European Data Protection: Handling Data Security Breaches

Axel Spies

European "data protection" is a maze of rules and regulations: Currently, some 33 different European jurisdictions (including the 25 countries within the EU), from Lisbon to the Ural River, have data protection laws.

To be more precise, the term "data protection"—which Europeans use much more frequently than the term "privacy"—does not only mean that the data is protected. The laws protect the personal information of those individuals to whom the personal information belong—the so-called "data subjects."

"Data subjects" is a broadly defined category. In the UK, Section 1 of the Data Protection Act of 1998 defines the term as "an individual who is the subject of personal data." In most countries, data subjects are only individuals—with some exceptions. In Italy, for example, data subjects include legal entities as well as individuals—company data (for example, data relating to clients, suppliers or even competitors) would also be subject to data protection. In various EU member states, data subjects' rights are protected by the national constitutions. All of these countries are concerned about data security breaches affecting personal data.

Frequent Misperceptions By U.S. Companies

U.S. companies with customers or business in Europe sometimes have a poor knowledge, or none at all, when it comes to the European data protection concept:

■ **First Misperception**: In the EU, data protection is governed by the 1995 European Directive, the Data Protection Directive (95/46/EC).

Dr. Axel Spies is a German attorney in Bingham McCutchen's Washington, DC office. He focuses on international telecom and data protection issues; he has authored numerous articles and studies in both areas.

While the Directive is certainly a key document, many EU member states, such as Sweden and Germany, had data protection laws long before the Directive was adopted. For example, the Data Protection Act of the tiny German state of Hessen is approximately 20 years older than the Directive.

While the Directive contains the framework for national data protection legislation, it must be transferred (or "transposed") into national law to become effective. Not all European countries have done so, and among those that have, how they did it varies. Some countries deem the Directive no more than a template, and in some of these cases, the secondary legislation needed to bring the Directive fully into force is missing. Where a full set of legislation exists, it often adds to the Directive by imposing country-specific requirements. An example is Italy, where a separate data security code exists.

To make the matter even more complicated, there are other privacy-related EU Directives in force, for instance one from 2002 governing electronic communications (telephone calls, emails, etc.). Many countries already have fully transposed this 2002 Directive into national law, while some haven't.

■ **Second Misperception**: European Data Protection Agencies are toothless paper tigers.

This viewpoint is wrong and can be dangerous. All EU member states have Data Protection Agencies, some of them even several (e.g., on the state level in Germany). Most national jurisdictions provide for a prior registration scheme (also called notification) before processing of personal data can take place. This means that a U.S. corporation with a branch or subsidiary in this country must register with a state authority if the branch or subsidiary processes personal data. Examples of such state authorities include the Commission de la Protection de la vie privée in Belgium, the Commission Nationale de l'Informatique et des Libertés (CNIL) in France, or the College van de Bescherming van Persoonsgegevens (CBP) in the Netherlands.

In some jurisdictions (for example Austria and Hungary), the registration number that the company obtains must be given to data subjects before their data can be collected. In many countries it is a criminal offense not to register. Penalties can be severe—imprisonment for officers of the company.

The French CNIL has become somewhat famous in the U.S. during the last few months because it rejected the registration of a number of U.S. companies who intended to install whistleblower telephone hotlines for their French employees, in accordance with the U.S. Sarbanes-Oxley Act. Confronted with CNIL's rulings that the legal requirements of this Act infringe with French data protection law, they found themselves between a rock and a hard place, facing sanctions in France or from the SEC. After a lengthy discussion between the CNIL, the other European data protection agencies and the U.S. Security and Exchange Commission, many questions have been answered, but the "whistleblower hotline" issue has not yet been fully put to rest.

■ **Third Misperception**: Data protection is a EU concept.

It is true the EU 1995 "Data Protection Directive" is a European legal document that the EU member states are expected to "transpose" into their national laws. But its impact goes far beyond that. Many countries outside the EU have adopted the EU concept of data protection (including Canada, Australia, Argentina, Hong Kong and—with some caveats—Japan), and others, such as India, are debating whether or not to adopt the concept because they want to do business with the Europeans. Most recently Russia has adopted a data protection act *à l'Européenne*—much to the dismay of some U.S. diplomats, who lobbied against the new Russian law.

Some US observers criticize this development as a European "domino strategy," arguing that the EU will only admit transfers of EU personal data to those countries that adopt the EU's data protection regime. Whether this is true remains to be seen—some Asian countries are trying to combine the European concept of data protection with a more U.S.-oriented self-regulatory approach to privacy. U.S. companies are also lobbying in Brussels to make the European regime more "user friendly."

■ **Fourth Misperception**: Data protection is an issue for my business partner in Europe who sends me the data, but not for me here in the U.S.

This is a trap that U.S. companies may fall into because the United States is, from the EU's view point, a country of inadequate data protection. In principle, such data transfers are prohibited by both the EU 1995 Data Protection Directive and the national data protection laws if the receiving country does not provide "a level of adequate protection" for the data. From the EU perspective, the United States falls under this category.

This means there are substantial contractual and litigation risks even if the U.S. company doesn't have operations in Europe. Under the EU's 1995 Data Protection Directive, a Data Protection Agency may take protective measures and fine companies that send data from Europe to a country that does not provide adequate protection. Without adequate protection, the EU has argued, the high standards of data protection established by the 1995 Directive and the national laws would be undermined. In order to enable companies to continue exporting data to other countries, in particular to the U.S., EU law and the national laws provide for other tools to protect personal data that is exported:

- The U.S. company must publicly and properly declare its adherence to the U.S.-EU Safe Harbor Privacy Principles that the U.S. Department of Commerce administers.
- The recipient of personal data enters into a contract with the sender in Europe assuring adequate data protection (e.g., incorporates model contractual provisions issued by the European Commission—"Model Contractual Clauses").
- The sending and receiving parties belong to the same corporate group and adhere to the same "Binding Corporate Rules" (BCR).

European data protection officials have repeatedly criticized the U.S. Department of Commerce, which they say is not doing a good job enforcing the US/EU Safe Harbor Principles against U.S. companies. But in fact, the Federal Trade Commission has oversight and can impose steep fines and other sanctions, for instance, if a company that registered under the Safe Harbor Principles does not submit and file an annual compliance statement with the Department of Commerce.

One of the alternatives—namely, that a U.S. company has Binding Corporate Rules that would cover all kinds of data flows within the corporate group to and from the EU—is piecemeal and burdensome for multinationals doing business in Europe. It remains very difficult for U.S. companies to push a unified set of data protection principles for their European branches through the European institutions. Apparently Phillips, GE and Daimler Chrysler are in the process of obtaining individual approvals of their BCR from more than 25 national data protection agencies, but so far no more than 11 have agreed. The fact is that BCRs at present are not a viable alternative for small or medium-sized U.S. companies with business in Europe.

The American Chamber of Commerce ("AmCham") and the International Chamber of Commerce ("ICC") have lobbied in Brussels for more industry-friendly solutions to allow international data transfers from Europe to the U.S. Both believe that the EU data protection directives haven't helped because each of the 25 member countries has its own regime for processing personal data.

AmCham's demands are, in particular, to simplify content demands and the review process for BCRs and, more importantly, to approve AmCham/ICC alternative standard contractual clauses for transfers from data controllers to data processors. However, observers on the ground believe that none of these initiatives will lead to changes of the law in the near future.

What's Next: Reporting Security Breaches

For many companies, reporting of security breaches to government authorities and making them public is a touchy issue that may damage customer relations, put them on a watch list and create a lot of bad publicity. In Europe, the reporting requirements are also country-specific.

The European Commission has announced plans that it would like to see reporting requirements being implemented EU-wide. The Commission is suggesting that companies "must notify their customers of any breach of security leading to the loss, modification or destruction of, or unauthorized access to, personal customer data." However, it is not clear whether this proposal is meant to be an alternative to informing a government agency, and who would be covered.

On the national level, the landscape in Europe varies. In Germany, for instance, there is no general requirement to disclose data breaches. However, many mid-sized and larger companies have data protection officers inside their German companies, who are responsible for compliance with the German Data Protection Act (Bundesdatenschutzgesetz) within the company. If a security breach occurs, the data protection officer is obliged to stop the security breach and would determine the need to report the breach either to the relevant data protection authority or to the data subjects themselves.

Outside the EU, the picture becomes even more blurry. In Norway, by contrast, the unauthorized disclosure of personal data must be reported to the Datatilsynet (the national data protection agency), but not to the "data subject" (the individual whose data has been disclosed). No time limit is given for the report, although the Datatilsynet expects a notification within about a week of the breach.

In any event, what could happen in many countries in Europe is that an individual suspecting a breach might demand access to his or her data, which might itself force disclosure of a security breach. The company will have to address these requests ordinarily within a short time period prescribed by law. In many cases, associations or even business competitors might be able to use this access request of an individual to disclose a suspected security breach.

Territory Full Of Legal Landmines

Almost all businesses are data intensive in one way or another. Those that understand the importance of good privacy and data protection practices will have an edge on their competitors that do not. Handling data security breaches is one important aspect of this strategy: Before taking actions after a breach or discovering of a data leak in the U.S, or else-

where, thought will need to be given to the effect outside of the country. It may be difficult to notify U.S. customers (e.g., under applicable California law) and not those outside the U.S.

The data breach issue is not limited to breaches within the EU alone: The UK Data Protection Agency (the "Information Commissioner") is investigating claims that bank and credit card details of UK customers handled by call centers in India are being offered for sale by fraudsters. The investigation was caused by findings of the TV station Channel 4: An undercover reporter for the popular "Dispatches" program was shown the personal data which was on sale. This shows that data breaches are in fact a global issue. Moreover, if a company handles data breach reports poorly, or does not report the breach at all, this may lead to possible criminal prosecution and expose managers and business partners□