Legal and Regulatory Update

Exporting personal data

Christine Reid

Received: (in final form): 23 October 2001

Christine Reid
A partner at law firm Manches, Christine Reid is an expert in information technology law, and advises on a wide range of IT related matters, including contracts for the development and licensing of software systems, hardware sales and purchases, systems support and maintenance, outsourcing and facilities management, consultancy services, data supply, business contingency arrangements, the Internet, data protection and intellectual property rights in connection with software and data.

Keywords: customer relationships, marketing software, application service providers, CRM, software vendors, outsourcing

Background

The European Commission has published model contract terms with a view to bringing some certainty as to how data controllers who need to send personal data overseas can do so without falling foul of the Data Protection Act. This paper has been prompted by the controversy generated by various drafts of those terms; but first some background.

The UK Data Protection Act 1998 came into force on 1 March 2000. It implemented the 1995 European Data Directive. Some countries in the European Union are still in the course of implementing it; not until 18 July 2001 was a bill on the protection of individuals regarding the processing of personal data presented to the French Council of Ministers, so even within Europe we have still not achieved the harmonisation of data protection laws that the European Commission set out to achieve in 1995.

Transferring data abroad

The eighth data protection principle

One of the most frequent and loudly voiced criticisms of the 1995 European Data Directive was that it would seriously hinder trade with countries outside the European economic area, particularly the USA. The provision that gave rise to these criticisms is now encapsulated in the eighth principle of the Data Protection Act 1998. That principle states:

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

(The EEA consists of the 15 member states of the European Union, plus Norway, Iceland and Liechtenstein.)

It was clear from the very beginning that major trading partners such as the USA, with its emphasis on freedom of information and with no equivalent of the Data Directive, did not ensure a level of protection for the rights of data subjects that the European Commission would consider to be adequate.

What is a transfer?

There has been much debate as to what amounts to a transfer for the purposes of the eighth principle. The Data Protection Act does not define the term. The UK Information Commissioner has expressed the view that it means 'to convey from one place, person, ownership, object, group etc, to another'. This is wide enough to cover a UK company sending personal

Christine Reid
Manches,
3 Worcester Street,
Oxford OX1 2PZ, UK
Tel: 44 (0)1865 722106
Fax: 44 (0)1865 201012
E-mail:
Christine.Reid@manches.co.uk

data to another member of its group of companies in the USA, perhaps because one of its members of staff is about to transfer to the Chicago office; or releasing personal data about its customers and contacts to a prospective purchaser of the business who is based outside the EEA; or someone in the UK office forwarding an e-mail to a colleague in the USA; or details of the customers of a UK company being processed in a customer relationship management centre in India.

That a transfer of personal data is taking place may not be immediately obvious: to take the first example above, the US office may access the UK database without anyone in the UK actively sending any data to the USA; or the personal data may be transferred in the course of a telephone convesation between someone in the UK office and someone in the US office; or an employee of the UK company may remotely access the UK database from his laptop whilst he as abroad on business. Publishing personal data on a website that may be accessed from anywhere outside the EEA is also a transfer of that data for the purposes of the eighth principle.

Personal data on websites

Adequacy

It is the duty of the data controller (that is, the individual or company that decides the purpose for which any data are to be processed and how they are to be processed) to decide whether or not any country to which the data are to be transferred affords an adequate level of protection for the rights and freedoms of data subjects. The onus is on the data controller to carry out a risk assessment each time personal data are transferred outside the EEA. Factors to take into account include the following.

Risk assessment

— The nature of the personal data. (At one end of the spectrum, are the data sensitive or, at the other end of the spectrum, are they widely known?)
— The country of origin of the data. (If the original country had poor data protection laws is there any reason why the data subject should be placed in a better position than if the data had never come into the EEA?)
— The country of final destination of the data. (If the data controller is making an initial transfer to a country which has been designated — see below — but is aware that the data will be transferred to a country with poor data protection laws, this should be taken into account.)
— The purposes for which, and the period for which, the data are intended to be processed. (The longer the period of processing, the greater the risk to the data subject's rights is likely to be.)
— Whether the data protection laws in the country of destination are adequate.
— The international obligations of that country.
— Any relevant codes of conduct or other rules in that country.
— The security measures taken in that country — for instance, is there compliance with BS7799 and will the data be encrypted?

It may not be an easy task for the controller to make a judgment as to the

Does the country have adequate data protection laws

adequacy of the data protection laws of another country. The Information Commissioner suggests that controllers look at whether the laws of that country limit the purposes for which personal data may be processed; whether there is a rule that personal data be accurate and kept up to date; whether there are rules about informing the data subject as to who is processing his data and the purpose of that processing; whether the law insists that technical and organisational measures are to be taken to protect the security of the data; whether data subjects have rights of access to their data, the right to rectify incorrect data, and the right to object to the data being processed; whether further transfers are restricted in a way similar to that under the eighth data protection principle; whether there are safeguards in relation to the processing of sensitive personal data; whether the data subject can prevent his data being used for direct marketing; and whether the data subject has the right to know the logic behind any automated decision making that affects him. In short, the data controller is to take a view on whether or not the country to which the data are to be transferred protects the rights of data subjects in the same way that they are protected within Europe. Only rarely will the answer to this question be in the affirmative.

Designated countries

The 'white list'

To help data controllers to make this assessment, it is intended to have a 'white list' of countries that have been designated by the European Commission as having adequate protection, but it seems that nothing moves quickly in the area of data protection; to date the European Commission has decided that only Switzerland and Hungary have an adequate level of protection, although discussions are under way with Australia, Canada and Japan. The likelihood is that some countries will be designated only for certain types of transfers so that, even if a country appears on the 'white list', sensitive personal data should not be transferred to that country, or possibly that data should not be transferred to it for the purpose of direct marketing or automated decision making. (Sensitive personal data are data concerning such matters as racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life and the commission of a criminal offence.)

CBI recommendations

The Confederation of British Industry (among others) has been concerned about how transfers of personal data outside the EEA will operate in practice and has been very active in suggesting changes to the model contract terms proposed by the European Commission. The CBI has identified the following types of transfer that it believes present a lesser or greater risk to the rights of data subjects.

Transfers to a third party who processes the data on behalf of the controller

In this instance, in order to comply with the seventh data protection principle even where the data are not being transferred outside the EEA, the data controller should have a written contract with the data processor that prohibits the processing of the data except in accordance with the controller's explicit instructions; that provides sufficient guarantees about

the technical and organisational measures taken to protect the security of the data; and that allows the controller to monitor the steps being taken to ensure compliance. This sort of contract, if properly drafted and enforced, should be sufficient to meet the adequacy test. (See the final exemption listed below and the section of this paper on the draft model clauses proposed by the European Commission.)

Transfers within a group of companies where there is an internal agreement in place
The internal agreement should be similar in its scope to the contract mentioned above, but it may be more convenient to have an internal policy or code rather than individual contracts between each member of the group.

Sector-specific protections

Transfers within a consortium of organisations that processes international transactions, such as banks
Here there may be sector-specific regulations that help to protect personal data.

Transfers between professionals such as lawyers
Again there may be (but will not always be) professional duties of confidence or other rules that protect data subjects.

Transfers that are akin to a licence to use, such as transfers of data for the purpose of direct marketing
In this sort of case there may be terms in the licence that restrict the use and onward transfer of the personal data.

Transfers that are akin to a sale of the data where there is no continuing relationship between the data controller transferring the data and the recipient
This presents the greatest risk that the personal data may be used in a way that impinges on the rights of the data subject.

Circumstances of the transfer

These categories are not part of the Data Protection Act, but they may help data controllers to evaluate the circumstances of the transfer and the risks involved in making it. They may help focus the mind on the fact that 'adequacy' will depend not only on the law in the country to which the data are transferred but also on the circumstances of the transfer.

Safe harbours

Last year and after much debate, the European Commission and the US government attempted to bridge the difference of approach between European Data Protection Principles and the US preferred option of the minimum of regulation (or at least a mix of legislation, regulation and self-regulation) by agreeing some safe harbour principles. Under these, the US Department of Commerce maintains a list of US companies that have agreed to adhere to requirements that, in the opinion of the European Commission, provide adequate protection for the rights of data subjects.

The safe harbour principles are as follows.

US principles

— The US company must inform individuals about the purposes for which personal data are collected and used, and how to contact the company if the individual wants to make a complaint or raise a query.
— Individuals must be given the opportunity to opt out if their data are to be disclosed for a purpose or used for a purpose incompatible with the purpose for which the data were originally collected.
— Disclosures to third parties must be consistent with the two principles above (notice and choice).
— Reasonable precautions must be taken to protect personal data from loss, misuse, unauthorised access, disclosure etc.
— Personal data must not be processed in a way that is incompatible with the purposes for which they were collected.
— Reasonable steps should be taken to ensure that the data are accurate, complete and current.
— Individuals must have access to their personal data and be able to have them amended, corrected or deleted.

To come within the safe harbour category, a US company must bind itself publicly to the safe harbour principles, by developing its own policies, participating in an industry programme (such as TrustE), or relying on US sector regulation. One of the requirements is the publication of a privacy policy.

The safe harbour website

Companies self-certify that they comply with the safe harbour principles. Certified organisations are listed at www.ita.doc.gov/ecom, the Department of Commerce's website. The first step for any data controller wishing to transfer personal data to someone in the USA is to go to that website and check whether the company's name appears on the list.

If a company on the list does not comply with the safe harbour principles, it will be subject to legal sanctions, for instance under s. 5 of the US Federal Trade Commission Act which outlaws misrepresentation and deceptive trade practices.

The safe harbour framework took months to negotiate with the Clinton administration, but the approach of the Bush administration is rather different and the safe harbour scheme has not proved popular with US businesses. Republicans argue that the European Data Directive is a restraint on trade. There is, however, hope on the horizon; the safe harbour scheme was given greater credibility recently when Microsoft decided to join.

Exemptions or derogations

The eighth data protection principle does not apply if the transfer falls within one of the following exemptions.

Consent

— The data subject has given his consent to the transfer. Consent is not defined in the Act but, as a general rule, consent must be freely given, informed, specific and active; it may not be implied from silence, but it may be inferred from action. For instance a visitor to a website may

be clearly informed, before he gives any information about himself, that his data may be transferred to a company outside the EEA and how the data will then be used — it is advisable to be specific if the data are to be used for direct marketing purposes. If the data subject then proceeds to submit his data you may infer that he is consenting to its transfer and use in this way. If sensitive personal data are being processed the data subject's consent must be explicit and therefore the data controller should make sure that the site contains a conspicuous notice to the effect that in submitting his data the data subject is consenting to the proposed transfer and use.

— The transfer is necessary for the performance of a contract between the data subject and the transferring controller, for example a travel agent making a hotel booking.

— The transfer is necessary for taking steps at the data subject's request with a view to entering into a contract with the data controller, for instance where a credit card company provides authorisation to an overseas Web merchant.

Necessary for contract

— The transfer is necessary for the conclusion of a contract between the controller and someone other than the data subject and that contract is entered into at the request of the data subject, or is in the data subject's interests.

— The transfer is necessary for the performance of such a contract.

— The transfer is necessary in connection with legal proceedings, obtaining legal advice, or exercising or defending legal rights.

— The transfer is necessary to protect the data subject's vital interests. Here the word 'vital' is used literally — it must be a matter of life or death.

Public interest

— The transfer is necessary for reasons of substantial public interest. This is likely to be in connection with the prevention and detection of crime.

— The transfer is an extract from a public register, provided the transferee complies with any restrictions on the use of that register.

— The transfer has been authorised by the Commissioner. This exemption is not intended to be widely used and the Information Commissioner will consider applications for authorisation only in limited circumstances.

— The transfer is made on terms of a kind approved by the Commissioner. The UK Information Commissioner has stated that she is likely to approve any terms approved by the European Commission.

If a controller wishes to send personal data to a company in the USA that is not on the Department of Commerce list or to a company elsewhere outside the EEA, it may do so provided an adequate level of protection for data subjects exists and that protection can be given by having a contract between the data controller who is transferring the data (in this case known as the exporter) and the recipient of the data (or the importer).

Draft model clauses

That brings us to the draft terms that have prompted this paper, or to give them their full title, 'The Draft Commission Decision on Standard

Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries'. The first draft of these terms appeared in the autumn of 2000. There was much adverse comment followed by a period of intensive consultation. Various revised drafts have been published, the latest on 1 October 2001. Member states were to comment on this draft at a meeting on 23–24 October and then the European Parliament will consider the draft. They are expected to be in final form by the end of 2001.

Model clauses website

A copy of the full text is available at http://europa.eu.int/comm/internal_market/en/dataprot/news/sccprocessors.htm.

The draft clauses are not short; they run to five pages, excluding the appendices that are designed to cover details of the data exporter's and the importer's activities, the data subjects, categories of data, sensitive data, processing operations and the technical and organisational measures to be taken to protect the security of the data. They envisage that the scenario is as in the first of the CBI's category of transfers.

Normally in England we expect a contract between A and B to define the rights and obligations of A and B, but the aim of the Data Protection Act is to protect the rights of data subjects. Therefore the contract between A and B, or the data exporter and the importer of the data, is designed to be enforceable by the data subject. That is still a fairly revolutionary concept in English law. We adopted the principle of third parties having rights under contracts only a couple of years ago; until then the doctrine of privity of contract did not allow anyone who was not a party to a contract to enforce it.

Who is liable?

In the early drafts of the model clauses it was envisaged that the data exporter and the data importer would be jointly liable to pay damages to the data subject whose data were unlawfully processed. This has now been changed, so that the data subject may enforce the clauses against the exporter and only against the importer in exceptional circumstances, for instance where the exporter has gone into liquidation or, without legitimate grounds, has refused to give instructions to the importer.

Under the clauses the data exporter gives warranties that will be enforceable by both the importer and the data subject. They include that the processing has been and will be carried out in accordance with data protection law, that the data importer is instructed to process only on behalf of the exporter and in accordance with data protection law, that the importer has given sufficient guarantees in relation to security measures, and that those measures are appropriate to protect the data and the exporter will ensure compliance with them. The effect of this is to give the data subject rights against the exporter for breach of contract in addition to the data subject's rights under the Data Protection Act, and the exporter will clearly be liable to the data subject if the importer misuses the data.

Dispute resolution

The exporter is obliged to give data subjects a copy of the clauses on request. This does not reflect any explicit provision of the Data Protection Act, but it is consistent with legislation that seeks to protect the rights of individuals and give them sufficient information to put them in a position to be able to enforce those rights.

The data importer agrees that data subjects may refer any dispute to mediation or the courts of the exporter's country, and that the supervisory authority (in the UK the Information Commissioner) may audit the data importer. The law applying to the contract is to be the law in the country where the exporter is established.

It is clear that the model clauses attempt to impose on non-European companies the data protection rules that the European Commission would like to see adopted — the data importer has to agree to process in accordance with the laws of the country in which the exporter is established.

The US Department of Commerce has criticised an earlier version of the model clauses as being 'unduly burdensome and . . . incompatible with real world operations'. It is likely that many will take the same view of the latest draft.