

Protecting personal information — over there

A look at privacy in the European Union

By Alison Wetherfield

There are times when European lawyers feel like the bearers of unnecessarily bad news to our U.S. clients.

“So, run that past me again,” says the client. “The expensive software we just bought that lets me transfer data about our European customers and employees to the U.S. at the press of a button — it may infringe data protection rights? I have to get individual written consent from Spain? And the French could fine me thousands of Euros for getting this wrong? And each of the European Union member states deals with this in a slightly different way? . . . Wonderful, tell me more.”

European data protection law can be a shock to the system. But clients can learn to love it. When a U.S. company shows that it abides by its European data protection obligations, it signals to its European customers and employees that it understands the European trading environment and is a sophisticated player.

The basic principles are not difficult to explain. All European Union member states (see the sidebar, *Who's in the EU*) are required to have domestic legislation implementing a 1995 directive “on the protection of individuals with regard to the processing of personal data and on the free movement of such data” — otherwise known as the

European Data Protection Directive. The directive reflects broad agreement that data about living individuals should be protected through a system of external supervision.

As a result, in all the separate European Union member states, data protection rules exist governing “data processing” — a definition covering any and all activity involving data, including collection, storage, transfer and destruction. The core rules are uniform and represent, in the main, a sensible basic code of practice for the processing of information.

In each separate jurisdiction in the EU, an institutional mechanism also now exists to allow independent investigation of complaints about data handling. A system of independent adjudication exists that allows compensation to be paid and sanctions imposed where appropriate.

Unfortunately, the relevant bodies have different names and powers and the sanctions also vary in each jurisdiction — another of those areas where the margin allowed for different approaches to implementation of European Union directives can drive one a little crazy. But the principle remains the same: Data protection *has* to be taken seriously. (See the sidebar, *Some basic definitions*.)

To illustrate the implementation, in the United Kingdom, where I practice, the relevant legislation is the Data Protection Act 1998, which:

- sets out eight “data protection principles” (the core rules) with which

all “data controllers” must comply;

- provides access to the courts in the event of breach of the principles or violation of certain rights enjoyed by “data subjects” (living individuals about whom data is processed);

- regulates the actions of the information commissioner, an independent ombudsperson to whom data subjects may also apply, and whom data controllers must “notify” regarding the purposes for which they process most data;

- gives the information commissioner powers to launch investigations of businesses in their role as data controller where individuals make complaints, and to issue “enforcement notices” backed up by the threat of fines of up to £5000 (or depending on the exchange rate, about \$9,000) for each data protection breach.

Turning back to commonalities across the European Union, the core data protection rules that all member states have implemented require, in summary, that data shall be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate
- not kept longer than necessary
- processed in accordance with the data subject's rights
- secure, and
- shall not be transferred to countries outside the European Economic Area (the 25 EU states plus Iceland, Liechtenstein and Norway) unless that country or territory ensures an ade-

Wetherfield is a partner at McDermott Will & Emery in London. Her e-mail is awetherfield@europe.mwe.com.

1 • Business Law Today • American Bar Association • November/December 2004 • Volume 14 • Number 2

“Protecting personal information — over there” by Alison Wetherfield, published in Business Law Today, Volume 14, No. 2, November/December 2004

© 2004 by the American Bar Association. Reproduced by permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

Who's in the EU

The member states of the **European Union** are: **Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, the United Kingdom, Cyprus, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovakia and Slovenia.**

The **European Economic Area** (which is relevant for data-transfer purposes) is all these countries plus **Iceland, Liechtenstein and Norway.**

quate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data (unless an exception to the rule applies).

It's that last principle that always surprises. A transfer is a transmission from one place or person to another with the intention that it be processed on receipt. Mass data transfers from computer to computer using telecommunication systems count. So too does the provision of information by someone in Europe to someone in the United States over the phone who then enters the information into a computer or into a paper-based filing system. Do the Europeans seriously believe they can monitor or stop this sort of data flow to and from businesses in Europe?

No, they don't. Spain, though, may be an exception. It has implemented the directive so narrowly as to require individual written consent to transfers of personal data to the United States. This is more often breached than observed, as might be expected given the level of information flow, but U.S. businesses in Spain get used to drafting consent lines into even the simplest

data collection forms.

Broadly, elsewhere in Europe, a number of exceptions to the rule usually apply, covering most legitimate business-related transfers. But the rule does mean that transborder dataflows may have European legal consequences that should be considered in advance of a data transfer. Any business with physical premises in a European jurisdiction that transfers data to a country without "adequate data protection laws" could be in breach and a data subject could exercise legal rights against it in the European jurisdiction.

The existence of the rule has, for example, shaped much of the European debate on a thorny subject also much in the U.S. media — the outsourcing of clerical and other services to India and other developing countries. While the European debate sounds all the same notes heard in the United States — the effect on the domestic workforce, the benefits for the global economy and so on — in Europe, we also discuss whether a developing economy could possibly ensure an adequate level of protection for the data identifying our individual customers and employees that would need to be exported to that economy in the course of the outsourcing. The labor unions have made a powerful argument out of this.

India has responded to this by accelerating plans for both federal and regional laws modeled on the European Data Protection Directive. ("Oh great!" says the long-suffering client. "So I'm going to have to register there with some body or three *as well* ...").

Back in Europe, the "exceptions to the rule" allow the European Commission to make a "finding" that a named country outside the European Economic Area (EEA) ensures an adequate level of protection by reason of its domestic law or international commitments. So far, however, the somewhat unlikely assortment of countries so recognized comprises only Argentina, Canada, Switzerland, Guernsey (one of the Channel Islands between Great Britain

and France), and the Isle of Man (a tiny 33-mile-long self-governing island between Great Britain and Ireland).

Where does this leave the United States? Despite the sentiments of some U.S. clients (particularly in the health-care sector, since the enactment of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)) that use of data is increasingly regulated at home, the European Commission has only recognized adequacy of protection for data transferred to the United States in two narrow situations.

In May 2004, it recognized adequacy of protection for personal data contained in the passenger name records of air passengers transferred to the U.S.' Bureau of Customs and Border Protection. In July 2000, it also recognized that U.S. corporations that have signed up for the Department of Commerce's Safe Harbor program adequately protect European data.

So what is the Safe Harbor program? Personal data can lawfully be sent from a European Union member state to a U.S. recipient after the U.S. undertaking has certified its adherence to the "Safe Harbor principles" devised by the U.S. Department of Commerce. Safe Harbor essentially provides a set of privacy principles that replicate the data protection principles enshrined in the directive concerning:

- notice (of intended use and intended recipients, and of how to limit use and make enquiries and complaints)
- choice (both opting out and opting in to proposed uses)
- onward transfer to third parties
- security
- data integrity
- data subject access rights
- enforcement mechanisms (including effective follow-up procedures).

Certification is annual, and involves providing the U.S. Department of Commerce with information about the undertaking and its intended use of the data.

Safe Harbor has its own drawbacks,

even though it does allow blanket transfer of personal data. First, it operates only between the European Union and the United States, and obviously many U.S. businesses will need to transfer data globally. Second, it requires the implementation of effective enforcement measures, involving independent mechanisms for investigation and resolution of complaints (including by way of the award of damages in appropriate cases).

Third, the sanctions the business agrees it will submit to if it does not live up to the principles have to be sufficiently rigorous to ensure compliance. This means that where a business relies to any degree on self-regulation, any failure by it to comply must fall under the enforcement jurisdiction of the Federal Trade Commission under Section 5 of the FTC Act, which deals with unfair or deceptive acts or practices (or in some circumstances under the jurisdiction of the U.S. Department of Transportation).

This all sounds very onerous. Examination of what is actually required of those organizations that sign up for Safe Harbor is, however, quite illuminating. It is a self-certification plan. The two most important components of the plan are the adoption of a “privacy policy,” and the provision of an independent recourse mechanism for investigation of any unresolved data subject complaints. These two elements have deterred many organizations.

It is important to note, however, that the scope of the privacy policy required is very limited. It does not have to relate to all data processed by the U.S. business, only to the types of data that might be transferred from its business or establishments in the EEA. Some entities that have signed up for Safe Harbor have indeed drafted long and complex privacy policies, which may, for example, in the health-care sector try to state in simple terms all HIPAA obligations — but that is not necessary.

It is also important to note that the

independent recourse mechanism need not involve great expense or exposure. Perhaps because of the disappointingly small number of organizations signing up for the plan, the U.S. Department of Commerce has agreed that if U.S. entities pay an annual fee and agree to cooperate with European Union member state data protection authorities and to accept their advice on remedial and compensatory measures for the benefit of individuals, that will suffice.

The EU has created a “data protection panel” staffed with representatives from the various member state data protection authorities to do this. If the panel were to operate and find deception or misrepresentation as to how transferred data had been used, they have the power to tell the Department of Commerce to remove the U.S. entity from the scheme, and the FTC powers under the FTC Act are always a back-

up threat.

Note, however, that so far, three years into the plan, the panel has attracted very little publicity. The European Commission Web site has a “members’ only” access control to any parts related to the panel. This suggests that its activities are carried out discreetly.

So is joining Safe Harbor advisable? U.S. businesses operating in Europe and facing criticism from employees, customers and commercial counterparties for not having thought through data transfer matters often consider it. But it is not the only way to silence critics. There are a number of other ways to satisfy European laws; more are in development.

Consent of the individual when the data is first collected may be the simplest route in some situations. Many companies devise pop-up screens

Some basic definitions

The EU Directive’s goal is achieved by the regulation of *processing of personal data about data subjects by data controllers*. The italicized concepts are critical. References to articles are to parts of the directive.

- **Processing** has an extremely broad definition. It covers all processing of data, online and off-line, manual (if in structured sets/files of data) as well as automatic (Article 3).

- **Personal data** is defined as information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity (Article 2). If data truly cannot be identified, the directive does not apply.

- **Data controllers** are the persons (in the European Union) who determine the purposes and means of the processing of personal data. Where a U.S. business has an establishment or makes use of equipment in an EU jurisdiction, it is likely to be a data controller. In relation to any particular data, there can be multiple data controllers if each entity is using the data for different purposes.

- **Data subjects** are the identified or identifiable people about whom data is processed (Article 2). The nationality and country of residence of data subjects is irrelevant. They are protected by the directive as implemented by the laws of a particular European Union member state so long as the relevant data controller has an establishment or makes use of equipment in that state.

— Alison Wetherfield

when collecting data from individual customers online, giving details of the purposes for which the data is collected and explaining where and how it will be used. If a customer cannot submit data without checking a screen box that he or she has been able to view this information and is happy to provide it in that knowledge, an electronic record of consent is created.

Model contractual clauses devised by the EU (incorporating all sorts of rights for data subjects, even if they are not party to the contract) are another alternative where the parties transferring and receiving data are not part of the same group. U.S. businesses in Europe quickly become accustomed to seeing clauses of this type. They are not mandatory. Legal advice should usually be sought if they become a deal breaker because alternatives do exist.

The European Commission is also working hard to develop model intra-group privacy policies that would satisfy the data transfer rules if adopted and enforceable in a number of jurisdictions. Many large groups are waiting to see whether these policies would be suitable for them. Some household names, like DaimlerChrysler, are investing considerable resources in their development. These policies

essentially take internal data handling and privacy policies (which are by now fairly standard in mid- and large-size businesses operating in the European Union) and make them contractual, so that the data controller can be sued for breach.

Then there are also pragmatic responses in particular jurisdictions. In the UK, for example, the legislation suggests that there is a strong *presumption of adequacy* on which the data controller with a legitimate business need to transfer data may rely. This presumption applies if there has been a risk assessment of:

- the nature of the personal data,
- the country of origin and final destination of the data,
- the purposes for which the data are intended to be processed,
- the period during which the data are intended to be processed, and
- any security measures taken in respect of the data in the third country,
- any legal measures in the jurisdiction providing any data protection rights (most important to security of data) and enforcement mechanisms. If the data controller decides, following such a risk assessment, that the level of protection afforded is adequate, that is, commensurate with any potential risk

to the rights and freedoms of the data subject, transfer may take place without breach of the UK's Data Protection Act.

Many U.S. businesses exporting data from the UK to affiliated companies in the United States make exactly this sort of risk assessment informally. Taking the additional step of paper trailing the thought process and checking the assumptions (particularly as to access to the data once in the United States) is a good idea if this approach is adopted.

The directive's exceptions can often therefore swallow the rule on permissible data transfer.

"So", says the client, "provided I let the clients and employees know how I want to transfer the data and why, and I think through how we'll provide security for the data and ensure that it does not go to third parties the data subjects don't know about, and we get a consent mechanism in place in Spain, and I develop a privacy policy and I think through whether we want to join Safe Harbor or use model clauses or contractual policies or just make a serious assessment of adequacy for particular transfers, we should be all right?"

"I suppose that makes sense. I may not like it, but at least I understand it."