INTRODUCTION
As markets become more global, data protection awareness and compliance in transborder data flows is becoming increasingly important. There are important issues for companies wishing to send personal data to countries outside the European Economic Area (EEA). This paper considers in detail the Eighth Principle under the Data Protection Act 1998 (the Act) and the ways in which compliance with its requirements may be achieved.

THE EU DATA PROTECTION DIRECTIVE
Directive 95/46/EC1 (the Directive) addresses the transfer of personal data to third countries in Articles 25 and 26. Article 25 provides that transfers of personal data to third countries where the data is intended for processing after transfer may only take place if the third country in question ensures an adequate level of protection.

The adequacy of the level of protection is to be assessed “in the light of all the circumstances surrounding a data transfer operation”. Consideration is to be given to issues including:

1. the nature of the data;
2. the purpose and duration of the processing operation;
3. the country of origin and of final destination;
4. the rules of law in the third country; and
5. any professional rules and security measures which are complied within the third country in question.

Article 29 provides for the establishment of a Working Party on the protection of individuals with regard to the processing of personal data.

THE EIGHTH DATA PROTECTION PRINCIPLE
The eighth principle of the Act implements the provisions of Article 25 of the Directive.

There are eight data principles under the Act, which data controllers are required to comply with when processing personal data. Compliance with the eighth principle goes hand in hand with compliance with the other seven principles set out in the Act.

The eighth principle states:

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The EEA consists of the following countries: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Liechtenstein, Luxembourg, Netherlands, Norway, Portugal, Spain and Sweden. The Channel Islands and the Isle of Man are not part of the EEA.

1 Directive 95/46 EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data
According to the Act, an “adequate” level of protection is one which is adequate in all the circumstances of the case, having regard to in particular to:

1. The nature of the personal data;
2. The country or territory of origin of the information contained in the data;
3. The country or territory of 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 enforceable in that country or territory; and
8. Any security measures taken in respect of the data in that country or territory.

This is not an exhaustive list. Adequacy requirements are considered in more detail below.

**DEROGATIONS FROM THE EIGHTH PRINCIPLE**

Article 26 of the Directive provides for derogations from the prohibition in Article 25. These have been incorporated into Schedule 4 of the Act, which sets out a number of derogations where the eighth principle will not apply:

1. The data subject has given his consent to the transfer:

   This exemption is likely to be relied upon by many companies, which could request consent from employees or other data subjects. The consent requirement is considered in more detail below.

2. The transfer is necessary:

   (a) for the performance of a contract between the data subject and the data controller; or
   (b) for the taking of steps at the request of the data subject with a view to his entering into a contract with the data controller.

3. The transfer is necessary:

   (a) for the conclusion of a contract between the data controller and a person other than the data subject which:
       (i) is entered into at the request of the data subject; or
       (ii) is in the interests of the data subject, or
   (b) for the performance of such a contract.

Contracts are not restricted to goods and services. The provisions may, for example, be relevant to employment contracts. Whether the transfer is necessary depends, in
the Commissioner’s view, on the nature of goods, services etc rather than the business structure of the data controller. For example, if the customer of a UK credit card holder uses his/her card in Japan it might well be necessary for the card issuer to transfer some personal data to Japan to validate the card and/or reimburse the merchant.

4. (1) The transfer is necessary for reasons of substantial public interest.

(2) The Secretary of State may by order specify:

(a) circumstances in which a transfer is to be taken for the purposes of sub-paragraph (1) to be necessary for reasons of substantial public interest; and

(b) circumstances in which a transfer which is not required by or under an enactment is not to be taken for the purpose of sub-paragraph (1) to be necessary for reasons of substantial public interest.

This is likely to occur in the areas of prevention and detection of crime, national security and tax collection. Personal data should only be transferred where there is likely to be substantial prejudice to the public interest if the transfer did not take place.

5. The transfer:

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

The legal proceedings do not necessarily have to involve the data controller or data subject.

6. The transfer is necessary in order to protect the vital interests of the data subject.

This concerns matters of life and death, such as the transfer of medical records where the data subject was seriously ill.

7. The transfer is part of the personal data on a public register and any conditions subject to which the register is open to inspection are complied with by any person to whom the data are or may be disclosed after the transfer.

This appears to allow the transfer of extracts from a public register but not the transfer of the entire register.

8. The transfer is made on terms which are of a kind approved by the Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects.

This is where model contract clauses may be used (see below).
9. The transfer has been authorised by the Commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects.

It is worth noting that none of the conditions above is “stronger” than the other – all should be given equal consideration in deciding a strategy for export of data.

Adequacy

In deciding on adequacy, data controllers are required to make a risk/adequacy assessment based on the facts of each case.

As stated above, Article 25(2) of the Directive states that adequacy shall be assessed in light of all the circumstances surrounding the data transfer, with particular consideration being given to the nature of the data, the purpose and duration of the proposed processing operation, the country of origin and of destination, the rules of law in force in the country receiving the data, and security measures in the third country.

The Act sets out a similar list of considerations in determining adequacy, as shown above.

In 1999, the Commissioner’s Office produced the Data Protection Registrar’s Legal Analysis (the Analysis), which suggests a good practice approach for assessing adequacy.

The Commissioner recommends that data controllers:

1. Consider whether the country to which the data is to be exported is the subject of an EU finding of adequacy. Companies are required to refer to any European Commission findings of adequacy in making their judgement on transfer of data. So far, the European Commission has designated Canada, Hungary and Switzerland as having adequate data protection laws in place. Personal data can therefore be exported to these countries without infringing the eighth principle.

There are a number of other countries outside the EEA which have data protection laws, which may be designated as “adequate” in future. These include Australia, Guernsey, Hong Kong, Isle of Man, Israel, Japan, Jersey, New Zealand, Poland, Slovak Republic, Slovenia and Taiwan.

In addition, in July 2000 a “Safe Harbour” agreement was reached between the EU and the US to allow exports of data to the US to those companies registering in the US as prepared to comply with the US Safe Harbour Agreement. This is considered in greater detail below.

2. Where transfers are not to the US under Safe Harbour, or to Hungary, Switzerland or Canada, then it is necessary to consider the type of transfer involved and whether this enables any presumption of adequacy. For example, cross-border transfers to data processors are presumed, in most cases, to be adequate. (A data processor is any person who processes the data on behalf of the data controller.) This is subject to overall compliance with the Act, in particular the requirements relating to security, and the requirement that there should be a written contract between the controller and the processor (under the seventh principle).

The Confederation of British Industry (CBI) has identified six categories of transfer which require different methods to determine adequacy. The first is a transfer to a
third party processor, as above. The others are transfers within an international company, transfers within a consortium of independent organisations set up to process international transactions, transfers amounting to a licence for use in respect of personal data used, for example in direct marketing, and transfers which amount to sale of data to a third party with no continuing relationship with the third party (this would be likely to be inadequate).

3. Consider and apply the “Adequacy Test”, including consideration and use of contracts and/or codes of conduct to create adequacy. The Adequacy Test is discussed in detail in the Analysis. Basically, it involves assessing all the circumstances of the case and considering the nature of the personal data to be transferred, the purposes of the proposed transfer, the period during which the data are intended to be processed and any security measures taken in respect of the data (the General Adequacy Criteria). In addition, data controllers should consider the law in force in the third country, the international obligations of the third country and any codes of conduct enforceable in that country (the Legal Adequacy Criteria). These factors do not constitute an exhaustive list of the issues to be considered.

The Commissioner recognises that it may be inappropriate, difficult, time-consuming and/or costly to consider the Legal Adequacy Criteria in the case of every transfer.

Data Controllers must also carry out an adequacy/risk assessment to decide the extent to which the proposed transfer will prejudice the fundamental rights and freedoms of data subjects, and in particular their right to privacy with respect to the processing of personal data.

4. Where it is doubtful that there is adequacy, consider the derogations in Schedule 4 of the Act, as discussed above.

**CONSENT**

As mentioned above, one of the derogations to the eighth principle is that the data subject has given consent to the transfer. The Commissioner has provided guidance on what constitutes consent for these purposes in her Legal Guidance under the Act:

“Transfers can be made with the consent of the data subject. Consent must be freely given. It can be made a condition for the provision of a non-essential service but consent is unlikely to be valid if the data subject has no real choice but to give his/her consent. For example, if an existing employee is required to agree to the international transfer of personal data any consent given is unlikely to be valid if the penalty for not agreeing is dismissal. Consent must also be specific and informed. The data subject must know and have understood what he/she is agreeing to. The reasons for the transfer and as far as possible the countries involved should be specified. If the data controller is aware of any particular risks involved in the transfer it should bring these to the data subject’s attention. Although all the circumstances of a particular case would need to be considered, it is possible to give some general examples.”
By signing below you accept that we can transfer any of the information we keep about you to any country when a business need arises. | Unlikely to produce valid consent.
---|---
By signing below you accept that we may pass details of your mortgage application to XYZ Ltd in Singapore who we have chosen to arrange mortgages on our behalf. You should be aware that Singapore does not have a data protection law. | Likely to produce valid consent.
---|---
By signing below you agree that we may pass relevant personnel records to our subsidiary companies in any country to which you are transferred. Your records will continue to be handled in accordance with our code of good practice although you might no longer have rights under data protection law. | Likely to produce valid consent in the case of an employee of a multinational group who accepts a job involving international postings and where the multinational has a group-wide data protection code.
---|---
By signing below you agree that we may pass information about you and your policy to other insurance companies with which we reinsure our business. These companies may be located in countries outside the UK that do not have laws to protect your information. Details of the companies and countries involved in your case will be provided on request.” | Likely to be acceptable where it is not practicable to list all the reinsurers and the countries in which they are located because the list is too long, because it changes regularly or because different reinsurers from the list are used in different cases.
---|---

Data controllers cannot infer consent from non-response to a communication. Even where consent has been given, data subjects have the right to withdraw consent at any time.

**Transfer or Transit**

A “transfer” is not defined in the Act, but the ordinary meaning of the word is transmission from one place to another. Transfers of data are covered by the Act, but transits are not. A transit would occur where, for example an email is routed via servers in a number of different countries before reaching its final destination. The transit occurs in the countries the email passes through, and the transfer for the purposes of the Act is the sending of the email to the final destination.

Personal data which is placed on a web site would seem to involve transfers to countries outside the EEA. The transfers are to any countries from which the web site is accessed. It is unlikely that technical means will be available to web site owners to prevent access to their web site from certain countries, so it may be safest to assume that all personal data placed on a web site is exported for the purposes of the Act. However, it would be highly problematic if consent was required every time personal data was posted on a web page. A case is pending before the European Court of Justice to decide the issue of whether the posting of
personal information on a globally accessible web page constitutes a transfer of information outside the EEA. The case concerns a Swedish web site which contained information relating to the congregation of a church. The Swedish Data Inspection Board determined that the Personal Data Act had been violated and Bodil Lindquvist, who set up the web site, was fined. Bodil appealed and the question was referred to the ECJ. A decision is expected in the autumn.

**MODEL CONTRACT CLAUSES**

On 15 June 2001, the European Commission approved a set of model contractual clauses for use by data controllers who wish to export data outside the EEA. On 27 December 2001, the European Commission adopted standard contractual clauses for export of data outside the EEA by data controllers to data processors. By using the model contractual clauses, data controllers can ensure they fulfill the adequacy requirement of the eighth principle. Copies of the model contract clauses are attached at Appendix 1.

The use of the model terms is not compulsory. A data controller may still come to the conclusion that there is adequate protection in place without the use of the model terms.

The Commissioner has issued Legal Guidance in relation to the model terms for data controllers exporting to data controllers. The Commissioner takes the view that the following options are available to data controllers who wish to take advantage of the derogation which states that the eighth principle will not apply where the transfer has been authorised by the Commissioner:

1. Use of the model terms word for word as a stand-alone contract, with completion of the “blanks”;
2. Use of the model terms word for word, with completion of the “blanks”, but including further terms, provided that the further terms do not contradict in any way the model terms;
3. Incorporation of the model terms into a contract containing other business terms, either word for word or with minimal changes required solely to enable the model terms to fit the context of the contract, in both cases with completion of the “blanks”;
4. Incorporation of the model terms into a contract containing other business terms, by reference to the Decision, by including the following wording within the contract:

   "The Standard Contractual Clauses for the transfer of personal data to third countries under Directive 95/46/EC contained in the Annex to the Commission Decision of 15 June 2001 are incorporated into the contract with the following changes:

   Data Exporter shall mean [name of data controller organisation]

   Data Importer shall mean [name of data controller organisation to which data are transferred]

   In Clause 5(b) the box in the first subparagraph should be treated as [being/not being] ticked and the box in the second subparagraph should be treated as [being/not being] ticked.

   [Clause 8 shall not be incorporated]"

---

2 Bodil Lindquist v Aklagarkammaren i Jonkoping
With reference to Appendix 1:

The Data Exporter is [specify activities relevant to the transfer]

The Data Importer is [specify activities relevant to the transfer]

The personal data transferred concern the following categories of Data Subjects: [specify]

The transfer is necessary for the following purposes: [specify]

The personal data transferred fall within the following categories of data: [specify]

The personal data transferred fall within the following categories of sensitive personal data: [specify]

The personal data transferred may be disclosed only to the following recipients or categories of recipients: [specify]

The personal data transferred may be stored for no more than [specify] (months/years).”

The Analysis raises concerns regarding the enforceability of contracts between data controllers by data subjects, in the event that the parties to the contract do not enforce it. At the time the Analysis was produced UK privity of contract rules did not permit a person who was not party to an agreement to enforce it. However, the UK Contracts (Rights of Third Parties) Act 1999, which received royal assent on 11 November 1999, provides that a person who is not party to a contract may enforce a term of the contract if:

(i) the contract expressly provides that he may; or

(ii) the term purports to confer a benefit on him.

The individual must be expressly identified in the contract by name, as a member of a class or as answering a particular description. In data transfer contracts, the data subjects could be identified as a class. This removes the problem of privity of contract in the UK.

From the point of view of the data controller, some of the model contract terms are onerous. In particular, data subjects who enforce terms of the contract as third party beneficiaries are entitled to compensation for damage suffered, and the data exporter and importer are jointly and severally liable, with the liability being unlimited.

The data exporter also has to warrant that if the transfer involves sensitive personal data, the data subject has been or will be informed that the data could be transferred to a jurisdiction not providing adequate protection, and that it will provide data subjects with a copy of the data export agreement upon request, and that it will respond in a reasonable time and to the extent reasonably possible to any enquiries from the relevant supervisory authority, or from the data subject.

There are also a number of obligations on the data importer, including warranting that it has no reason to believe that local legislation in the country of receipt will prevent it from fulfilling its obligations under the contract.

Although the model terms present a solution to the requirements of the eighth principle, they may not be welcomed by companies outside the EEA, who have no local experience of
complying with the data protection requirements imposed by the model contract terms, and will be agreeing to be bound by EU laws and to being judged by EU courts.

ICC CLAUSES

On 17 September 2001, seven leading business organisations\(^3\) submitted an alternative set of model contract clauses to the European Commission for approval. A further draft was submitted in January 2002. The object of submitting alternative clauses was to adopt a more flexible, pragmatic approach than that adopted by the European Commission, but resulting in the same level of protection.

Businesses had a number of concerns regarding the European Commission’s model contract terms, including:

1. Confidentiality – the clauses allow data subjects to be represented in complaints by “associations”, which has the potential to expose confidential data to such groups.
2. Lack of commercial viability – for example, the parties undertake not to vary the terms of the clauses.
3. Conflicts with domestic law of the importer – obligations on data importers may conflict with requirements to which they are subject under domestic law.
4. Liability Concerns – as mentioned above, there are concerns regarding joint and several liability and the wide-ranging rights of data subjects to bring claims against data controllers.
5. Further Requirements – the contracting parties are required to provide substantial detail about the transfer.

The main differences between the Commission’s clauses and the proposed clauses are:

1. There are extra protections for data subjects, for example, upon request data importers must provide data exporters with evidence of adequate financial resources, and exporters must use commercially reasonable efforts to ensure that the importer can comply with its obligations.
2. The dispute resolution clause obliges the parties to abide by a decision of a competent court or data protection authority, once all appeals have been exhausted.
3. Provisions on auditing and inspection of the importer are more flexible.
4. The liability rules reflect existing data protection law (i.e. each party is liable for the damages it caused) and there is no joint and several liability.
5. The indemnity clause is not obligatory.

---

\(^3\) International Chamber of Commerce (ICC), the Federation of European Direct Marketing (FEDMA), the EU Committee of the American Chamber of Commerce in Belgium (Amcham), the Japan Business Council in Europe (JBCE), the Confederation of British Industry (CBI), International Communications Round Table (ICRT), and the European Information and Communications Technology Industry Association (EICTA).
6. The clauses may be varied to the extent the variation does not adversely affect data protection obligations to data subjects.

The current position is that the Article 29 group met on 5 September 2002 and the model contract was on the agenda. Some industry representatives were present at the meeting. It appears that the group’s attitude to the clauses is very negative, although the Commission is not as negative. There appear to be a few points which are sensitive, but it remains to be seen whether the Article 29 Working Party will reject the contract as a result. The next stage may be an opinion from the Working Party.

**US Safe Harbour**

The Safe Harbour Agreement between the EU and the US allows export of personal data to the US to companies which have signed up to the scheme. US companies were able to subscribe to the principles online at the US Department of Commerce’s website with effect from 1 November 2000. The list of subscribers is available on the US Department of Commerce website. There are now 231 subscribers, including Microsoft and Hewlett Packard.

The Safe Harbour is not generally available to financial services companies and certain other regulated industries, such as telecommunications, which are not regulated by the Federal Trade Commission because they fall outside of the Federal Trade Commission Act or outside of the ambit of the Department of Transportation. This means that banks, savings and loans and credit unions are not eligible for the Safe Harbour. However, the US Treasury Department, in conjunction with inter-agency counterparts, has recently resumed discussions with the European Commission in an effort to resolve this issue. The latest round of talks, held in Brussels in July, was called “productive”, but were intended primarily as an opportunity to exchange information. US and EU officials said that when the Safe Harbour agreement was reached, financial services could not be covered because the Gramm-Leach-Bliley Financial Services Modernisation Act of 1999 had not yet taken effect. The GLB has now come into force (1 July 2001) but financial services are still not covered under the Safe Harbour.

US firms are now seeking an adequacy determination for the privacy provisions of the GLB and other US and state statutes rather than eligibility for US financial services under the Safe Harbour.

It is understood that the EU has concerns, for example, that personal data which is transferred from the EU to the US may leak into the US system in general beyond the intended recipient. They also have concerns over whether the privacy rules that apply to the initial recipient will also apply to other recipients, and whether there is recourse to proper dispute resolution procedures.

Even if an adequacy determination is made, it normally takes at least four to five months for the decision to be formally implemented.

The US Department of Commerce web site lists a number of benefits of the Safe Harbour, including:

---

5 [http://web.ita.doc.gov/safeharbour/SHList.nsf/webpages/safe+harbour+list](http://web.ita.doc.gov/safeharbour/SHList.nsf/webpages/safe+harbour+list)
1. All 15 member states of the EU will be bound by the European Commission’s finding of adequacy;

2. Companies participating in the Safe Harbour will be deemed adequate and data flows to those companies will continue;

3. Member state requirements for prior approval of data transfers will either be waived or approval will be automatically granted; and

4. Claims brought by European citizens against US companies will be heard in the US subject to limited exceptions.

Other advantages are that the safe harbour provides predictability and continuity, a single privacy regime for all US companies, it is less expensive and more targeted than other methods of compliance, and companies can sign up by category of personal data, such as human resources, on line or offline. Conversely, there are disadvantages, for example the unpredictability of the Federal Trade Commission assuming new regulatory and enforcement powers with no track record, and the fact that the regime is not available for financial services companies.

Organisations which have joined the Safe Harbour are required to comply with seven Safe Harbour principles:

1. **NOTICE**

   Organisations must notify data subjects of the purposes for which their data will be used, provide information on how data subjects can contact them with inquiries or complaints, the types of third parties to which it discloses the data and the choices and means offered for limiting its use and disclosure. For a third party which is acting as an agent, notice and choice (see below) do not need to be provided.

2. **CHOICE**

   Data subjects are to be given the choice to opt out of their data being disclosed to a third party, even if for the same purpose for which it was originally collected, or used in any way which is incompatible with the purposes for which it was originally provided or subsequently authorised by the data subject.

   Organisations must give data subjects explicit choice to opt in, in respect of sensitive personal data (e.g. medical conditions, racial origin), where the information is to be disclosed to a third party or used for a purpose other than that for which it was originally collected.

3. **ONWARD TRANSFER**

   When disclosing information to third parties, organisations must apply the notice and choice principles. Where the third party is acting as an agent, the organisation may transfer data as long as it ensures that the third party subscribes to the Safe Harbour principles, or is subject to the Directive or another adequacy finding, or the organisation enters into a written agreement with the third party requiring that the third party provides at least the same level of privacy protection as is required by the relevant principles. If the organisation complies with these requirements, it shall not
be held responsible (unless the organisation agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organisation knew or ought to have known the third party would process it in a contrary way and the organisation has not taken reasonable steps to prevent or stop such processing.

4. **ACCESS**

Data subjects are entitled to access to their data, and to correct, amend or delete the information where it is inaccurate.

5. **SECURITY**

Organisations are required to take reasonable precautions to protection personal data from loss, misuse and unauthorised access, disclosure, alteration and destruction.

6. **DATA INTEGRITY**

Organisations must ensure that data is relevant, accurate, complete and current.

7. **ENFORCEMENT**

There must be dispute resolution procedures in place to investigate and resolve complaints and award damages where the applicable law or private sector initiatives provide. Sanctions must be sufficiently rigorous to ensure compliance by the organisation.

Sanctions which may be applied by dispute resolution bodies must include publicity for findings of non-compliance and deletion of data in certain circumstances. They may also include suspension from membership in a privacy program (and thus effectively suspension from the Safe Harbour) and injunctive orders. In addition, the Federal Trade Commission, comparable US government agencies and/or the states may provide overarching government enforcement of the Safe Harbour principles. The Federal Trade Commission would take action in relation to unfair or deceptive practices in or affecting commerce.

So what has the reception been to the Safe Harbour in the US?

On 8 March 2001, the Subcommittee on Commerce, Trade and Consumer Protection of the House Committee on Energy and Commerce held a hearing on the Directive and the Safe Harbour. Members of the subcommittee raised concerns regarding the implications of the Safe Harbour for trade within Europe. In particular, there were concerns that the Safe Harbour would impose enormous added costs and legal liabilities to American companies that conduct business on-line.

In February 2002, the EU Working Party concluded that a “substantial number” of Safe Harbour self-certifying organisations lacked sufficient “transparency” and “less than half” of Safe Harbour participants post privacy policies that reflect all seven principles. On 2 July 2002, the data protection Working Party produced a Working Document on Functioning of the Safe Harbour Agreement. The review found that the Working Party should be provided with up to date information in respect of some issues related to implementation of

---

the Safe Harbour agreement. It calls upon all the authorities, organisations and associations concerned to collect, by 31 October, updated, specific information including relating to:

1. Arrangements to increase transparency in respect of the signatory organisations;
2. Verification mechanisms in respect of the procedure for adhering to the agreement;
3. The initiatives to be adopted to enhance knowledge of the prerequisites for adherence to the Safe Harbour; and
4. The measures to be adopted to refine dispute resolution mechanisms and arrangements for cooperation between the European data protection panel, dispute resolution bodies and the Federal Trade Commission.

The Safe Harbour is to be formally reviewed in July 2003.

**DIRECT COMPLIANCE**

An alternative suggested by some commentators is for data importers outside the EEA to comply with EU data protection laws. This approach has not been officially approved, but could possibly be used to ensure that the adequacy requirement of the Directive is satisfied.

This approach would be suitable for multinational companies transferring personal data within the same corporation, or among parents, subsidiaries and affiliates that are under common control. The company would adopt a company wide data protection policy which ensures compliance with the principles of the Directive with respect to personal data transferred from the EEA. The company would then make its own determination that intra-company transfers of personal data are adequately protected for the purposes of the Directive. The policy and adequacy determination would be submitted for approval to the data protection authority of the country exporting the data. However, it is not clear that in the UK the Information Commissioner would give their approval. In the 1999 Analysis the Information Commissioner stated that she would only give approval to a transfer as ensuring adequate safeguards in accordance with the final derogation from the Eighth principle in extremely limited circumstances.

**OECD GUIDELINES**

On 23 September 1980, the Organisation for Economic Co-operation and Development (OECD) adopted guidelines on the protection of privacy and transborder flows of personal data. The guidelines have had an important influence on the development of privacy laws internationally.

The aim of the guidelines is to provide protection for individuals as well as allowing a free flow of information for trade purposes. The guidelines consist of five parts. Part One contains definitions and specifies the scope of the guidelines, indicating that they represent minimum standards. The basic principles set out in Part Two of the guidelines include recommendations on collection limitation, purpose specification, use limitation, security safeguards, openness, individual participation and accountability. Part Three deals with principles of international application. Part Four covers means of implementing the basic principles and Part Five is concerned with mutual assistance between member countries of the OECD.
SUMMARY AND CONCLUSION

The Directive contains important provisions relating to transborder data flows for processing purposes, and these have been incorporated into the UK Act as the eighth principle. The Commissioner has produced guidance on the issue and the European Commission has approved model contract clauses and come to an agreement on Safe Harbour with the US, in order to allow transfer of data out of the EEA.

The legislation relating to transborder data flows are provided to protect data subjects, but it is not surprising that the Directive has caused much debate in countries outside the EEA, which feel that the Directive is creating global legislation by the back door by imposing obligations on organisations outside the EEA to comply with EU laws.
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

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
Tel +44 (0) 20 7626 7937
WWW.SIDLEY.COM

ALL PARTNERS ARE EITHER SOLICITORS OR REGISTERED FOREIGN LAWYERS

This briefing has been prepared by Sidley Austin Brown & Wood, London for informational purposes only and does not constitute legal advice. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this without seeking professional counsel.

Copyright © Sidley Austin Brown & Wood, London 2003
APPENDIX 1

Commission Decision of 15 June 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries

Commission Decision of 27 December 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Processors established in Third Countries