Launching a Whistleblower Hotline Across Europe
Table of Contents

Abstract..................................................................................................................2

Issues Faced by Multinationals When Launching a European Hotline.........................2

Three-Step Process for Developing a Solution..........................................................4

Overview of Data Privacy Compliance by Nation......................................................6

Austria
Belgium
Czech Republic
Denmark
Finland
France
Germany
Ireland
Italy
Netherlands
Norway
Poland
Portugal
Russia
Slovak Republic
Spain
Sweden
Switzerland
United Kingdom

References..................................................................................................................33
Launching a Whistleblower Hotline across Europe

Abstract

In the wake of significant corporate accounting scandals involving major U.S. companies such as Enron, WorldCom and Tyco, many companies have implemented confidential third-party whistleblower hotlines as a means of receiving and handling complaints pertaining to unethical behavior within the organization.

In the ensuing decade since these scandals, hotline use has evolved to the point where it has gained widespread acceptance and is even considered to be a best practice. Studies conducted by the Ethics Resource Center indicate that in many cases, hotline implementation has had a positive impact on the ethical behavior in organizations while helping to reduce the occurrences of misconduct.

While whistleblower hotlines are now prevalent in the United States, attempts at hotline implementation by U.S. multinationals within their European operations have been problematic at best. In general, Europeans tend to be more protective of their personal privacy than Americans, and more stringent data privacy laws are in place in many European nations.

There has also been a great deal of pushback from certain members of the European Union concerning hotlines. France, for instance, has been openly critical, indicating that their use can actually impede U.S. companies from doing business in the country. In European nations deeply impacted by World War II such as Germany, France and Netherlands, hotline use is typically viewed as the equivalent of snitching or spying, invoking memories of a dark time where fears of dictatorial rule created feelings of unrest and distrust amongst the populace.

Issues Faced by Multinationals When Launching a European Hotline

Donald C. Dowling, Jr., International Employment Partner at White & Case, LLP, a leading global law firm, provides an overview of the challenges multinationals face when attempting to implement a whistleblower hotline in Europe. The following brief article, “Launching a Whistleblower Hotline across Europe,” is an excerpt from a 2011 piece titled “Global Whistleblower Hotline Toolkit: How to Launch and Operate a Legally-Compliant International Workplace Report Channel” that was written by Dowling for the White & Case website:

“As corporate social responsibility and business ethics continue to grab attention, evermore-sophisticated ‘best practices’ and compliance strategies emerge. A key practice that anchors many corporate social responsibility programs and compliance initiatives is launching and publicizing an internal whistleblower procedure, report channel, or ‘hotline’ that entices insiders to denounce colleagues’ misdeeds so management can root out corporate crimes, corruption and cover-ups.

Workplace whistleblower hotlines take many forms. Some stand on their own while others comprise part of a broader corporate code of conduct, code of ethics, compliance or social responsibility program. Some run in-house while others are outsourced. There are single global hotlines and there are aligned but separate report channels across local affiliates.
Some hotlines are closed to staff in certain countries. Whatever the form or reach, the idea behind a workplace hotline is simple: Empower insiders who hear about white collar crime, policy breaches or other wrongdoing to come forward with allegations so management can investigate, right wrongs, and punish the guilty.

Domestically within the US, workplace whistleblower hotlines are a largely uncontroversial ‘best practice’ to which few ever object. But tensions rise when a multinational extends report channels abroad. In Europe in particular, whistleblower hotlines can spark blowback from staff, employee representatives and government enforcers, and can trigger confounding legal issues without US counterpart. To a socially-responsible American, the hurdles impeding European whistleblower hotlines have gotten higher than they should have any right to get.

Over a dozen European jurisdictions interpret their local domestic data protection laws (either by regulation or at least by data agency pronouncement) specifically to rein in employer hotlines. And an EU advisory body called the Article 29 Working Party issued a persuasive but non-binding report that recommends all 27 EU states embrace a particularly-restrictive interpretation of EU data law to restrict hotlines.

Broadly speaking, Europeans see hotlines as threatening privacy rights of denounced targets and witnesses when hotlines are not ‘proportionate’ to other report channels in European workplaces.

Among the specific hurdles that European jurisdictions erect to frustrate hotlines, the 12 biggest are:

1. Restrictions against hotlines accepting anonymous denunciations
2. Limits on the universe of ‘proportionate’ infractions on which a hotline accepts denunciations
3. Limits on who can use a hotline and be denounced by hotline
4. Hotline registration requirements
5. Alignment with ‘proportionate’ alternate report channels in the workplace
6. Notices to employees, targets and witnesses explaining their rights
7. Restrictions against outsourcing hotlines
8. Communications to targets/witnesses disclosing specific whistleblower denunciations
9. Complying with “sensitive” (EU data directive article 8) data restrictions as to criminal data received by hotline
10. Rights to access, rectify, block or eliminate personal data processed via hotline
11. Restrictions against transferring hotline data outside of Europe
12. Deleting/purging data in hotline call files’
In the article, Dowling also states that before offering a hotline in a particular EU state, companies should attempt to isolate the unique issues that pertain to local law. To do so, they should check to determine which of these 12 issues are present in the relevant jurisdiction. (Refer to the summaries of local law that appear later in this paper.) Companies should then take steps necessary to make hotline reporting protocols and employee communications packages comply. Some multinationals have successfully dealt with these issues by developing a variable European hotline structure, while others tailor specific hotline protocols for each member state.

**Three-Step Process for Developing a Solution**

While Dowling indicates that there is no one perfect solution or “magic bullet” to resolving the hotline dilemma in European nations, he does suggest the implementation of a three-step process that enables multinational companies to tailor a solution to their unique situation. The following are actions that Dowling believes a company should take when establishing a hotline in any EU business operation:

**Step 1: Assess its position regarding EU data protection law issues.**

The issues relevant to implementing whistleblower hotlines include:

- Limiting the list of reportable offenses pertaining to the whistleblower hotline
- Integrating hotlines into the specific structures and protocols that pertain to European workplaces
- Discouraging anonymity, while keeping silent about anonymity in Spain and France
- Not requiring rank-and-file workers to report on colleagues’ misconduct
- Clearly communicating due process rights, particularly the presumption of innocence
- Obtaining permission to implement a hotline where necessary, as mandated by local data privacy agencies
- Translating hotline communications into the applicable local language
- Ensuring that any hotline calls routed outside the EU comply with applicable rules pertaining to the restriction of data sent abroad
- Securing hotline data in accordance with EU data security laws
- Conducting internal investigations of hotline complaints in accordance with accepted European practices
- Purging or destroying records of incidents as soon as the matter is resolved

**Step 2: Choose the appropriate strategy.**

According to Dowling, after assessing its position in relation to EU data protection issues, the company should then choose from one of five possible strategies for developing a hotline in Europe.

*Strategy #1: No hotline- Completely avoid implementation of any type of hotline in Europe.*

*Strategy #2: One global hotline- Use one hotline for all global operations, although this may result in a hotline that is overly restrictive for effective use in U.S. operations.*
Strategy #3: Two hotlines - Implement one hotline for U.S.-type operations and another for European-type operations.

Strategy #4: Tailored hotlines - Create one hotline template and tailor it to each European jurisdiction. This approach is likely the best way to ensure full compliance with European laws and processes.

Strategy #5: Informal reporting procedures - Rely upon “under the radar” reporting procedures instead of a full-blow hotline, although this could lead to compliance issues in some cases.

**Five Potential Hotline Strategies**

- **Strategy 1: No Hotline**
- **Strategy 2: One Global Hotline**
- **Strategy 3: Two Hotlines**
- **Strategy 4: Tailored Hotlines**
- **Strategy 5: Informal Reporting Procedures**

**Step 3: Inform/Consult/Co-determine**

Before implementing any of the above strategies in Europe, companies should take the time to inform/consult/co-determine with worker representatives in the European operation prior to launching.
Overview of Data Privacy Compliance by Nation

As each European nation offers its own unique set of laws, rules and regulations pertaining to data privacy compliance, it is important to gain an awareness of the laws before launching a hotline in a particular nation. White & Case has developed the following summary of the applicable data privacy practices in many European countries to assist in the process. Please note that these are the laws and practices that were in place as of October, 2007.

Austria

Austria, as a member of the European Union ("EU"), was required to implement the EU Data Protection Directive 95/46/EC (the "Directive") into its national legislation. The Directive was implemented in Austria pursuant to the Austrian Data Protection Act 2000 (the "Act"). The Act established a Data Protection Commission ("DPC") and a Data Protection Council that have powers of investigation and enforcement to ensure compliance with the Act.

Collection and Processing of Personal Data

**Compliance Alternatives** An employer may process personal data if the data constitutes a legitimate element in conducting the employer’s business or in complying with the employer’s contractual and other obligations with the employee.

**Disclosure/ Registration** Generally, prior to processing employee data, an employer must file a notification with the DPC for registration in the Data Processing Register. The notification has to state the categories of recipients - including possible recipient states abroad - as well as the legal basis for and the purpose of the processing of data, a description of the categories of the individuals concerned by the processing and the kind of data relating to them.

**Other Requirements** Employees have the right to access, correct, delete, or keep confidential their personal data. Employees also have the right to know the origin of the data and the identity of data recipients. An employer must take measures to ensure the security and confidentiality of personal data. Under Austrian labor law, if a works council has been established, the council’s consent may be required to process and transfer employees’ personal data.

Transfer of Personal Data

**Compliance Alternatives** The cross-border transfer of personal data does not require authorization from the DPC if 1) the data has already legitimately been published, 2) the data transferred is indirectly personal to the recipient; 3) the cross-border transfer is otherwise authorized by directly applicable legal provisions; 4) the data is transferred for private purposes or journalistic activities, 5) the employee has clearly consented to the cross-border transmission; 6) the transfer is necessary to fulfill a contract in the clear interest of the employee; or 7) the transfer is necessary for the establishment, exercise or defense of legal claims before a foreign authority and the data was collected legitimately.
Absent an exemption (e.g., employee consent), the cross-border transfer of personal data to a country that does not provide adequate data protection requires a permit from the DPC. Use of an intercompany agreement (e.g., standard contractual clauses) is recommended to facilitate DPC permission.

No authorization is required for data transfers to recipients in countries with an adequate level of data protection (e.g., member states of the EU).

**Other Requirements** If an employee gives his written consent to the transfer of data, the consent must specifically state the entities to which data are to be transferred, the purpose of the data transfer, the exact kinds of data to be transferred and the notice that the employee's consent may be withdrawn at any time. The declaration of consent should be printed in such a way that it is clearly separated from any other wording. Also, the declaration of consent should be followed by a separate signature of the employee.

**Belgium**


**Collection and Processing of Personal Data**

**Compliance Alternatives** The collection and processing of personal data is allowed where: 1) the employee consents; 2) it is necessary for the employment contract; 3) it is necessary for compliance with a legal obligation to which the employer is subject; 4) it is necessary to protect the vital interests of the employee; 5) it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the employer or in a third party to whom the data is disclosed; or 6) it is necessary for the legitimate interests pursued by the employer or by the third party to whom the data is disclosed, provided that the interests or fundamental rights and freedoms of the employee are not overridden.

**Disclosure/ Registration** None applicable.

**Other Requirements** Facts regarding the processing of personal data must be provided to employees at the time of the collection of the personal data. The employee also must be allowed to access the personal data to make sure it is accurate.

**Transfer of Personal Data**

**Compliance Alternatives** The cross-border transfer of personal data is allowed where: 1) the employee consents; 2) it is necessary for the employment contract; 3) it is necessary for the conclusion or performance of a contract between the employer and a third party that is in the interest of the employee; 4) it is necessary or legally required on important public interest or legal grounds; 5) it is necessary to protect the vital interests of the employee; or 6) the data is from a public register. Transfer of personal data from Belgium to non-EU/European Economic Area countries is permitted to the extent that such
countries provide an adequate level of protection. Belgium has approved a standard contract for cross-border transfer to a data employer, pursuant to which employee consent is not required. For the transfer of data to the US, Belgium will view compliance with the US/EU Safe Harbor principles as compliance with the cross-border transfer law in Belgium.

**Other Requirements** The employee must be given advance notice of any transfer to third party recipients.

## Czech Republic

The collection, processing, and transfer of personal data are regulated under the Data Protection Act (the "Act"). Since the Czech Republic joined the European Union ("EU") in May 2004, the Act was subject to revisions necessary to implement the EU Data Protection Directive 95/46/EC.

### Collection and Processing of Personal Data

**Compliance Alternatives** An employer may process personal data without a consent of an employee, provided that he is carrying out processing which is essential 1) to comply with legal obligation of the employer (e.g., for social security purposes, an obligation under the Czech Labor Code, etc.) or 2) for fulfillment of an employment contract to which the employee is a contracting party or 3) for negotiations on conclusion or alteration of an employment contract. In the case of collection and processing of personal data for other purposes, the employee’s written consent is required.

The employer is obliged to inform the employee of the scope in which and the purpose for which the personal data shall be processed, who and in what manner will process the personal data, to whom the personal data may be disclosed and of the right of the employee to access to its personal data.

**Disclosure/ Registration** An employer may collect and process personal data regarding its employees without any notification to the Czech Office on Protection of Personal Data (the "Authorities"), provided that data are collected and processed to comply with the employer’s obligations under the Czech law.

**Other Requirements** An employer who collects personal data is obliged to: 1) determine the purpose for which personal data will be collected, and collect data only within the scope of such purpose; 2) determine the means and method of data processing and maintenance (e.g., electronic); 3) maintain only true and correct personal data, and allow access to and rectification of personal data; 4) maintain personal data only for a necessary period of time; 5) collect personal data openly; and adopt measures preventing unauthorized or accidental access to personal data, their alteration, destruction or loss, unauthorized transmission or other unauthorized processing, as well as other misuse of personal data.

Employees must be informed in writing about the possibility to access their data. In the event that data are from a source that is unrelated to the employee, the employer must inform the employee in writing of the origin and nature of such data.
Transfer of Personal Data

**Compliance Alternatives** Free flow of personal data shall not be restricted if data are transferred to a member state of the European Union. Personal data may be transferred to third countries if the prohibition of restriction of the free movement of personal data is ensuing from an international treaty or if the personal data are transferred on the basis of a decision of an institution of the European Union.

Where the abovementioned conditions are not met, the transfer of personal data may only be carried out with the permission of the Authorities provided the employer proves that: (1) data transfers are carried out with the consent of the employee; (2) there are sufficient specific guarantees for personal data protection in the country where personal data are to be processed; (3) the personal data concerned are part of publicly accessible data files or are accessible to someone who proves legal interest; (4) the transfer is necessary to exercise an important public interest; (5) the transfer is necessary for negotiating the conclusion or change of an contract, carried out at the instigation of the employee, or for the performance of a contract to which the employee is a contracting party; (6) the transfer is necessary to perform a contract between the employer and a third party, concluded in the interest of the employee, or to exercise other legal claims, or (7) the transfer is necessary for the protection of rights or important vital interests of the employee, in particular for rescuing life or providing health care. When granting the permission to the transfer, the Authorities will specify the period of time during which the controller may perform data transfers.

**Other Requirements** None applicable.

Denmark

The Danish Constitution of 1953 contains provisions relating to privacy and data protection. Denmark, as a member of the European Union ("EU"), was required to implement the EU Data Protection Directive 95/46/EC (the "Directive") into its national legislation. The Directive was implemented in Denmark pursuant to the Act on Processing of Personal Data (the "Act"), which became effective in 2000. An independent agency, the Data Protection Agency ("DPA") enforces the Act.

**Collection and Processing of Personal Data**

**Compliance Alternatives** In general, personal data may be processed in circumstances including where: 1) the employee has given his or her explicit consent; 2) processing is necessary (a) for the performance of a contract to which the employee is a party (NB an employment relationship is a de facto contract) or (b) to take steps at the employee's request prior to entering into a contract; 3) processing is necessary for compliance with a legal obligation to which the employee is subject, or 4) processing is necessary for the purposes of the legitimate interests pursued by the employer or by the third party to whom the data are disclosed, and these interests are not overridden by the interests of the employee.

Absent an exemption (e.g., employee's explicit consent), sensitive data (e.g., racial or ethnic origin, political opinions, party affiliation, and religion) may, however, not be processed.
**Disclosure/ Registration** Generally, the DPA must be notified prior to the processing of personal data. The DPA is required to record data processing activities in a register accessible by the general public. The employers processing of non-sensitive personal data regarding employees does not require notification to the DPA.

**Other Requirements** The employer must implement appropriate technical and organizational security measures to protect personal data against accidental or unlawful destruction, loss or alteration and against unauthorized disclosure, abuse or other processing in violation of the provisions set out in the Act.

An employee may withdraw his or her consent to the processing of data relating to him or her. The employer must, at the request of the employee, rectify, erase, or block data which turns out to be inaccurate or misleading or is in any other way processed in violation of law or regulations.

Upon request from the employee, the employer is obliged to inform the employee whether or not data relating to the employee are being processed, and if data is being processed, the employer shall notify the employee about 1) the data that are being processed, 2) the purposes of the processing, 3) the categories of recipients of the data, and 4) any available information as to the source of such data.

**Transfer of Personal Data**

**Compliance Alternatives** The transfer of data to a country outside the EEA may take place only if the third country in question ensures an adequate level of data protection.

Additionally, transfer of data to a third country may take place if: 1) the employee has given his explicit consent; 2) the transfer is necessary (a) for the performance of a contract between the employee and the employer or (b) to take steps at the employee’s request prior to entering into a contract; 3) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the employee between the employer and a third party; 4) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims; 5) the transfer is necessary in order to protect the vital interests of the employee; 6) the transfer is made from a register which according to law or regulations is open to consultation either by the public in general or by any person who can demonstrate legitimate interests; 7) the transfer is necessary for the prevention, investigation, and prosecution of criminal offenses and the execution of sentences or the protection of persons charged, witnesses or any other persons in criminal proceedings; or 8) the transfer is necessary to safeguard public or national security.

If the legal basis for the transfer is no 2), 3) or 4), prior approval of the transfer must be obtained from the DPA.

The DPA may authorize a transfer of personal data to a third country with an inadequate level of protection if an employer provides adequate safeguards with respect to the protection of the rights of the employee. The DPA may require the fulfillment of additional conditions for such a transfer.
Use of standard contractual clauses is advised to facilitate DPA authorization for data transfer. The EU commission has prepared a model contract that can be used.

Furthermore, personal data may be transferred to US companies participating in the Safe Harbor program, as such companies due to the Safe Harbor data processing obligations are considered to ensure an adequate level of data protection.

Other Requirements None applicable.

Finland

The Constitution of Finland provides privacy rights for all individuals. Finland, as a member of the European Union ("EU"), was required to implement the EU Data Protection Directive 95/46/EC (the "Directive") into its national legislation. The Directive was implemented in Finland pursuant to the Personal Data Act 1999 (the "Personal Data Act"). The Personal Data Act applies to the public and private sectors as well as manual and automated files. The Act on the Amendment of the Personal Data Act entered into force on December 1, 2000 and sets forth certain additional provisions for the cross-border transfer of personal data.

The Act on Data Protection in Working Life (the "Working Life Act"), which became effective on October 1, 2004, supplements the Personal Data Act. The Working Life Act relates solely to the relationship between an employee and an employer. The Office of the Data Protection Ombudsman ("DPO") is an independent governmental agency that guides and controls the processing of personal data and provides related consultation. The Data Protection Board ("DPB") deals with questions of principle relating to the processing of personal data. Both the DPO and the DPB have decision-making authority under the Personal Data Act.

Collection and Processing of Personal Data

Compliance Alternatives Under the Personal Data Act, personal data may be processed in certain circumstances, including where: 1) the employee unambiguously consents to the processing; 2) processing is necessary (a) to perform a contract to which the employee is a party (N.B. an employment relationship is a de facto contract) or (b) to take steps at the employee's request prior to entering into a contract; 3) processing is necessary to protect the vital interests of the employee; 4) processing is necessary for compliance with a legal obligation; 5) there is a relevant connection between the employee and the operations of the employer, based on the employee being in the service of the employer; or 6) the data relates to the employees of a group of companies or another comparable economic group, and the data is processed within such group.

Further, the Working Life Act specifically governs the processing of employees' personal data. Under the Working Life Act, an employer can only process personal data that is directly necessary for the employment relationship and concerns management of the rights and obligations of the parties to the relationship or benefits provided by the employer for the employee, or arises from the special nature of the work (so-called necessity requirement). No exceptions can be made to this provision even with the
employee's consent. Generally, an employer must collect information concerning the employee from the employee. The employee's consent or an exemption to the consent requirement (e.g., obtaining a credit report or criminal record to determine employee reliability) is required for an employer to collect an employee's personal information from a third party.

Absent an exemption or the employee's express consent, the processing of sensitive data (e.g., racial or ethnic origin, political opinions, party affiliation, and religion) is prohibited.

**Disclosure/ Registration** Generally, an employer must disclose its data processing activities to the DPO. However, an employer is not required to disclose data processing activities to the DPO in certain circumstances, including where: 1) the employee has unambiguously consented to the processing; 2) the processing is necessary to perform a contract to which the employee is a party or in order to take steps at the request of the employee before entering into a contract; or 3) the processing is necessary to protect the vital interests of the employee.

**Other Requirements** Generally, an employee is entitled to know what data concerning him or her has been recorded in a personal data file or that the file does not contain any such data.

An employer must ensure that incorrect, incomplete, or outdated personal data is not processed. An employer must take measures to ensure the security and confidentiality of personal data (duty of care).

Privacy in electronic communications (including private e-mail messages and private phone calls) is protected in Finland. In addition to the Working Life Act, the Act on the Protection of Privacy in Electronic Communications (effective as of September 2004) should be taken into consideration as regards ensuring that possible monitoring and any other measures taken by the employer in respect of the privacy of the employee's phone calls and other electronic communication take place in accordance with applicable law.

**Transfer of Personal Data**

**Compliance Alternatives** Finland permits cross-border transfer of personal data without prior DPO notification, in certain circumstances, including where: 1) an employee provides an unambiguous consent to the transfer, 2) the transfer is necessary for the performance of a contract to which the employee is a party, 3) the transfer is made to a country with an adequate level of data protection (e.g., EU member states or European Economic Area countries), or 4) the transfer is made using certain standard contractual clauses approved by the European Commission.

For the transfer of data to the US, Finland will consider compliance with the US/EU Safe Harbor principles as compliance with the cross-border transfer law in Finland.

**Other Requirements** None applicable.
France

The collection, processing, and transfer of personal data are regulated under the Data Processing, Data Files and Individual Liberties Law of 1978 (the “Law”). France, as a member of the European Union (“EU”), was required to implement the EU Data Protection Directive 95/46/EC (the “Directive”) into its national legislation. Further amendments to the Law came into effect in August 2004, bringing the Law in line with the requirements of the Directive. The Commission Nationale de l’Informatique et des Libertés (“CNIL”) is the national authority in charge of data privacy. In May 2005, the CNIL published a guide on international data transfers.

Collection and Processing of Personal Data

**Compliance Alternatives** Personal data collected must be necessarily and directly linked to the position offered, or the employee’s professional qualifications to perform the job. Employees must be: 1) asked whether they wish to provide the data; 2) informed of the mechanism and purpose of collection, and the persons who will have access; 3) given the option to refuse to provide the data, and notified of any consequences of such refusal; and 4) given the right to access and rectify the personal data, or to withdraw consent. In lieu of consent, personal data also may be collected and processed in certain circumstances, including where it is necessary for the legitimate interests of the company, unless such interests are overridden by the interests or fundamental rights and freedoms of the employee concerned.

Employee consent, among other requirements, is required when processing sensitive data (e.g., racial or ethnic origin, political opinions, party affiliation, and religion).

**Disclosure/ Registration** The Works Council must be informed/consulted before the introduction or modification of any system of the employer allowing the automated processing of employee data. The CNIL must be notified of certain mandatory information, as well as the commitment of the employer that the processing of data will comply with the provisions of the Law. The processing only can be implemented upon CNIL’s acknowledgement that such notification has been received. Companies that choose to appoint a data protection officer are exempt from certain notification requirements.

**Other Requirements** None applicable.

Transfer of Personal Data

**Compliance Alternatives** The cross-border transfer of personal data is allowed where: 1) the employee consents; 2) it is necessary for the performance of the employment contract; 3) it is necessary for a contract between the employer and a third party that is in the interest of employee; 4) it is necessary or legally required on important public interest or legal grounds; 5) it is necessary to protect the vital interests of the employee; or 6) the data is from a public register.

An employee’s social insurance number cannot be transferred abroad under any circumstances for identification purposes.

The transfer of personal data from France to non-EU/European Economic Area countries is permitted to the extent that such countries provide an adequate level of protection. Although France has not expressly
approved a standard contract for cross border data transfers, the EU Commission ruled that certain standard contractual clauses offer sufficient safeguards. France, as an EU Member state, recognizes these contractual clauses as adequate. Non-standard contracts or codes of conduct are acceptable, provided they contain adequate safeguards for privacy rights and the exercise of associated rights, and are authorized by the CNIL. The CNIL also encourages the use of binding corporate rules.

For the transfer of data to the US, France will view compliance with the US/EU Safe Harbor principles as compliance with the cross-border transfer law in France.

**Other Requirements** If data will be transferred outside of France, this fact, as well as the nature of the data, the purpose and conditions, and the country to which the data is to be transferred, must be included in the notification made to the CNIL. The employer and the third party recipient must conclude an agreement, whereby the third party recipient agrees to comply with the French laws on the protection of the data, and this agreement must be included in the filing with the CNIL.

**Germany**

Germany, as a member of the European Union ("EU"), was required to implement the EU Data Protection Directive 95/46/EC (the "Directive") into its national legislation. The Directive was implemented in Germany in May 2001 pursuant to an amendment of the German Federal Data Protection Act.

**Collection and Processing of Personal Data**

**Compliance Alternatives** The collection and processing of personal data is allowed where: 1) the employee consents; 2) it is for the purposes of an employment agreement; 3) it is necessary to safeguard the valid interests of the employer and the employee does not have an overriding legitimate interest to exclude the data; 4) the data generally is accessible, or the employer has the right to publish the data, unless the employee’s legitimate interest in precluding the data clearly outweighs such interest; 5) it is necessary to protect public interests and the legitimate interest of a third party, and the employee does not have a legitimate interest in the data being excluded; or 6) permission exists under national law (e.g., collective labor agreements).

When processing sensitive data (e.g., racial or ethnic origin, political opinions, party affiliation, and religion), the employee’s explicit consent is required, unless such data is necessary to pursue or defend against legal claims, or it concerns health data related to any sick leave taken by the employee.

**Disclosure/ Registration** An employer must appoint a data protection official if there are more than nine employees in Germany involved in the “automated processing of data” (which includes the processing of data by computers). The data protection officer can be an in-house employee, should not be a member of management, should be in an independent position to ensure company compliance with German data privacy requirements, and should “qualify” by attending some seminars on data protection that are readily available in Germany.

**Other Requirements** None applicable.
Transfer of Personal Data

**Compliance Alternatives** Only if an employer in Germany does not appoint a data protection officer, it must register with the data protection authorities if it automatically processes and transfers (including within Germany). To register, the employer must complete and submit a simple form to the local data protection authority (e.g., if the company resides in Hamburg, the data protection authority of Hamburg would be the relevant local authority). No fee is required. No approval by the authorities is required. The form generally calls for information that includes the following: name and address of company; managing person of company; names of person(s) involved in the processing of data; purpose of processing and use of data; the group of persons affected by the processing of data; if data is transferred within or outside of Germany, the name of the transferees; and information on how the data is kept secure (technical measures taken to ensure that the data cannot be stolen, etc.).

The cross-border transfer of personal data from Germany to non-EU/European Economic Area ("EEA") countries is permitted where: 1) such countries provide an adequate level of protection, or 2) the employee consents; or 3) it is necessary for the performance of an employment contract; or 4) it is necessary for a contract between the employer and a third party that is in the interest of the employee; or 5) it is necessary or legally required on important public interest, or for the establishment, exercise or defense of legal claims; or 6) it is necessary to protect the vital interests of the employee; or 6) the data is from a public register.

The transfer of personal data from Germany to non-EU/European Economic Area ("EEA") countries is also permitted to the extent that the data transferor and transferee have entered into the European standard contract for cross-border data transfers. Alternatively, non-standard contract or codes of conduct are acceptable, provided they contain adequate safeguards with respect to privacy rights and the exercise of associated rights, and if the data transfer operation or particular categories of transfer operations according to the contract or codes of conduct have been approved by the competent supervisory authority. For the transfer of data to the US, Germany views compliance with the US/EU Safe Harbor principles as compliance with the cross-border transfer law in Germany.

**Other Requirements** It is not permissible to transfer employee data to any trade union in order to enable the trade union to collect debts, or to any insurance company for advertising purposes.

Ireland

The Constitution of Ireland does not provide an express right to privacy, however, it has been held to establish an implied right to privacy. The Data Protection Act 1988 (the “Act”) implemented the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Ireland, as a member of the European Union ("EU"), was required to implement the EU Data Protection Directive 95/46/EC (the “Directive”) into its national legislation. The Directive was implemented in Ireland pursuant to the Data Protection (Amendment) Act 2003, which amended the Act. The Office of the Data Protection Commissioner ("DPC") enforces the Act.
Collection and Processing of Personal Data

**Compliance Alternatives** Personal data may be processed in circumstances including where: 1) the employee has given consent; 2) processing is necessary (a) to perform a contract to which the employee is a party (N.B. an employment relationship is a de facto contract) or (b) to take steps at the employee’s request prior to entering into a contract; 3) processing is necessary for compliance with a legal obligation; 4) processing is necessary to protect the vital interests of the employee; 5) processing is necessary for a public purpose; or 6) processing is necessary for the legitimate purpose of the employer (e.g., personnel and human resources purposes), except where the processing is unwarranted by reason of prejudice to the fundamental rights and freedoms or the legitimate interests of the employee.

Sensitive data (e.g., racial or ethnic origin, political opinions, party affiliation, and religion) may be processed only if the conditions for personal data processing (e.g., performance of a contract to which the employee is a party) are met along with an additional condition including 1) employee’s explicit consent to the processing employee, 2) processing is necessary for a right or obligation under employment law, or 3) processing is necessary for a public purpose.

**Disclosure/ Registration** Certain categories of data controllers and data processors (e.g., financial institutions, insurance companies, and companies which keep sensitive data) must register with the DPC before processing personal data.

**Other Requirements** An employer must keep employees’ personal data secure from unauthorized access, disclosure, destruction or accidental loss. An employer must ensure that employees’ personal data is kept accurate and up-to-date.

**Transfer of Personal Data**

**Compliance Alternatives** Cross-border transfer of personal data to a country outside the European Economic Area (“EEA”) is permitted if that country ensures an adequate level of data protection, as determined by the EU Commission or the DPC.

Cross-border transfer of personal data to a country outside the EEA with inadequate data protection is permitted if the transfer is: 1) consented to by the employee, 2) required or authorized under an enactment, convention or other instrument imposing an obligation on the State, 3) necessary for the performance of contract between the employer and the employee, 4) necessary for the taking of steps at the request of the employee with a view to his or her entering into a contract with the employer, 5) necessary for the conclusion of a contract between the employer and a third party, that is entered into at the request of the employee and is in the interests of the employee, or for the performance of such a contract, 6) necessary for the purpose of obtaining legal advice, 7) necessary to urgently prevent injury or damage to the health of an employee, 8) part of the personal data held on a public register, or 9) authorized by the DPC where the employer adduces adequate safeguards with respect to the privacy and fundamental rights and freedoms of individuals and for the exercise by individuals of their relevant rights under the Act or the transfer is made on terms of a kind approved by the DPC as ensuring such safeguards (e.g., standard contractual clauses, US/EU Safe Harbor principles).
Where employees' personal data is transferred within a multinational group for regular personal and human resources purposes, explicit employee consent is not necessary. The DPC has concluded that an employee working for a multinational company implicitly consents to his or her personal data being shared or transferred within that organization.

**Other Requirements** None applicable.

**Italy**

The Constitution of Italy provides privacy rights for all individuals. Italy, as a member of the European Union ("EU"), was required to implement the EU Data Protection Directive 95/46/EC (the "Directive") into its national legislation. The Directive was implemented in Italy pursuant to Law No. 675 of December 1996 (the "Law"). The Law along with other legislative initiatives, were consolidated by way of the Data Protection Code, namely, Legislative Decree No. 196 of 30 June 2003 (the "Code"), which was enforced on 1 January 2004. The Code governs the collection, processing and use of personal data in the private and public sectors. The Supervisory Authority for Personal Data Protection (the "Authority") enforces the Code.

**Collection and Processing of Personal Data**

**Compliance Alternatives** Personal data may be processed in circumstances including where: 1) the employee consents to the processing, 2) the processing is necessary (a) for the performance of obligations resulting from a contract to which the employee is a party (N.B. an employment relationship is a de facto contract) or (b) to take steps at the employee's request prior to entering into a contract, or 3) for the performance of a lawful obligation.

Sensitive data (e.g., racial or ethnic origin, political opinions, party affiliation, and religion) may be processed only if the employee gives his or her written consent and the processing is authorized by the Authority.

**Disclosure/ Registration** Generally, an employer must register with the Authority prior to processing employees' personal data.

An exemption from registration exists if data processing is carried out exclusively to comply with specific obligations in connection with personnel and human resources matters and the data is kept for no longer than is necessary.

**Other Requirements** Personal data must be accurate and up-to-date. An employee has a right to object to the processing of his or her personal data.

**Transfer of Personal Data**

**Compliance Alternatives** Generally, employee consent is required for the transfer of personal data outside the EU. However, employee consent is not required if the cross-border data transfer is 1)
necessary for the performance of obligations resulting from a contract to which the employee is a party, or in order to take steps at the employee's request prior to entering into a contract, or for the conclusion or performance of a contract made in the interest of the employee; or 2) authorized by the Authority.

The Authority has authorized the transfer of personal data from Italy to countries outside the EU where the transfer is made using standard contractual clauses or where the laws of the country of destination ensure adequate protection of the data (e.g., Hungary and Switzerland).

For the transfer of data to the US, Italy will view compliance with the US/EU Safe Harbor principles as compliance with the cross-border transfer law in Italy.

**Other Requirements** None applicable.

**Netherlands**

The Constitution of the Netherlands provides traditional privacy rights for all individuals and protects the personal data of individuals. The Netherlands, as a member of the European Union (“EU”), was required to implement the EU Data Protection Directive 95/46/EC (the “Directive”) into its national legislation. The Directive was implemented in the Netherlands pursuant to the Personal Data Protection Act (the “Act”), which revised and expanded the Data Registration Act of 1998. The Dutch Data Protection Authority (“DPA”) enforces the Act.

**Collection and Processing of Personal Data**

**Compliance Alternatives** Personal data may be processed in circumstances including where: 1) the employee has unambiguously given his or her consent; 2) the processing is necessary (a) to perform a contract to which the employee is a party (e.g., an employment relationship is a de facto contract) or (b) to take steps at the employee's request prior to entering into a contract; 3) the processing is necessary to comply with a legal obligation to which the employer is subject (e.g., tax law provisions regarding income tax), 4) the processing is necessary to protect the vital interests of the employee; 5) processing is necessary for the proper performance of a public law duty by an administrative body, or 6) the processing is necessary for upholding the legitimate interests of the employer or of a third party to whom the data is supplied, except where the interests or fundamental rights and freedoms of the employee, in particular the right to protection of individual privacy, prevail.

Personal data may only be collected and processed for specified, explicit, and legitimate purposes. The data must be adequate, relevant, and not excessive in relation to the purposes for which it is collected and/or further processed.

Generally, the processing of sensitive data (e.g., racial or ethnic origin, political opinions, party affiliation, and religion) is prohibited. There are exemptions. An exemption e.g., exists for processing data about employees’ race for identification purposes or in connection with an affirmative action program.
An employer must provide employees with information including the purpose(s) of the processing for which the data are intended. More detailed information should be provided where given the type of data, the circumstances in which they are to be obtained or the use to be made thereof; this is necessary in order to guarantee that the processing is carried out in a proper and careful manner. An exemption to this requirement exists if the employee already possesses the described information.

**Disclosure/ Registration** Generally, the fully or partly automated (and certain manual) data processing must be reported to the DPA for registration in a public registry. However, certain categories of data processing (e.g., personnel and human resources data) are exempt from the reporting requirement, provided certain requirements are fulfilled.

**Other Requirements** An employer may submit a code of conduct to the DPA for review and determination that the code implements the Act and other legal provisions in connection with the processing of personal data. This is usually used by a group of organizations in a particular line of business.

An employer must secure and maintain the confidentiality of personal data.

An employee may request access to his or her personal data, and request that an employer correct, supplement, delete, or block his or her data if it is factually inaccurate, incomplete, or irrelevant to the purpose or purposes of processing, or is being processed in any other way which infringes a legal provision.

**Transfer of Personal Data**

**Compliance Alternatives** Under the Act, an employer is permitted to transfer employees' personal data to EU member countries and non-EU countries with adequate levels of data protection, provided that the other requirements of the Act are fulfilled.

An employer may transfer data to a country with an inadequate level of data protection in circumstances including where: 1) the employer obtains unambiguous consent to the proposed transfer from the employee; 2) transfer is necessary (a) for the conclusion or performance of a contract between the employee and the employer or (b) to take steps at the employee's request prior to concluding a contract; or 3) transfer is necessary for the performance or conclusion of a contract concluded or to be concluded in the interests of the employee between the employer and a third party.

Alternatively, an employer may apply for a permit from the Minister of Justice for transfer of personal data to a country with an inadequate level of data protection. The use of standard contractual clauses will facilitate the grant of a permit.

**Other Requirements** None applicable.
Norway

The Norwegian Constitution of 1814 does not contain specific privacy provisions. The Personal Data Act of 2000 (the “Act”) regulates the processing of personal data. Although Norway is a member of the European Economic Area (“EEA”), but not a member of the European Union (“EU”), the Act implements the EU Data Protection Directive 95/46/EC into Norway’s national legislation. The Act applies to both the public and private sectors. The Data Inspectorate (“Inspectorate”), an independent administrative agency, enforces the Act.

Collection and Processing of Personal Data

Compliance Alternatives Personal data may only be processed: 1) if the employee has consented to such processing; 2) if there is statutory authority for such processing; 3) to fulfill a contract to which the employee is party (e.g., an employment relationship is a de facto contract), or to take steps at the employee’s request prior to entering into such a contract; 4) to enable the employer to fulfill a legal obligation; 5) to protect the vital interests of the employee; 6) to perform a task in the public interest; 7) to exercise official authority; or 8) to enable the employer or third parties to whom the data is disclosed to protect a legitimate interest, except where such interest is overridden by the interests of the employee.

Sensitive data may be processed in circumstances including where: 1) the employee consents to such processing; or 2) there is statutory authority for such processing.

Disclosure/ Registration Generally, an employer must notify the Inspectorate prior to: 1) processing an employee’s personal data by automatic means or 2) establishing a manual personal data filing system containing sensitive data.

Generally, an employer must obtain a license from the Inspectorate prior to processing sensitive data, unless the employee has volunteered the data.

An exemption from the notification and license requirements exists if: 1) an employee consents to the processing of his or her personal/sensitive data, 2) the data is connected to the employment relationship, and 3) the data is intended for human resources/employee administration purposes.

The Inspectorate may decide that the processing of data other than sensitive data is subject to licensing if such processing otherwise would violate the employee’s substantial privacy interests. An employer may demand that the Inspectorate decide whether processing is subject to licensing.

Other Requirements Personal data must be kept accurate and up-to-date, and not stored any longer than is necessary.

When processing an employee’s personal data, an employer must provide the employee with information including: 1) the purpose of data processing, 2) whether the data will be disclosed, and if so, the identity of the recipient, and 3) the existence of the rights to demand access and correction of the data.
Transfer of Personal Data

Compliance Alternatives Generally, the cross-border transfer of personal data is only permitted to countries that ensure an adequate level of data protection.

The cross-border transfer of personal data to countries with inadequate data protection is allowed if: 1) the employee has consented to the transfer, 2) there is an obligation to transfer the data pursuant to an international agreement or as a result of membership of an international organization, 3) the transfer is necessary for the performance of a contract with the employee, or for the performance of tasks at the employee’s request prior to entering into such a contract, 4) the transfer is necessary for the conclusion or performance of a contract with a third party in the interest of the employee, 5) the transfer is necessary in order to protect the vital interests of the employee, 6) the transfer is necessary in order to establish, exercise or defend a legal claim, 7) the transfer is necessary or legally required in order to protect an important public interest, or 8) there is statutory authority for demanding data from a public register.

Alternatively, the Inspectorate may allow transfer to countries with an inadequate level of data protection if an employer provides adequate safeguards (e.g., an intercompany agreement) with respect to the protection of the rights of the employee. The Inspectorate may stipulate conditions for the transfer.

Other Requirements None applicable.

Poland

The Constitution of Poland provides traditional privacy rights for all individuals and protects the personal data of individuals. The Law on the Protection of Personal Data Protection (the “Law”) was enacted in October 1997 and took effect in April 1998. Poland joined the European Union (“EU”) in May 2004. In August 2001, the Law was amended to bring it into compliance with the EU Data Protection Directive 95/46/EC. The Bureau of Inspector General for Personal Data Protection (the “Bureau”) enforces the Law.

Collection and Processing of Personal Data

Compliance Alternatives Generally, the processing of personal data is permitted only if: 1) the employee has given his or her consent; 2) processing is necessary in order to exercise rights and duties under a legal provision; 3) processing is necessary (a) for the performance of a contract to which the employee is a party (N.B. an employment relationship is a de facto contract) or (b) to take steps at the employee’s request prior to entering into a contract; 4) processing is necessary for the performance of a task provided for by law and carried out in the public interest; or 5) processing is necessary for the purpose of the legitimate interests pursued by the employer or data recipients, provided that the processing does not violate the rights and freedoms of the employee.
Generally, the processing of sensitive data (e.g., racial or ethnic origin, political opinions, party affiliation, and religion) is prohibited. Exemptions to such prohibition include where: 1) the employee gives his or her written consent, and 2) the processing is necessary for the purpose of carrying out the obligations of the employer with regard to employment of its employees and other persons, and is otherwise legally permitted.

**Disclosure/ Registration** Generally, an employer must notify the Bureau of data processing activities for registration in a public register. An exemption from the notification requirement exists for personal data processed in connection with employment or providing services to the employer.

**Other Requirements** An employer must provide the employee with information including: 1) the purpose of data processing, 2) data recipients, and 3) the existence of the employee's rights of access and correction of the data.

An employer must implement appropriate organizational and technical measures to secure personal data and protect it against accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure or access, as well as any other form of unlawful processing.

**Transfer of Personal Data**

**Compliance Alternatives** Generally, personal data can only be transferred to a third country that ensures at least the same level of data protection as Poland.

However, personal data may be transferred to a third country that does not ensure at least the same level of data protection as Poland if: 1) the employee has given his or her written consent; 2) the transfer is necessary for the performance of a contract between the employee and the employer or takes place in response to the employee's request, 3) the transfer is necessary for the performance of a contract concluded in the interests of the employee between the employer and third party; 4) the transfer is necessary or required by reasons of public interests or for the establishment of legal claims; 5) the transfer is necessary in order to protect the vital interests of the employee; or 6) the transfer relates to data which is publicly available.

Alternatively, the transfer of personal data to a third country which does not ensure at least the same level of personal data protection as Poland may be permitted with the Bureau's prior approval, provided that the employer ensures adequate safeguards (e.g., standard contractual clauses) with respect to the protection of privacy, rights, and freedoms of the employee.

**Other Requirements** None applicable.

**Portugal**

The Constitution of Portugal provides traditional privacy rights for all individuals and protects the personal data of individuals. Portugal, as a member of the European Union ("EU"), was required to implement the EU Data Protection Directive 95/46/EC (the "Directive") into its national legislation. The Directive was implemented in Portugal pursuant to Law 67/98 of October 26th on the Protection of Personal Data (the
The Law regulates the collection, use, and transfer of personal data in manual or electronic form. The National Data Protection Commission ("DPC"), an independent agency, enforces the Law.

Collection and Processing of Personal Data

**Compliance Alternatives** As a general rule, the employee’s unambiguous consent is required for the processing of personal data. However, the Law also admits some exceptions to the general consent rule: 1) the processing is necessary (a) to perform a contract to which the employee is a party (NB. an employment relationship is a de facto contract) or (b) to take steps at the employee’s request prior to entering into a contract or a declaration of the employee’s intent to negotiate; 2) processing is necessary for compliance with a legal obligation to which the employer is subject; 3) processing is necessary to protect the vital interests of the employee if he or she is physically or legally incapable of giving his or her consent; 4) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the employer or in a third party to whom the data are disclosed; or 5) processing is necessary for pursuing the legitimate interests of the employer or the third party to whom the data is disclosed, except where such interests should be overridden by the interests for fundamental rights, freedoms, and guarantees of the employee.

Absent an exemption (e.g., employee’s explicit consent or authorization by the DPC), sensitive data (e.g., racial or ethnic origin, political opinions, party affiliation, and religion) may not be processed.

**Disclosure/ Registration** Generally, prior to processing an employee’s personal data, an employer must notify the DPC.

An exemption from the notification requirement exists for the collection and processing of personal data related to 1) payment of salaries and other employee benefits; 2) calculation of withholding tax and social security obligations; 3) compliance with a court decision or collective agreement; 4) calculation of employee participation in company profits, and 4) statistical purposes concerning the processing of salaries.

These exemptions from notification are only applicable in the exact terms of the Exemption Decisions of the DPC (e.g., payment of salaries with transfer of data to other country, either EU or not, the exemption does not apply and the employer remains obliged to notify the DPC).

**Other Requirements** An employee has a right to object at any time to the processing of data relating to him or her.

An employer must provide employees with information including: 1) the purpose of data processing, 2) the recipients or the categories of recipients of such data, and 3) the existence of rights to access and correct the data.

An employer must process personal data in a confidential manner.

An employer must implement appropriate organizational and technical measures to secure personal data and protect it against accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure or access as well as any other form of unlawful processing.
The DPC encourages the drafting and submission of industry-specific codes of conduct intended to contribute to the proper implementation of the Act. The DPC determines whether such codes comply with the laws and regulations regarding personal data protection.

Russia

Russia adopted a specific law on personal data protection ("Personal Data Law") on 27 July 2006, taking on a similar approach to the EC Data Protection Directive. The Personal Data Law came into force on 26 January 2007. It applies to employees' data protection, along with the prohibition of the processing of information about an individual's private life without his or her consent laid down in the Constitution of the Russian Federation and the relevant specific rules set out in the Labor Code. The Personal Data Law is enforced by the Federal Service for Supervision in the Area of Mass Media, Communications, and Cultural Heritage Protection.

Collection and Processing of Personal Data

**Compliance Alternatives** The employer can collect, keep, use, disseminate or otherwise process an employee's personal data without his or her consent only within the limits and subject to the requirements set out in the applicable legislation. Pursuant to the Personal Data Law, the employee's personal data processing is only allowed without his or her consent if: 1) it is required for the purposes of an agreement (an employment or civil law agreement) to which the employee is a party; 2) it is based on a federal law setting out its purpose, its terms, and the competence of a person processing personal data; 3) it is necessary for statistical or other research-related purposes; 4) it is necessary in order to protect life, health, or other vital interests of the employee provided it is impossible to obtain his or her consent; 5) it is necessary for the administration of postal and electronic communications; 6) it is necessary for journalistic, scientific, literary, or other creative activity provided that the latter does not violate the rights and freedoms of the employee; or 7) the employee's personal data is subject to mandatory publication under a federal law, including the personal data of civil officers.

In addition, the Labor Code provides, inter alia, that employees' personal data: 1) may be processed only for employment-related purposes; 2) may be obtained from the employee him/herself; 3) may not be obtained from or disclosed to a third party unless the employee gives written consent; and 4) may be transferred within the employer company under internal regulations provided an employee's signed acknowledgment of company under internal regulations provided an employee's signed acknowledgment of the internal regulations.

The processing of sensitive data (e.g., racial or ethnic origin, political opinions, religious or philosophical convictions, state of health, and intimate life) and biometrical data is subject to special requirements.

**Disclosure/ Registration** Neither the effective legislation nor the Personal Data Law require an employer to notify of or register its databases containing employees' personal data with any governmental authority.

**Other Requirements** Under the Personal Data Law, an employer must provide, upon an employee's request, access to the employee's personal data and to information regarding the processing of the
employee’s personal data, including: 1) confirmation that personal data is processed and the purpose of the processing; 2) methods of data processing; 3) information on individuals that may have access to his or her personal data; 4) list of personal data being processed; 5) terms of processing of personal data, including storage terms; and 6) information on legal implications of personal data processing.

Access to an employee’s personal data is restricted where: 1) personal data, including the data obtained during investigation and intelligence activities, is processed for the purposes of the country’s defense, security and public order; 2) personal data is processed by investigation bodies; or 3) access to personal data violates the constitutional rights and freedoms of other individuals.

The employer must amend, block, or destroy an employee's personal data upon the employee's request if the personal data is incomplete, outdated, untrue, illegally obtained, or not necessary for the purposes of its processing.

If an employee’s personal data was obtained from a third party, an employer must notify the employee prior to his or her personal data processing of the following: 1) the purpose of, and legal ground for, personal data processing; 2) prospective users of personal data; and 3) the rights of the employee as a data subject.

The employer must ensure confidentiality of its employees' personal data and protect employees' personal data against accidental or unlawful access, destruction, alteration, blocking, copying, unauthorized disclosure or any other unlawful action.

**Transfer of Personal Data**

**Compliance Alternatives** Under the Personal Data Law, the cross-border transfer of personal data is allowed where: 1) personal data is transmitted to a country that provides an adequate level of data protection; 2) the employee gives written consent; 3) it is provided for in international treaties related to visa issuance, or legal assistance on civil, family and criminal matters; 3) it is set forth by federal laws if it is necessary to protect the country's constitutional order, defense and safety; 4) it is necessary for the performance of a contract to which the employee is a party; or 5) it is necessary to protect life, health or other vital interests of the employee or any other individual provided it is not possible to obtain the employee's written consent.

If personal data is transmitted outside Russia based on the employee's written consent, the latter must include: 1) name of the employee; 2) name of the employer; 3) purpose of personal data processing; 4) list of personal data which can be processed; 5) list of data processing operations and a general description of personal data processing methods; and 6) term of validity of the consent and the procedures for its withdrawal.

**Other Requirements** None applicable.
Slovak Republic

The Slovak Republic as a member of the European Union ("EU") has implemented the EU Data Protection Directive 95/46/EC into its national legislation. Collection, processing, and transfer of personal data are regulated under the Act no. 428/2002 Coll., On Personal Data Protection, as amended (the "Act").

Collection and Processing of Personal Data

**Compliance Alternatives** Collection and processing of personal data is permissible where: 1) the employee consents; 2) the personal data are processed pursuant to special laws that stipulate a list of categories of personal data, the purpose of their processing and the group of data subjects; 3) this is necessary for the performance or conclusion of a contract to which the employee is a party; 4) this is necessary for the protection of life, health or property of the employee; 5) the processing concerns solely the title, name, surname, and address of the employee, with no risk of addition of other personal data, and these data are used solely for the controller's needs in terms of correspondence with the employee and record-keeping of such data; 6) the processed personal data have already been made public; in such cases they must be duly labeled as such; 7) it is necessary for the fulfillment of an important task carried out in the public interest; and 8) it is necessary for the protection of statutory rights and legitimate interests of the controller or the third party.

If the collection and processing of personal data concerns “sensitive” data, additional requirements apply.

**Disclosure/ Registration** The general obligation of database registration does not apply to (i) employers who collect and process personal data for exercising such rights and obligations as ensue for an employer from existing or terminated employment relationships, and (ii) employers whose database is subject to the internal supervision of a data protection officer who has been appointed in writing by the employer.

Employers must nonetheless register their database with the data privacy authority for the collection, processing, and transfer of sensitive data that are expected to be transferred, with the employee’s consent, to a third country that does not ensure an adequate level of protection of personal data.

Unless the database registration requirement applies, employers are obliged to keep their own public records of the database, containing: 1) information on the employer; 2) purpose of the processing of personal data; 3) list of personal data; 4) group of data subjects; 5) group of recipients or third parties to whom the personal data will likely be made available; 6) third countries, if data transfer to the same is anticipated, and the legal basis of the trans-border flow; 7) legal basis of the database; 8) characteristics of the measures that ensure the integrity of personal data; 9) date of commencement of the processing of personal data.

**Other Requirements** Employers who collect personal data are obliged to: 1) determine the purpose for which personal data will be collected and processed, and collect data only within the scope of such purpose; 2) determine the means and method of data processing; 3) maintain only true and correct personal data, and allow access and rectification of personal data; and 4) maintain personal data only for the necessary period of time.
Employers are also obliged to take appropriate technical, organizational, and personal measures to ensure the integrity of personal data by protecting them against accidental or unlawful damage or destruction, accidental loss, alteration, unauthorized access and disclosure, as well as any other unauthorized forms of processing.

**Transfer of Personal Data**

**Compliance Alternatives** The personal data may be freely transferred to EU countries and countries that provide an adequate level of personal data protection. If a third country does not ensure an adequate level of protection of personal data, the personal data may be transferred to this country only on the basis of a decision by the European Commission or if any of the following conditions is fulfilled: 1) the employee gave written consent, knowing that the country of final destination does not ensure an adequate level of protection; 2) the transfer is necessary for performance of a contract between the employee and the employer or for establishment of pre-contractual measures upon request of the data subject; 3) the transfer is necessary for the conclusion or performance of a contract between the employer and a third party in the interest of the employee; 4) the transfer is necessary for implementation of an international treaty that binds the Slovak Republic, or the transfer is obligatory by law due to pressing public interest or for proving, filing, or defending a legal claim; 5) the transfer is necessary for protection of vital interests of the employee; or 6) the transfer concerns personal data which constitutes a part of the lists, registers or files that are maintained and made accessible to the general public under special laws or that must be made available, under these laws, to persons who prove a legal claim and fulfill the prerequisites for disclosure prescribed by law.

Permission for transferring personal data must be obtained from the data protection authority only if the employer commissions an entity residing in a non-EU country with processing of the personal data on the employer’s behalf.

**Other Requirements** None.

**Spain**

The Constitution of Spain provides traditional privacy rights for all individuals and protects the personal data of individuals. Spain, as a member of the European Union ("EU"), was required to implement the EU Data Protection Directive 95/46/EC (the "Directive") into its national legislation. The Directive was implemented in Spain pursuant to the 1999 Data Protection Act (the “Act”). The Act regulates the collection, use, and transfer of personal information in both the public and private sectors. The Data Protection Agency ("DPA") enforces the Act.

**Collection and Processing of Personal Data**

**Compliance Alternatives** Personal data may be processed in circumstances including where: 1) the employee has given consent; 2) processing is necessary (a) to perform a contract to which the employee is a party (e.g., an employment relationship is a de facto contract) or (b) to take steps at the employee's
request prior to entering into a contract; 3) processing is necessary for compliance with a legal obligation; 4) processing is necessary to protect the vital interests of the employee; 5) processing is necessary for a public purpose; or 6) processing is necessary for the legitimate purpose of the employer (e.g., personnel and human resources purposes), except where the processing is unwarranted by reason of prejudice to the fundamental rights and freedoms or the legitimate interests of the employee.

Sensitive data may only be processed where: 1) the employee consents to such processing; or 2) there is statutory authority for such processing.

**Disclosure/ Registration** An employer must register its data processing activities with the DPA before processing personal data.

Employers may submit codes of conduct relating to data processing for approval and entry in the DPA’s General Data Protection Register.

**Other Requirements** Generally, an employee is entitled to know what data concerning him or her has been recorded in a personal data file. An employer must provide an employee with information including: 1) the existence of a file or personal data operation, the purpose of collecting the data, and the recipients of the information, and 2) the employee’s rights of access, rectification, erasure, and objection

An employer must ensure that personal data is correct. An employer must take measures to ensure the security and confidentiality of personal data.

**Transfer of Personal Data**

**Compliance Alternatives** The DPA must be notified before personal data is transferred to a third country.

Generally, personal data can only be transferred to a third country that ensures at least the same level of data protection as Spain (e.g., EU member states or European Economic Area countries).

However, personal data may be transferred to a third country that does not ensure at least the same level of data protection as Spain if: 1) the employee has given his or her consent; 2) the transfer is necessary for the performance of a contract between the employee and the employer or takes place in response to the employee’s request, 3) the transfer is necessary for the performance of a contract concluded in the interests of the employee between the employer and third party; or 4) the transfer is necessary or required by reasons of public interests or for the establishment of legal claims.

Alternatively, the transfer of personal data to a third country which does not ensure at least the same level of personal data protection as Spain may be permitted with prior approval of the Director of the DPA, who may grant it if adequate guarantees are obtained. Use of standard contractual clauses is advised to facilitate authorization for data transfer.

For the transfer of data to the US, Spain will view compliance with the US/EU Safe Harbor principles as compliance with the cross-border transfer law in Spain.

**Other Requirements** None applicable.
Sweden

The Constitution of Sweden provides traditional privacy rights for all individuals and protects the personal data of individuals. Sweden, as a member of the European Union ("EU"), was required to implement the EU Data Protection Directive 95/46/EC (the "Directive") into its national legislation. The Directive was implemented in Sweden pursuant to the Personal Data Act 1998 (the "Act"). The Personal Data Ordinance 1998 provides supplementary regulations concerning the processing of personal data under the Act. The Data Inspection Board (the "DIB") enforces the Act.

Collection and Processing of Personal Data

Compliance Alternatives Under the Act, personal data may be processed in circumstances including where: 1) the employee unambiguously consents to the processing; 2) processing is necessary (a) to perform a contract to which the employee is a party (e.g., an employment relationship is a de facto contract) or (b) to take steps at the employee’s request prior to entering into a contract; 3) processing is necessary to protect the vital interests of the employee; or 4) processing is necessary for compliance with a legal obligation.

Absent an exemption (e.g., employees’ express consent or compliance with employment laws), the processing of sensitive data (e.g., racial or ethnic origin, political opinions, party affiliation, and religion) is prohibited.

Disclosure/Registration An employer must disclose its data processing activities to the DIB unless it appoints a data protection representative, who independently ensures that personal data is processed in accordance with the Act.

Other Requirements When processing an employee's personal data, an employer must provide the employee with information including: 1) the data being processed, 2) the purpose(s) of the processing, 3) the recipients of the data, 4) any available information as to the source of such data, and 5) rules on the right of access to and the right to rectify the data relating to the employee.

An employer must ensure that incorrect, incomplete, or outdated personal data is not processed. An employer must take measures to ensure the security and confidentiality of personal data. However, it should be noted that it is permitted to process personal information without prior consent of the relevant persons in an unstructured form, for example when referred to in a text.

Transfer of Personal Data

Compliance Alternatives Sweden permits cross-border transfer of personal data in circumstances including where: 1) an employee provides unambiguous consent, 2) the transfer is necessary for the performance of a contract to which the employee is a party, 3) the transfer is made to a country with an adequate level of data protection (e.g., EU member states or European Economic Area countries), 4) the transfer is made using standard contractual clauses, or 5) the transfer is in compliance with the US/EU Safe Harbor principles.

Other Requirements None applicable.
Switzerland

The Constitution of Switzerland provides traditional privacy rights for all individuals and protects the personal data of individuals. The collection, processing, and transfer of personal data are regulated under the Federal Data Protection Act of 1992 (the "Act"). The Act applies to the public and private sectors. Switzerland's twenty-six cantons (states) have separate data protection laws and their own data protection commissioners. The Office of the Federal Data Protection Commissioner (the "DPC") enforces the Act and maintains the Register for Data Files. Provisions of the Civil Code and the Penal Code also provide privacy protection.

Collection and Processing of Personal Data

**Compliance Alternatives** Generally, under the Act, an employee's personal data may be processed if the processing does not unlawfully infringe the employee’s privacy. An infringement of privacy shall be unlawful unless it is justified by 1) the consent of the employee, 2) an overriding public or private interest, or 3) the law.

Under the Swiss Code of Obligations, the processing of data relating to an employee is limited to 1) data pertaining to the employee’s ability to perform his or her work and 2) data relating to the completion of employment contracts.

**Disclosure/ Registration** Generally, an employer must register its data processing activities with the DPC before processing sensitive data (e.g., racial or ethnic origin, political opinions, party affiliation, and religion), creating personal profiles, or communicating personal data to a third party.

An exception to the registration requirement exists in circumstances where processing is subject to a legal requirement and the employee is aware that the data is being processed.

**Other Requirements** Generally, an employee is entitled to know what data concerning him or her has been recorded in a personal data file. Upon request by the employee, an employer must provide 1) information on all data relating to the employee contained in the employee’s file and 2) the purpose and, if necessary, the legal basis for the processing, the categories of processed data, the individuals involved in the processing, and the individuals designated to receive the file.

An employer must ensure that personal data is correct. An employer must take measures to ensure the security and confidentiality of personal data.

Transfer of Personal Data

**Compliance Alternatives** Switzerland permits cross-border transfer of personal data in circumstances where the employee’s personal privacy is not seriously endangered and the data receives protection equivalent to that provided under Swiss law. The DPC recommends the use of standard contractual clauses to ensure that these conditions will be met.
In the absence of a legal obligation and where the employee has no knowledge of the transmission, the employer must notify the DPC before transferring files containing personal data abroad. Prior declaration is not necessary if the files are exported to a country with an equivalent regime of protection and provided that they are not to be re-exported to a country with no such equivalent regime and do not constitute sensitive personal data.

**Other Requirements** The European Union ("EU") and Switzerland consider that their respective legislation provides an adequate level of protection for personal data. Accordingly, cross-border data flows between Switzerland and the EU are presumed to be in compliance with the EU Data Protection Directive 95/46/EC and the Act.

**United Kingdom**

The United Kingdom ("UK"), as a member of the European Union ("EU"), was required to implement the EU Data Protection Directive 95/46/EC (the "Directive") into its national legislation. The Directive was implemented in the UK in March 2000 when the Data Protection Act 1998 (the "Act") came into force. There are two transitional periods: the first expired on October 24, 2001, and the second, which gives transitional relief to only a very limited category of personal data, expires on October 24, 2007. The processing of certain personal data does not become fully subject to the Act until the latter of these dates. The Office of the Information Commissioner (the "Information Commissioner") enforces the Act. In June 2005, the Information Commissioner published the Employment Practices Data Protection Code to assist employers in understanding and complying with the Act.

**Collection and Processing of Personal Data**

**Compliance Alternatives** "Processing" of personal data has a very wide definition and essentially covers most operations relating to the data, including its collection, storage and transfer. Processing is allowed where: 1) the employee consents; 2) it is necessary for the performance of, or entering into, a contract to which the employee is a party; 3) it is necessary to comply with a legal obligation to which the employer is subject, 4) it is necessary in order to protect the vital interests of the employee; 5) it is necessary for the administration of justice, the functions under any enactment, the Crown, the government, or public functions in the public interest; or 6) it is necessary for legitimate interests pursued by the employer, or third party recipients, unless it prejudices the rights and freedoms or legitimate interests of the employee. These conditions are subject always to the processing being "fair and lawful".

With respect to the collection and processing of sensitive data (e.g., racial or ethnic origin, political opinions, party affiliation, and religion), additional requirements apply.

**Disclosure/ Registration** An employer, as a “data controller”, is required to notify the Information Commissioner and register databases containing employees’ personal data. Details of the employer are entered into the Register of Data Controllers and made publicly available. The notification must include descriptions of the data, such as the types of data to be collected, the employees about whom the data
will be held and the purposes for which the data will be processed. The Information Commissioner must be notified of any changes or amendments to any entry in the Register of Data Controllers.

Other Requirements Personal data must: 1) be obtained for specified and lawful purposes; 2) not be processed in a manner incompatible with such purposes; 3) be adequate, relevant and not excessive in relation to the purpose for which they are processed; 4) not be kept for longer than is necessary for the purpose; and 4) be kept accurate and up-to-date.

Appropriate technical and organizational measures must be taken against unauthorized or unlawful processing of, accidental loss or destruction of, or damage to, personal data.

Transfer of Personal Data

Compliance Alternatives The cross-border transfer of personal data outside of the European Economic Area (“EEA”) is prohibited unless that country ensures an “adequate level of protection” in relation to the processing of personal data. Derogations to this prohibition include where: 1) the employee consents to the transfer; 2) it is necessary for the employment contract; 3) it is necessary for the performance of a contract between the employer and a third party that is in the interest of the employee; 4) it is necessary on substantial public interest grounds; 5) it is necessary in connection with legal proceedings; 6) it is necessary to protect the vital interests of the employee; or 7) the data is from a public register.

To the extent that countries outside the EEA provide an adequate level of protection in relation to the processing of personal data, transfer of data is permitted. The UK has approved three sets of standard contractual clauses for cross-border data transfers and is a keen advocate of Binding Corporate Rules, pursuant to which employee consent is not required. Non-standard contracts and codes of conduct are also acceptable provided a sufficient finding of adequacy has been made in relation to the safeguards afforded to the personal data. For the transfer of data to the US, the UK will view compliance with the US/EU Safe Harbor principles as compliance with the cross-border transfer law in the UK.

Other Requirements If data will be subject to transfers outside the EEA, such information must be reflected in the notification to the Information Commissioner.
References


http://www.whitecase.com/hrhottopic_1207/

http://www.whitecase.com/hrhottopic_1107/

http://www.whitecase.com/articles-11112011/

http://www.whitecase.com/presentations/dataprivacy/