

Recent Developments in EU Employee Data Privacy Law

SEBASTIEN DUCAMP, CHERYL TAMA OBLANDER, AND HEATHER BENNO

The authors explain how U.S. businesses with operations in Europe can reduce the risk of liability and sanctions by taking precautions to safeguard employee privacy.

Recent privacy legislation in the European Union has posed specific challenges to U.S. employers who conduct business in Europe by regulating their ability to collect, retain, and transfer employee data within Europe and internationally. In 1995, the European Parliament adopted the EU Data Protection Directive (Directive 95/46/EC, “Directive”) to “respect [man’s] fundamental rights and freedoms, notably the right to privacy, and [to] contribute to economic and social progress, trade expansion and the well-being of individuals.”¹ The Directive creates a comprehensive program of data protection law throughout Europe. It applies to any data processed within the EU that identifies or could identify any person, including information collected and retained by employers. The Directive is implemented on a national level by each Member State’s data protection legislation. This legislation and the framework that the Directive established often conflict with U.S. interests in workplace transparency and information-flow for security

The authors, attorneys with Winston & Strawn LLP, can be reached sducamp@winston.com, ctama@winston.com, and hbenno@winston.com, respectively.

purposes. As a result, U.S. companies have been forced to tread cautiously between U.S. legislation encouraging data flow, such as Sarbanes-Oxley, and privacy laws across the EU.

THE EU DATA PROTECTION DIRECTIVE

The Directive has two main purposes: (1) to protect individual privacy, and (2) to standardize privacy regulations to encourage secure data flow between EU Member States and third parties that enforce similar levels of data protection. The EU pursues these goals by establishing standards on data quality, criteria for data processing, notice and consent requirements, and the right to access personal data. The Directive requires the following:

- Personal data must only be collected for legitimate purposes such as (1) the performance of a contract to which the subject of the data (“data subject”) was a party; (2) compliance with a legal obligation; or (3) any purpose to which the data subject unambiguously consents.
- The data must be processed fairly and lawfully. The entity processing personal data (“data controller”) has a duty to inform the data subject of its identity, the purpose of the data processing, and other specifics relating to the data processing.
- The data must be accurate and up-to-date. Data subjects have the right to access their personal data and to change or delete incorrect information.
- Data controllers must implement security measures to ensure that personal data is adequately protected.
- Violations of data privacy regulations invite judicial remedies, administrative remedies, liability, and sanctions.

Personal data is broadly defined under the Directive. It includes information such as personal contact information; physical characteristics; family, lifestyle, and social circumstances; employment information; and financial information. Another category of data, “sensitive data,” is

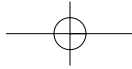
subject to heightened processing restrictions. Sensitive data includes data that reveals an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, or sexual preference.

In addition to regulating the treatment of personal data within the EU, the Directive also regulates the transfer of personal data from an EU Member State to a third party country. With some narrow exceptions, the Directive requires third party countries that receive data from an EU Member State to enact similarly stringent data protections. The EU Member States and the European Commission have deemed current U.S. privacy protections inadequate for third party transfer purposes. Nevertheless, U.S. companies have received little guidance on how the European law affects the transfer of human resources data between business operations in Europe and elsewhere.

THE "SAFE HARBOR" AGREEMENT AND OTHER OPTIONS

To avoid disrupting transatlantic trade, the U.S. Department of Commerce and the European Commission negotiated the "Safe Harbor" framework in 2000. Under Safe Harbor, EU Member States will allow data transfers between Europe and U.S. companies that establish privacy processes that comply with the Directive's requirements. Companies who choose to take part in Safe Harbor must annually certify their continued compliance with the Safe Harbor Principles, which require the following: notice to data subjects when data will be processed for a purpose different than that originally reported; data subjects' right to opt-out of data disclosure; data access rights for data subjects; onward transfer limitations; data integrity and security; and enforcement. By certifying that strict data privacy protections are in place, companies are immune from privacy infringement suits in Europe. As of the end of 2003, 400 U.S. companies had endorsed the Safe Harbor Principles.

As an alternative to Safe Harbor certification, U.S. companies are able to exchange data with operations in Europe if they comply with the data protection requirements of the Member States in which they operate.



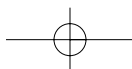
PRIVACY & DATA SECURITY LAW JOURNAL

For example, some Member States allow U.S. entities to form data protection contracts with European subsidiaries based on EU pre-approved terms. U.S. companies may also implement Binding Corporate Rules, which were drafted by the EU's Working Party on the Protection of Individuals with regard to the Processing of Personal Data. By instituting Binding Corporate Rules, a company pledges that its data protection procedures satisfy the demands of participating Member States' data protection authorities. These options have been more popular with U.S. companies than certifying under Safe Harbor because Safe Harbor certification subjects employers to the Federal Trade Commission's enforcement jurisdiction.

DATA PROTECTION IN THE EMPLOYMENT CONTEXT – STEPS TO ENSURE COMPLIANCE

All U.S. multinational organizations should consider how their data operations could be altered by the Directive, the Safe Harbor Principles, and each Member State's data protection regulations. Data operations should be understood to include any procedures that an employer establishes to encourage or manage the flow of information about employees, potentially without that employee's consent, such as whistleblowing systems. A business with operations in Europe can reduce the risk of liability and sanctions by taking precautions to safeguard employee privacy. The following precautions should be considered:

- Undertake a personal data audit to determine whether you engage in employee data transfers that may be subject to the Directive or other regulations.
- Publish a policy notifying employees of the type of personal data being collected, how it will be used, and the purpose of collecting the data. This policy should also include information on employee monitoring, surveillance, drug testing, or genetic testing that the employer conducts. Employers should enforce the policy to avoid invasion of privacy grievances and to establish evidence that the policy is controlling.



RECENT DEVELOPMENTS IN EU DATA SECURITY LAW

- Identify employee representatives or trade unions with a right of consultation in developing the privacy policy. Even in Member States where it is not necessary to consult employee representatives, doing so may ameliorate employee perceptions of privacy invasions in the workplace.
- Determine whether the Member State in which you operate requires employers to obtain prior authorization from a national data protection authority for the collection, processing, and/or transfer of personal data, and, if not, whether employers must declare such data activity.
- If possible, obtain unambiguous consent to data handling from employees, including (1) sensitive personal data processing; and (2) personal data disclosures and onward transfers to non-EU countries that do not meet the Directive's demands.
- Provide employees with a reasonable opportunity to access personal information and to correct errors in that information.
- Develop systems for updating employee information and verifying the accuracy of retained information.
- Ensure that files and databases containing personal information are secure and handled only by personnel trained in the company's security policy.
- Adopt compliant methods of transferring data to third parties outside of Europe, such as Safe Harbor certification or data protection contracts.
- Promptly delete data when it is no longer used for its original or approved purpose, or when the approved time period for maintaining the data lapses.

NOTE

¹ Council and European Parliament Directive 95/46/EC, Recitals 2, 1995 O.J. (L 281) 31, *available at* http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm.