be made to ensure that those who Process on their behalf, do so only upon their instructions and under a written contract which obliges them to also ensure the same level of security as would be expected from the Controller.

Prohibition on Transfers outside the EEA

Member States must ensure that Controllers do not transfer to countries outside of the European Union unless the recipient country provides an adequate level of protection for the Personal Data. The Controller must

assess the adequacy of protection in light of a large number of factors, including, the nature of the Personal Data, the country of origin, and the laws in place in the recipient country. The EU Commission can make a finding on the adequacy of any particular non-EU country, and Member States are expected to give effect to such findings as necessary in their national laws. So far the EU Commission has made findings of adequacy with respect to Hungary, Switzerland and Canada. The US has reached agreement with the EU Commission on a set of "Safe Harbor" Principles to which organisations in the US may subscribe to in order to be deemed "adequate" to receive Personal Data from Controllers in the EU.

In the event that it is not possible to ascertain "adequacy", transfers may be permitted in a limited number of prescribed situations. These include, but are not limited to, situations where the individual has unambiguously consented to the transfer, the transfer is necessary to perform or conclude a contract that the Controller has with the individual or, alternatively, with a third party if the contract is in the individual's interests.

In addition, the European Commission has approved standard contractual clauses which may be used by Data Controllers (separate wording has been approved for Data Processors) when transferring Personal Data to non – EEA countries. If the contract includes these clauses, the Personal Data will be presumed to be adequately protected.

The EU's Article 29 Working Party is also currently consulting on a direct compliance strategy, or what is being called "binding corporate rules", which may be available as an alternative means of authorising transfers of personal data outside the EEA. This approach would be suitable for multinational companies transferring personal data within the same company, or among parents, subsidiaries and affiliates that are under common control. Under this approach, the company would adopt a group wide data protection policy which satisfies an approved criteria laid down by the Article 29 Working Party and if the rules bind the whole group, then those rules could be approved as providing adequate data protection for personal data transfers throughout the group of companies. Moreover, these rules could also be drafted to comply with privacy laws in other countries. In the UK, the Information Commissioner has recently expressed a commitment to working with multinational groups who wish to develop such a set of rules.

For further information on the prohibition of transfers outside the EEA, particularly in the US see Sidley Austin Brown & Woods briefing paper 'EU Regulation of Transborder Data Flows'.

Marketing

The EU Telecommunications (Data Protection and Privacy) Directive 97/66/EC places requirements on Member States in relation to the use of Personal Data for direct marketing. Direct marketing for these purposes constitutes unsolicited faxes, or making unsolicited telephone calls through the use of automated calling machines. In such instances the direct marketer needs to have the prior consent of the recipient. In other instances of unsolicited calls for the purposes of direct marketing, it is left up to the Member States to decide whether such calls will require the recipient's consent or, alternatively will be prohibited to potential recipients who have indicated that they do not wish to receive such calls.

The Electronic Communications (Data Protection and Privacy) Directive, which was due to be implemented by national legislation before 31 October 2003, will replace Directive 97/66/EC referred to above. One of the aims of this new directive is to extend the restrictions on direct marketing to e-mail communications, so that the prior consent of the recipient is required. For further information see Sidley Austin Brown & Wood's briefing paper 'New Legal Requirements in Online Marketing'.

What Rights do Individuals have under the EU Data Protection Directive?

Access and Rectification

Member States are expected to reserve for individuals the right to obtain access to Personal Data held about them and, to be able to ask for the Personal Data to be rectified where they are inaccurate.

Right to Object

Individuals should be afforded rights allowing them to object to certain types of Processing. In particular, where Processing is carried out on the basis of the public interest or in the legitimate interests of the Controller, the individuals in question should have the right to object to such Processing on compelling legitimate grounds. For example, this would be the case if the Processing would

cause those individuals unwarranted harm. Individuals are also to be allowed to object to direct marketing and to decisions which significantly affect them being made solely on the basis of automated Processing.

Issues to Consider

Have you lodged a notification/registration in each Member State that your organisation does business in? Are your existing notifications sufficient?

Do you have a justification for Processing the Personal Data within your control (e.g. legitimate business interest, consent from Data Subject, etc…). Are you Processing any 'sensitive' Personal Data? If so, do you have explicit consent to do so?

Are you notifying the relevant individuals (e.g. employees, employees of clients, employees of suppliers, other business contacts) of the Processing you are conducting?

Have you got adequate security measures and a data retention policy in place?

Are you responding properly to any requests from individuals whose Personal Data you hold to requests for access and/or rectification?

Are you transferring or providing access to Personal Data outside of the European Economic Area? If so, do you have a justification for doing so (e.g. the individual's consent, necessary to carry out a contract with the individual, etc…)?

Useful Sites

The EU maintains a site which contains links to the Directive, information about the implementation of the Directive in the EU Member States, details of the data protection regulators in the EU Member States, and associated official documents (e.g. EU approved model contracts for transfers of data to non EEA countries). The website is located at
http://europa.eu.int/comm/internal_market/en/dataprot/

EU Business also maintains a web page with a variety of commentaries on EU data protection as well links to copies of official documents. Its data protection web page is located at
http://www.eubusiness.com/cgi-bin/item.cgi?id=19123

Sidley Austin Brown & Wood, has no responsibility for any of the websites listed above.

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

REGULATED BY THE LAW SOCIETY