russell kelley consulting

PRACTICE NOTE ON
EMPLOYEE DATA PROTECTION FOR INTERNATIONAL GROUPS

Practice Notes represent the author's view of good practice in a particular area. They are not legal advice and the author will not accept any legal liability in relation to them.

Issue

With the advent of the Internet, the protection of personal data – and particularly the transfer of personal data from a country with adequate legal protection to another country without adequate legal protection – has become a priority for the European Union and for many countries.

Many international groups are involved in businesses which inherently involve the storage and processing of the personal data of customers, including on-line vendors and marketers, financial institutions and pharmaceutical companies. Since third party personal data is involved, these companies are subject to special scrutiny with respect to their compliance with applicable privacy and data protection laws. But virtually all international groups store and process the personal data of their employees, and are therefore subject to the same data protection laws if not to the same degree of scrutiny. Similarly, many international groups also outsource travel services and corporate credit card management to outside service providers who maintain databases with related EU employee data that can be accessed from outside the EU, which the law requires – and their employees expect – the groups to protect.

Until recently, employee data was often stored and used in the country of employment only, and was not transferred to other countries. Web-based human resource information systems now permit an international group to store the personal data of its employees around the world in a centralized database – typically located in its headquarters country – which can then be accessed by authorized persons at the global, regional and country headquarters of the group, and possibly at shared service centers, as well. Each time an authorized person in another country accesses the database, there is an international transfer of personal data which is subject to applicable data protection laws.

The principal data protection compliance issue arising in connection with web-based human resource information systems stems from the EU Data Protection Directive ("the Directive"), which permits the transfer of personal data of EU employees from the EU to other countries only where such other countries or the data recipients in such countries have in place adequate data protection controls.

The European Commission has determined that Argentina, Canada, Guernsey, Iceland, Isle of Man, Jersey, Norway and Switzerland provide adequate protection to

personal data, but that the United States does not have an adequate level of data protection controls. The EU does, however, accept that the transfer of personal data from the EU by any party – an affiliate, a client, or a supplier – to a U.S. entity that has certified under the U.S. Department of Commerce "Safe Harbor" program meets the requirements of the Directive.

Strategy

To be able to comply with applicable laws, the first step is to identify in which country the employee database will be located, the countries whose employees' data will be stored on the database, and the countries which will have access to the employee database. If the database and all international transfers are within the European Union (and the short list of other countries deemed by the EU to provide adequate privacy protection), it is sufficient for the entities exchanging data to be in compliance with the law of the relevant EU member countries. If the transfers are between the EU and countries other than the short list of countries deemed by the EU to provide adequate privacy protection, the possible compliance solutions are for the entities exchanging data to enter into Intra-Group Data Transfer Agreements based on the Model Clauses published by the European Commission, or to adopt and implement Binding Corporate Rules. If the transfers are between the EU and the United States, the "Safe Harbor" solution is also available. The various solutions are discussed below.

Relevant Laws and Regulations

The EU Data Protection Directive

The EU Data Protection Directive is intended to protect the privacy of all personal data that are under the control of an entity established in the EU, or of an entity established outside the EU but collecting or otherwise processing data within the EU. All 28 EU Member States had enacted national data protection legislation that fulfill the Directive's requirements; nonetheless, there are significant differences in the data protection laws enacted by the Member States.

The Directive is predicated on the principle that in order to be lawful, the collection and processing of personal data must comply with a number of principles, among them:

- Personal data shall be processed fairly and lawfully; in most cases, this requires ***informed consent*** of the person whose data are processed ("data subject").
- Personal data shall be obtained only for one or more specified and ***lawful purposes***.
- Personal data shall be ***adequate, relevant and not excessive*** in relation to the purpose or purposes for which they are processed.
- Personal data shall be ***accurate***.
- Personal data shall ***not be kept for longer than is necessary*** for the purpose for which they were collected.
- Data subjects have the ***right to access, correct, delete and, where justified, oppose*** processing of their personal data.

- Appropriate ***technical and organizational measures*** shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the EU unless that country or territory ensures an ***adequate level of protection*** for personal data.

"Personal data" mean "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 his physical, physiological, mental, economic, cultural or social identity". ***Data are considered personal when they may enable anyone to link information to a specific person, even if the person or entity holding those data cannot make that link.*** Examples of such data include street address, bank statements, credit card numbers, telephone numbers, and IP addresses.

A "data controller" is a person who decides how and why personal data are to be "processed".

"Processing" is broadly defined to involve any manual or automatic operation on personal data, including their collection, recording, organization, storage, modification, retrieval, use, transmission, dissemination, publication, blocking, erasure or destruction, ***or even mere access to personal data***.

In addition to complying with the basic principles set forth in the Directive, in many cases a controller will also need to undertake formalities with the relevant data protection authority ("DPA"). Such formalities vary greatly, from on-line registration of the controller with the DPA, to notification of a specific database to the DPA, to submitting detailed information to the DPA in order to obtain an authorization prior to commencing any processing.

Of particular concern to groups with global employee databases is the fact that transfers of personal data from the EU to other countries are lawful only under specific conditions, principal among them that the receiving country offers adequate protection to personal data. There are exemptions to this requirement, in particular where the data subject has consented to the transfer, or where the transfer is necessary in order to perform obligations under a contract to which the data subject is a party. However, the DPAs' interpretations of these exemptions are sufficiently narrow that repeated, large-scale transfers of employee data cannot benefit from any exemption.

Ensuring the lawful transfer of employee data will therefore depend on the country to which the data will be transferred. In the case of the United States, the European Commission deems that there is adequate protection if data are transferred to an entity that is certified under the U.S. Department of Commerce's data privacy Safe Harbor. Transfers to an entity located in Argentina, Canada, Guernsey, Iceland, Isle of Man, Jersey, Norway and Switzerland are also permissible, as the European Commission has determined that those countries provide adequate protection to personal data. For transfers of personal data to all other countries, or to a non-Safe Harbor certified U.S. entity, signature and implementation among group entities of a contract based on the European Commission-approved Model Clauses for the transfer of personal data (in

essence, an Intra-Group Data Transfer Agreement) would satisfy the Directive's requirements. Finally, the implementation of Binding Corporate Rules among group entities is another alternative for ensuring permissible transfers of data outside the EU.

The principal benefit of Safe Harbor certification for a U.S. entity is that it covers receipt by that entity of all data from the EU, regardless of the identity of the data exporter. In other words, the Safe Harbor-certified entity may lawfully receive personal data from an affiliate, a supplier or a client based in the EU without any additional formalities or delays and specifically without entering into separate Data Transfer Agreements. Because Data Transfer Agreements must, in many EU countries, be authorized in advance by the DPA, Safe Harbor certification can be a very efficient means of compliance for U.S. companies that receive data from several EU entities and/or countries, and the EU entities that transfer that data.

Data Protection in the United States

The United States has no single, overarching privacy law comparable to the Directive. Instead, privacy regulation applies to specific business sectors, communications media and for data elements that create data security risk. Examples include the Health Insurance Accountability and Portability Act of 1996, which regulates privacy in the health care sector, and a variety of U.S. federal and state regulations covering sensitive data elements that create a risk of identity theft or fraud. Significantly, unlike the EU, the United States does not prohibit data transfers to other countries that do not have in place a certain level of data protection.

The EU has deemed that the United States (like most other countries) does not provide an "adequate" level of privacy protection.

The Safe Harbor program was negotiated between the EU and the U.S. in 2000 to facilitate U.S.-EU commerce and to find a compromise approach that would more efficiently satisfy the EU's requirements for data transfers outside the EU. A U.S. legal entity's self-certification to the U.S. Department of Commerce of compliance with the seven Safe Harbor principles permits the transfer of data from the EU to that entity. Compliance with the Safe Harbor program is subject to annual internal compliance reviews or audits and violations may be enforced by the Federal Trade Commission.

The Safe Harbor principles are as follows:

- Notice (information about data collection, such as the purpose for collecting information and contact information for questions or complaints).
- Choice (usually the ability to opt-out, except in the case of unanticipated uses of EU personal information not addressed in the notice).
- Onward transfer (application of the notice and choice principles for disclosure of information to a third party and a requirement to bind vendors who receive EU personal data to comply with the Safe Harbor principles in their handling of that data).
- Security (reasonable precautions to protect collected data).
- Data integrity (use of the collected information for its intended purpose).

- Access (allowing individuals to correct, amend or delete inaccurate information about themselves).
- Enforcement (mechanisms for ensuring compliance with the other principles, recourse for adversely affected individuals and consequences for non-compliant organizations).

Note that EU authorities take the position that U.S. entities who receive personal data from the EU may not transfer those data outside the U.S. to a third party without using a Directive-compliant data transfer agreement (e.g., an Intra-Group Data Transfer Agreement).

Data Protection in Other Countries

Although the initial focus of compliance is usually the EU, given its legal regime and the importance the region holds for many international groups, other countries, such as the EEA countries (Iceland, Norway and Switzerland), Argentina, certain provinces of Canada, Israel, and Uruguay also have robust data protection laws.

Key Issues for International Groups

Location of Employee Database

Locating the employee database in the United States instead of the EU would present some compliance advantages. For example, issues raised by processing restricted, or sensitive data (see below) related to non-EU employees would be more easily managed if those data were stored in the United States rather than in the EU. Nonetheless, the principal compliance measures outlined in this note – Safe Harbor certification, Intra-Group Data Transfer Agreement, and possibly employee notice and other measures – would still be required even if the database were located in the United States.

Basic Requirements for Lawful Data Processing

Among the numerous requirements for lawful data processing under the Directive, the following are particularly critical for global employee databases:

- Employee data should be processed only for specified explicit and legitimate purposes for which they were collected, and/or as necessitated by performance of the employment contract.

- Employee data must be objective, relevant and not excessive in relation to the purposes for which they are processed.

- Employee data should be accessible only on a need-to-know basis.

- Employee data must be timely archived or destroyed pursuant to Groupe document and data archiving policies.

- A decision that produces legal effects or significantly affects the employee may not be based solely on automated processing of data.

Security

The architecture of the global employee database must ensure that the system and its operation (i) do not create security risks for the database or the group generally, and (ii) comply with relevant group policies and procedures (if they do not, appropriate modifications should be made).

Types of Data Processed

The collection and processing of sensitive data including "religion", "ethnicity", "disability" and "national ID", may be illegal or restricted in a number of countries.

Except where explicitly required or tolerated by law, data referring to employee religion and ethnicity should not be collected and processed. Where required or tolerated, such data should remain in local databases whenever possible in order to avoid additional requirements to carry out formalities with the DPA in the country where the centralized database is located.

The processing of data regarding disabilities may only be permissible where strictly necessary to administer employee benefits.

In France, for example, the processing of social security numbers requires the prior authorization of the DPA unless an exception applies (e.g., in order to prepare payroll or administer benefits).

Employment Law Requirements

Depending upon the location and number of employees of the group entity processing data in the global employee database, it may be necessary to inform, consult or reach an agreement with the local worker representative, works council, hygiene and safety committee or trade union(s). This will need to be determined on an entity-by-entity basis. For example, French courts consider that the implementation of employee evaluations requires consultation of the works council. To the extent such a consultation was already held with respect to a previous evaluation method, it should be determined whether further consultation is required due to the roll-out of the global employee database.

Notice to Employees

Giving notice of data processing to the data subject (the employee who is the subject of the personal data) is a basic requirement for lawful processing under the Directive. In addition, local employment laws may necessitate individual notification to employees of certain processing activities.

DPA Formalities

DPA formalities regarding the global employee databases will vary from country to country. In France, for example, the functionalities of a human resource information system may only require a simplified notification to the DPA, provided that the

database does not contain restricted types of data (see above), and to the extent that transfers of data are made only to Safe Harbor certified entities in the U.S.

Data Transfers Outside the EU

United States

As discussed above, Safe Harbor certification by each U.S. entity that will have access to EU employee data via the human resource information system will ensure compliance of those transfers with the Directive.

Rest of World

To meet the requirements of the Directive, transfers to entities outside the EU (other than entities that are Safe Harbor certified, or located in countries with equivalent protection) must be made pursuant to (i) Intra-Group Data Transfer Agreements based on the Model Clauses published by the European Commission as a means to ensure compliance with the Directive when transferring personal data outside the EU, or (ii) Binding Corporate Rules.

(i) Intra-Group Data Transfer Agreements (based on the Model Clauses)

The signature and implementation of Model Clauses permit the transfer of personal data between an EU data exporter and a non-EU data importer. The key aspects of the Model Clauses are as follows:

- The non-EU data importer must adhere to the Directive's data protection principles.
- The EU data exporter and the relevant DPA have rights to audit the data importer.
- The data importer may in certain cases be held directly liable to data subjects in the event of violation of the Model Clauses.

Although the Model Clauses are based on the assumption that there will be one data exporter and one data importer, it is now common practice to apply the Model Clauses across a group of companies via an Intra-Group Data Transfer Agreement, pursuant to which all adhering group companies located outside the EU agree to abide by the terms of the Model Clauses.

Note that each individual legal entity outside the EU which imports EU employee data must be a signatory to the Intra-Group Data Transfer Agreement.

(ii) Binding Corporate Rules

Another way to meet the Directive's requirements for transfers of data outside the EU is to enter into Binding Corporate Rules, a set of data protection principles that is adopted by entities in a group to ensure adequate protection of data in all countries where the group is present. This alternative is more burdensome than implementing

Intra-Group Data Transfer Agreements since BCRs must be approved by the DPA in each relevant EU Member State, and require a high level of internal compliance, including annual audits and certifications and specific personnel training. Although the DPAs have made a concerted effort to facilitate the implementation of BCRs by allowing groups to obtain preliminary approval from a coordinating DPA, the process is still long (generally well over a year to draft proposed BCRs and obtain approval from the coordinating DPA; full implementation can easily run two years).

Conclusion

To eliminate the sometimes significant differences in the data protection laws enacted by the EU Member States, the European Commission issued a proposed General Data Protection and Privacy Regulation in January 2012 aimed at providing a single set of privacy rules for all EU member states, with a single DPA responsible for each international group depending on where the group is based or which DPA it chooses. The new Regulation is expected to become law in 2014, and take effect in 2016. While the new Regulation will simplify compliance, it will also entail stricter enforcement and severe potential penalties of up to 2% of worldwide turnover. It is, therefore, imperative that international groups ensure that their data protection compliance programs are in place before the new Regulation takes effect.

21 August 2013