

# Data Protection Law in the *European Union*

European data protection law is vastly different from U.S. privacy law, regulating virtually all information about individuals, applicable to all industry types, and taking a much more expansive view of the types of activities that should be controlled and restricted. The consequences for violating these laws, which can include injunctions that interfere with business activity and criminal penalties, are also notably different from U.S. penalties, which tend to be limited to relatively modest monetary sanctions. If your company or client does business with or employs EU residents, this article will help you identify whether EU data protection compliance is something you need to address.

By Elizabeth H. Johnson

The European Union established the first legal system in the world to produce a comprehensive, omnibus approach to privacy and data protection. The legal regime established in the EU is unique because of its expansive nature, featuring active oversight and enforcement of complex laws and regulations that cover all industry sectors and all types of data processing.

The strict and comprehensive nature of EU data protection law stems from the European experience in World War II, when personal information was collected and used for the purpose of genocide. As a result, the philosophical underpinnings of EU data protection law contrast greatly with those of U.S. privacy law, which tends to focus on preventing identity theft and fraud. Conversely, EU data protection law tends to offer much broader coverage and is more restrictive in the limitations it imposes.

Europe's sad history with respect to the abuse of personal information has led Europeans to treat data protection as a fundamental human right. The laws protecting this right can be traced to human rights treaties and various national constitutions. In a groundbreaking judgment rendered in 1983, the German Federal Constitutional Court recognized a "right to informational self-determination," which is also recognized in various human rights treaties concluded by European nations.

The EU currently consists of 27 European nations, or member states. To govern this coalition of states, EU government bodies produce legal frameworks known as directives, which member states are then required to implement by enacting and enforcing codifying legislation. Because member states' laws may vary in the way they implement EU directives, compliance with EU data protec-



tion law requires understanding both the relevant directives and the variations of each particular member state's enabling legislation.

Because the EU issues directives, EU data protection law has several key features that are common in each member state, including the creation of a minimum level of data protection for individuals and the elimination of restrictions on data transfers among EU member states (recognizing that implementation of directives related to data protection ensures the minimum level of protection). Compliance with these requirements is interpreted and enforced by national regulatory bodies referred to as data protection authorities (DPAs). Private entities often complain that the rules of EU data protection law are overly bureaucratic (for example, rules on registering databases with DPAs), inflexible and burdensome (for example, rules governing international transfers of data), and difficult to follow because individual nations' interpretations of these requirements can vary widely. The lack of harmonization among member states is one of the primary criticisms levied against the EU model of data protection.

## Introductory Concepts

The EU's data protection law is replete with its own terminology, which can often make the rules difficult to understand. One of the most important terms is "personal data," which is the information safeguarded by EU data protection law. "Personal data" are defined as "any 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 the person's 'physical, physiological, mental, economic, cultural or social identity.'" Obviously, the concept of personal data is quite broad and includes almost any type of data that can be traced to an individual. Although U.S. entities are often concerned only with compliance as it pertains to information about customers, the broad European definition of personal data requires private entities to con-

This article originally appeared in the September issue of *The Federal Lawyer*. Used with permission.

sider compliance with respect to the personal data of their employees, customers, suppliers, vendors, and other contacts. These individuals, whose personal data receive the legal protections discussed herein, are referred to as “data subjects.” Any individual residing in the EU or whose personal data are processed in the EU is potentially a data subject.

The term “data processing” is also significant and further broadens the scope of EU data protection law. “Data processing” is defined as “any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.” Again, this term is quite broad, encompassing virtually any use of personal data, including mere collection. Related concepts include “data controllers,” that is, the entities that have the authority to determine how personal data are processed (usually the business that “owns” the data), and “data processors,” that is, the third parties that process personal data at the direction of data controllers. Data processors may have significant access to personal data and may even collect it for data controllers.

#### Legal Instruments and Basic Principles

EU data protection law is governed primarily by three directives: (1) the General Directive, (2) the Directive on Privacy and Electronic Communications, and (3) the Directive on Data Retention. As discussed above, each EU member state is required to enact national laws that give force and effect to these directives.

#### **General Directive**

The major instrument of EU data protection law is the Data Protection Directive, or “General Directive,” which was adopted on Oct. 24, 1995. The General Directive is founded on six primary principles:

1. Legitimacy: Personal data may only be processed for limited, legitimate purposes.
2. Finality: Personal data may be collected only for specified, legitimate purposes and may not be further processed for any incompatible purpose.
3. Transparency: Data subjects must receive information about the processing of their personal data.
4. Proportionality: Personal data must be relevant and not excessive in relation to the purpose for which they are collected and processed.
5. Confidentiality and security: Technical and organizational measures appropriate to the risks presented by the data processing must be in place to ensure the confidentiality and security of personal data.
6. Control: Data protection authorities must enforce data protection law.

Under the General Directive, personal data may be used only for the purposes to which the individual has

consented or for purposes that would be reasonably obvious to the individual on the basis of the information provided at the time the data were initially collected. Explicit consent is virtually always required when the personal data are deemed “sensitive,” defined as information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning the person’s health or sex life. Some member states also view criminal histories or driving records as sensitive personal data.

Data subjects must be provided with certain information when their data are collected for processing, including the following:

- the identity of the entity processing the data;
- confirmation that their data will be processed and the purposes of the processing;
- the categories of data concerned and the recipients or categories of recipients to whom the data will be disclosed;
- the logic involved in any automatic data processing; and
- the subject’s right to request rectification of inaccurate data and erasure or blocking of data processing that does not comply with the directive.

#### **Directive on Privacy and Electronic Communications**

The Directive on Privacy and Electronic Communications addresses data protection in the electronic communications sector, which includes telecommunications, faxes, e-mail, the Internet, and similar services. Specifically, this directive applies to personal data processed in publicly available electronic communications services in public communications networks in the community. Providers of such services must take appropriate technical and organizational measures to safeguard their systems and services. Member states are required to ensure the confidentiality of communications by national legislation, though limited exceptions are provided when government wiretapping activities and national security interests necessitate disclosure. Among other provisions, the processing of traffic and billing data is subject to further restrictions. In particular, subjects of data searches are given specific rights with regard to itemized billing, calling line identification, call forwarding, directories, and unsolicited calls.

#### **Data Retention Directive**

In the EU, member states often obligate providers of publicly available electronic communication services to retain certain data—primarily communications traffic data—to ensure that such data are available for law enforcement, national security, and related purposes. The Data Retention Directive attempts to harmonize the various retention requirements imposed by member states. The directive requires telecommunications companies to retain a wide range of data, including incoming and outgoing telephone numbers (fixed and mobile), the duration of the calls, addresses of Internet providers (dynamic and static), log-in and log-off times, and e-mail activity.

Member states can decide for themselves how long data should be retained within a minimum of six months and a maximum of 24 months from the date of communication, but the data must be erased after this time. Processing of the data during the retention period must be carried out in accordance with the requirements of the General Data Protection Directive, which member states must implement by Sept. 15, 2007.

#### Practical Implications

EU data protection law has important practical implications for companies conducting business in the region. For instance, the transparency principle mandates that companies must notify all data subjects (customers, employees, and so forth) of the types of personal data collected, the purposes for which they are processed, and the categories of recipients to whom the data may be disclosed. In addition, the proportionality principle requires companies to consider carefully the types of personal data necessary for the companies' purposes and to limit their collection to only those data. The most significant and burdensome of the EU data protection requirements are discussed below.

#### **Data Processing Registrations**

Companies doing business in the EU are often required to notify data protection authorities of the companies' data-processing activities, whether the firms conduct these activities themselves or contract with a service provider to do so. Most member states prescribe a registration procedure by virtue of which each DPA must be notified of any database containing personal data. The DPA may use specific application forms for this procedure, and the form and scope of the forms vary widely among member states. For example, registrations in the United Kingdom are often only a page or two in length, whereas the application form used in Italy is 86 pages long. The process is further complicated by the typical requirement that these forms be submitted in the local language. Despite wide variations among member states, the registration usually entails providing a contact person and describing the type of personal data processed, data subjects affected, purposes of the processing, security applied to the data, and any transfers or disclosures of the data.

Article 18(2) of the General Directive allows member states to create exceptions to the registration requirement. However, although some nations do provide such exceptions, this practice is hardly uniform. One of the more common exceptions applies when a company appoints a data protection officer to safeguard personal data processed by or on behalf of the company. The laws of France, Germany, Luxembourg, Sweden, and the Netherlands provide for such an exception. Usually, the company must notify the DPA of the data protection officer's appointment, and that officer is required to keep inventories of the data processing activities that would otherwise have been registered with the DPA. These inventories could, in principle, be reviewed by the DPA in the event of an inspection. The company must ensure that, if the

data protection officer is to have other job responsibilities, these must not conflict with the responsibility to uphold EU data protection principles.

#### **International Data Transfers**

Among the restrictions of greatest importance to companies are those pertaining to the international transfer of personal data. Personal data may not be transferred to countries outside the EU unless there is a "legal basis" for the transfer. Several possible grounds may provide a legal basis to transfer personal data to a non-EU country. First, the European Commission may issue an official "adequacy finding," determining that the country in question offers an adequate level of data protection on the basis of its national laws. Since the enactment of the General Directive, the European Commission has issued only a very small number of adequacy determinations; these cover Argentina, Canada, Guernsey, the Isle of Man, and Switzerland.

There are several other potential legal bases for international data transfers when the country to which personal data will be sent has not received an adequacy finding. The most important such legal bases are the following:

- The consent of the individual whose data are being transferred: Consent can be difficult to manage in practice, however, because consent may be revoked. In addition, consent is not always considered legally valid, particularly in the employment context, in which consent is sometimes viewed as coerced.
- Execution of the EU-approved "standard contractual clauses": These standardized data transfer agreements are concluded between the "data exporter" (the entity in the EU) and the "data importer" (the entity outside the EU), which agree to grant certain protections to the data. The clauses have been given an adequacy finding by the EU and therefore may not be modified by the signing parties; rather, the parties are required to describe the nature of their data transfer in an annex to the clauses. Some countries require the executed clauses to be filed with the DPA, and several require affirmative approval from the DPA prior to the transfer. As such, the clauses are difficult to use in practice, particularly when a company seeks to transfer personal data to hundreds of its subsidiaries worldwide, because each of these entities would be required to execute the clauses.
- The transfer is necessary for the performance of a contract between the entity transferring the personal data outside the EU and the individual whose data are being processed: This legal ground is construed strictly and is useful only in certain narrowly defined situations (for example, when a person in Europe books a hotel for a foreign vacation and needs to transfer data about his or her stay to the hotel outside the EU).
- The U.S. Safe Harbor program: This program is a voluntary, self-regulatory scheme that has received an adequacy finding from the European Commission. Companies choosing to join the program must certify their

compliance on an annual basis. The program is available only to entities subject to Federal Trade Commission jurisdiction; therefore, the program only provides a legal basis for transfers of personal data from the EU to entities that have been certified as safe harbors in the United States.

- Implementation of “Binding Corporate Rules”: Binding corporate rules are a set of data processing rules and principles adopted by a company that bind all of the company’s entities worldwide to certain data protection requirements. These rules must be approved by DPAs but, once approved, allow the legal international transfer of personal data among the entities bound to comply with the binding corporate rules. Through the use of these rules, the entire corporate group essentially becomes a “safe haven” in which personal data can be freely transferred from one corporate member to another, receiving the same protection wherever the data are sent and shifting the burden of ensuring compliance to companies themselves.

Because many companies in Europe spend considerable time and money complying with the EU law’s restrictions on international data transfers, the regulations have significant economic implications. The restrictions can have particularly serious consequences for outsourcing transactions, because a company in Europe may not transfer personal data for outsourcing purposes to, for example, China or India, without first identifying one of the specific valid legal bases for the transfer, as discussed above. This often adds considerable cost and complexity to outsourcing transactions.

### **Direct Marketing**

The Directive on Privacy and Electronic Communications directs member states to allow unsolicited commercial telephone calls, e-mails, and faxes only with the prior consent of the recipient. Two types of consent are recognized in the EU: “opt-in,” or explicit, consent is obtained when the data subject affirmatively indicates his or her preference to receive marketing communications; and “opt-out” consent is obtained when the data subject is presented with an opportunity to object to receiving marketing communications but does not do so.

The media by which marketing communications are sent will dictate the form of consent required. Though the requirements vary by member state (as with most areas of EU data protection law), opt-in consent usually is required prior to sending faxes or placing telephone calls. Opt-in consent also is typically required prior to sending unsolicited e-mail communications. An exception is made for marketing e-mails sent to data subjects with whom a company already has an “existing business relationship.” In that circumstance, the company is considered to have obtained “soft opt-in” consent from the data subject if the contact information was obtained in the course of a sale, contracting, or negotiations and the proposed communication pertains to products and services similar to those that were the subject of the existing business relationship.

Regardless of the type of consent obtained at the outset, every direct marketing message sent subsequently must contain a mechanism to enable the data subject to opt out of receiving further messages at little or no cost to the data subject.

### **Enforcement of the Law**

Enforcement of data protection law in the EU is often less visible than it is in the United States. DPA decisions often go unpublished, and the authors of judicial opinions in European legal systems are usually unknown. Moreover, there is no doubt that the broad scope of EU’s data protection law and the general lack of resources available to many national DPAs cause many violations to go unpunished.

Nevertheless, the level of enforcement of data protection law is increasing in Europe; criminal penalties, fines, injunctions, and so forth, can be imposed on violators of the law. One German DPA, for instance, required a major company to remove all cookies from its Web site, which significantly affected its online presence. The action was never made public, but the effect was just as serious as if the company had been forced to pay a large fine. A few other prominent examples of enforcement actions include:

- The Italian DPA investigated and prosecuted a company that illegally processed data for commercial solicitation. After discovering the company’s failure to register its processing activity, the DPA issued an order blocking further data processing and reported the case to the criminal court.
- The Spanish DPA imposed a fine of several hundred thousand euros against a television producer who failed to appropriately secure a database containing the personal data of participants in a television show and transmitted that data to third-party advertisers without the consent of the participants.
- A Finnish court ordered several top executives of a large telecommunications company to be jailed for illegally monitoring their employees’ business telephones. The executives later received suspended sentences.

DPAs initiate most enforcement measures either in response to a complaint from an individual or on their own initiative. Individuals may also bring lawsuits based on data protection violations, but such lawsuits have been rare. Implementation of the General Directive has, however, given individuals an increased opportunity to file lawsuits directly against companies for misuse of personal data, because the directive obligates member states to create a direct cause of action.

Enforcement actions can cover a wide variety of legal violations. Among the most popular grounds for enforcement actions are failing to register data processing with the data protection authorities, sending unsolicited marketing material (particularly spam), and transferring personal data outside the EU without a valid legal basis. In addition, employees and their representatives often file

complaints against employers for violations of data protection law.

#### Emerging Issues: Legislation Dealing with Information Security Breaches

Information security breaches have received the greatest attention from legislators, regulators, and media in the United States. Commentators in both the United States and the EU have noted the irony that, despite the EU's comprehensive regulation of data protection and the relative lack of such in the United States, the EU has yet to require entities to notify EU residents when their personal data have been exposed as a result of a security breach.

The data protection authorities could, in turn, require security audits, levy fines, and publicize the breach in order to notify affected individuals. Although the proposals would apply only to Internet service providers and network operators, EU courts have previously expanded the reach of the Directive on Privacy and Electronic Communications and could do so again. The requirement to notify data protection authorities, rather than each affected individual, reflects the much lower occurrence of private enforcement (that is, individual lawsuits) in the EU as compared the situation in the United States.

Only a select few breach-related enforcement actions have been reported in the EU, though it is much less common for enforcement actions to be publicized in Europe than is the case in the United States. In December 2006, Vodafone was fined 76 million euros (\$103 million) by the Greek DPA, which alleged that Vodafone failed to protect its network from hackers who monitored more than 100 mobile phone accounts. The amount of the fine reflects the high-profile nature of the incident: the hacking occurred during the 2004 Olympic Games in Athens, and the accounts targeted included those of Greek Prime Minister Costas Karamanlis, senior military officers, and journalists. Adding to the scandal, Vodafone's network planning manager in Greece was found dead of hanging not long after he reported to his supervisors that he had discovered the spying software and only one day before the company notified authorities of the hacking. Vodafone is appealing the fine.

Shortly after news of the enforcement action taken on Vodafone, reports surfaced that the Nationwide Building Society was fined £980,000 by the Financial Services Authority (FSA) following the theft in August 2006 of an employee's laptop computer containing customers' personal data. The FSA alleged that Nationwide did not have in place adequate information security procedures and controls. Because Nationwide agreed to settle the action promptly, it received a 30 percent reduction in the original fine of £1.4 million. Nationwide notified its customers of the incident, and both the FSA and Nationwide agreed that the FSA can order regulated financial institutions to provide such notification.

#### Conclusion

EU data protection law was finalized just before the dawn of the Internet age in the mid-1990s, and this timing

is reflected in a number of provisions of the General Directive that are difficult to reconcile with the demands of the online world (for example, choice of law provisions, which are notoriously difficult to apply in an online context). Perhaps most notably, the requirement to legalize personal data transfers to countries that have not received an adequacy determination significantly hinders companies' ability to provide global access to data, contract with data vendors in non-EU jurisdictions, and modify their data flows once they have achieved compliance. This requirement also complicates any number of areas requiring international data transfers, including outsourcing and national security, as evidenced by the disputes between the United States and the EU over transfers of financial information by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) and airlines' records of passengers' names.

Achieving compliance with EU data protection law is further complicated by a lack of harmony among the member states that must implement the EU directives. Even some of the most basic concepts of the General Directive (such as the definition of "personal data") differ in each member state's implementation, making it difficult for companies with an extensive presence in the EU to achieve complete compliance with every member state's interpretation of the directive.

There is no doubt that EU data protection law has a substantial impact on day-to-day business practices. Legal obligations—such as providing detailed notices to employees and customers, registering databases with the national data protection authorities, and putting restrictions on international data transfers—impose substantial compliance costs on companies doing business in the EU. Although criticism of the EU approach has intensified because of the increased level of impediments to global data flows, a growing number of jurisdictions, including Russia and Dubai, have adopted comprehensive data protection laws based on the General Directive. Consequently, companies must not only be prepared to navigate the varied data protection compliance issues that arise when doing business in the European Union or with residents of EU member states but also be aware of the privacy and data protection laws that are emerging with increasing frequency across the globe. TFL

---

*Elizabeth H. Johnson is an attorney with Hunton & Williams' Privacy and Information Management practice, which was recently named "head and shoulders above the rest" in a Computerworld survey of corporate privacy officers. Her practice spans all areas of privacy law, including conducting comprehensive privacy and information security assessments, producing records management programs, advising on global data transfer issues, and producing privacy notices, contracts, policies, and procedures. Johnson routinely counsels clients regarding compliance with various statutory and regulatory requirements in jurisdictions such as the EU, federal, and various states including North Carolina, where she is based.*