

A Regional Guide to Employee Data Privacy

EMEA

Introduction

Data privacy is a priority for all employers but especially those with operations in more than one country. It impacts all aspects of the employment relationship and, with the increase in data transfers between businesses and across borders, employers often need to comply with multiple laws to minimize the risk of significant fines and liabilities.

A Regional Guide to Employee Data Privacy is designed to help employers navigate the specific, and increasing, challenges of handling employee data in different jurisdictions. Covering 24 key countries, the guide contains the following:

- **Key Questions & Answers** – covering applicant and employee personal data, privacy statements and policies, retention periods for employee data, transfers of employee data overseas and to third parties, sanctions for breach and potential pitfalls for employers;
- **GDPR Overview** – highlighting the major changes and requirements introduced by the new European General Data Protection Regulation (“GDPR”), affecting businesses both within and outside the European Union; and
- **“In Brief” and “In Detail” Guidance** – providing both quick reference and more detailed content across all jurisdictions.

We hope that you will find this publication useful. It has been compiled by lawyers from a major international law firm as well as partner law firms in other jurisdictions.

USER GUIDE 



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 

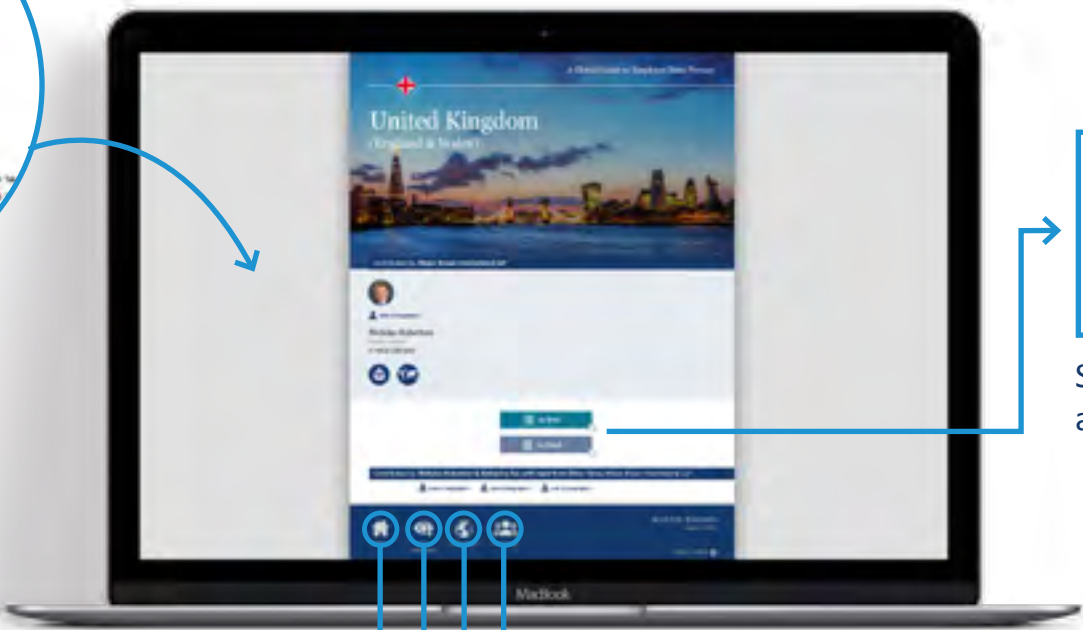
User Guide



Contents

Select a country

- Albania
- Andorra
- Austria
- Belgium
- Bulgaria
- Croatia
- Cyprus
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Ireland
- Italy
- Latvia
- Lithuania
- Malta
- Netherlands
- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Spain
- Sweden
- Switzerland
- Turkey
- United Kingdom
- United States



United Kingdom
(Kingdom of Great Britain)

Click to return to introduction

Click for overview of the European General Data Protection Regulation ("GDPR")

Click to select another country

Click to browse the directory of contacts



In Brief

In Detail

Switch between "In Brief" and "In Detail" guidance

GDPR Overview

The new European General Data Protection Regulation¹ (“**GDPR**”) came into force throughout the European Union (“**EU**”) on May 25, 2018. Unlike previous European data protection legislation, the GDPR does not require implementing national legislation, but is directly applicable. It introduces significant changes and additional requirements that will have a wide-ranging impact on employers both within and outside the EU.

Key Changes and Additional Requirements

- **European data protection law can now apply worldwide** – The GDPR covers not only the processing of personal data by an establishment of a controller or processor in the EU, regardless of whether the processing takes place in the EU, but also organizations outside of the EU insofar as their data processing activities are related either to offering goods or services to EU individuals, or to monitoring their behavior within the EU.
- **Tougher sanctions** – The maximum fine for a breach of the GDPR has been substantially increased to a maximum of 4% of an enterprise’s worldwide turnover, or EUR 20 million per infringement, whichever is higher.
- **A new data breach notification obligation** – Organizations now have to notify the relevant data protection authority of a breach without undue delay and where feasible within 72 hours. A notification must also be made to the individuals affected without undue delay where there is a high risk to their rights and freedoms.
- **New data privacy governance, record of processing activities and impact assessment requirements** – Many organizations now need to appoint a data protection officer to be responsible for implementing and monitoring that organization’s compliance with the GDPR and to carry out assessments of the organization’s data processing. Organizations are now also required to maintain a record of their processing activities and undertake data protection impact assessments for higher risk processing.
- **A requirement to implement “privacy by design” and “privacy by default”** – Businesses must now take a proactive approach to ensure that data protection is already integrated when technology is created and implemented, and that an appropriate standard of data protection is the default when personal data is being processed.

¹The full text of the GDPR is available [here](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN

GDPR Overview (continued)

- **Stronger rights for individuals** – Employees now have the following rights, and organizations will need to determine how they will enable their employees to exercise them:
 - **Access and information:** Employees can request a copy of the personal data their employers hold about them, and must be informed of, among other details, the purposes of processing, the categories of personal data concerned and the recipients to whom the data will be disclosed.
 - **Rectification:** Employees can request correction of any incomplete or inaccurate information.
 - **Erase (right to be forgotten):** Employees have the right to request deletion or removal of their personal data if they have been processed unlawfully, are no longer needed for their original or another lawful purpose, have to be erased for compliance with a legal obligation, or if the employee has withdrawn his/her consent or exercised his/her right to object to processing.
 - **Objection to processing:** If the employer relies on legitimate interests for processing, the employee can object to this processing on grounds relating to his/her particular situation.
 - **Restriction of processing:** Processing needs to be restricted if the employee contests the accuracy of the data, if the processing is unlawful or if the employer no longer requires the data for their original purpose, but the employee needs them for the establishment, exercise or defense of legal claims.
 - **Data portability:** Employees can request a copy of their personal data in a machine-readable format in order to transfer them to another recipient. Where technically feasible, the employer can also be required to carry out the transfer directly.
- **Enhanced requirements for the supply chain** – Businesses must only use other parties to process personal data that provide sufficient guarantees that they will implement appropriate security measures to satisfy the requirements of the GDPR. These service providers will now be held accountable for their own level of appropriate security, must document their processing to the same extent under the GDPR and must obtain prior consent to employ sub-processors. Existing contracts with third parties therefore need to be reviewed and are likely to require amending.
- **One-stop shop principle** – For organizations operating in more than one EU Member State, the GDPR implements a so-called one-stop shop principle. Such organizations will be able to liaise with one data protection authority (the “**lead authority**”). The lead authority is tasked with coordinating actions regarding the cross-border activities, thereby closely involving other authorities.



HOME

GDPR
OVERVIEW

COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN

GDPR Overview (continued)

In addition, particular areas of concern for employers are:

- **Processing and consent** – The GDPR enhances the requirements for a valid consent. It needs to be given freely, be specific, informed and unambiguous, and must take the form of an affirmative action or statement. In addition, data subjects have the right to refuse and to withdraw their consent at any time. In principle, consent can also be the legal basis for data processing in an employment situation. However, due to the imbalance of power between employer and employee, it may be questionable whether the consent was voluntary; often, employees will feel that they have no option but to consent.
- **Special categories of personal data** – Some special categories of personal data (“sensitive data”) are more closely protected. This is information that relates to someone’s race or ethnicity, political opinions, religious or philosophical beliefs, trade union membership, health, sex life and sexual orientation, and genetics/biometrics. In addition to the requirements described above, consent to the processing of these categories of data must be explicit, making it even more difficult for employers to rely on consent.
- **International transfers of data** – Cross-border data transfers may only take place if the transfer is made to an “adequate jurisdiction,” or if appropriate safeguards have been provided. Third countries (i.e., countries outside the European Economic Area (“**EEA**”)) can be determined “adequate” if the European Commission finds that they ensure an adequate level of data protection. Such an adequacy decision has, in particular, been adopted with regard to the EU-US Privacy Shield framework, thus allowing data transfers to US companies that have self-certified under the Privacy Shield. A transfer to countries lacking this status requires a lawful data transfer mechanism, such as standard contractual clauses adopted by the European Commission, or binding corporate rules that have been approved by the competent data protection authorities.

While many employers have taken steps to ensure compliance with the GDPR, it will have a continuing impact on businesses both within and outside the EU.

[HOME](#)[GDPR
OVERVIEW](#)[COUNTRIES](#)[DIRECTORY](#)

August 2018

SCROLL DOWN

Contents

Select a Country/Jurisdiction

 Belgium	 Iceland	 Saudi Arabia
 Czech Republic	 Ireland	 South Africa
 Denmark	 Israel	 Spain
 Egypt	 Italy	 Sweden
 France	 Netherlands	 Switzerland
 Germany	 Norway	 Turkey
 Greece	 Poland	 United Arab Emirates
 Hungary	 Russia	 United Kingdom





Belgium



Contributed by: **Van Olmen & Wynant**



In Brief



In Detail

Contributed by: **Nicolas Simon**, Van Olmen & Wynant



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Belgium

In Brief

1. Does employee data privacy law in your jurisdiction go beyond the GDPR?

Yes, but only on very specific subjects such as genetic data, biometric data or data concerning health.

2. Is there a law regulating applicant personal data?

Yes, Collective Bargaining Agreement no. 38, but it is less strict than the GDPR.

3. Is there a law regulating employee personal data?

In addition to the general provisions of the GDPR, there is a Privacy Act of July 30, 2018.

4. Do I need to have a privacy statement or agreement?

You need to prove that employees have been informed about their GDPR rights.

5. How long must I retain employee data? What is best practice?

Best practice is to determine the retention period based on each kind of data, keeping in mind that the limitation period for a contractual claim is generally five years from the end of the contract.

6. Can I transfer employee data overseas?

Yes, subject to the requirements of the GDPR.

7. Can I transfer employee data to a third party?

Yes, subject to the requirements of the GDPR.

8. What are the consequences of breach?

Administrative fines that can be imposed by the supervisory authority as foreseen by the GDPR (Article 83), or criminal fines that can be imposed by a court, ranging from EUR 800 to EUR 240,000.

9. What are the main pitfalls?

Employers may be unable to justify a dismissal due to their failure to comply with the GDPR.





Belgium

In Detail

1. To what extent does employee data privacy law in your jurisdiction go beyond the GDPR?

The Privacy Act of July 30, 2018 (“**Privacy Act**”) specifies the following elements regarding the GDPR:

- For the processing of genetic data, biometric data or data concerning health, it is necessary to comply with the following additional requirements, based on Article 9(4) of the GDPR:
 - o The categories of persons allowed to access the data must be designated, specifying their function regarding the processing of the concerned data;
 - o The list of the concerned categories of persons must be made available to the supervisory authority;
 - o The designated persons must be bound by a legal, administrative or contractual duty of confidentiality;
- Processing of personal data relating to criminal convictions and offenses, in accordance with Article 10 of the GDPR, is allowed:
 - o by legal or natural persons for the management of their own litigation;
 - o by lawyers or legal advisers for the defense of their clients;
 - o by other persons for substantial public interest reasons or tasks, assigned by law;
 - o for the necessity of scientific, historical or statistical research or for archiving purposes.

In this case, the categories of people accessing the data must be listed, with a description of their function, and the list must be made available to the supervisory authority. Moreover, the persons accessing the information are bound by a duty of confidentiality.

- When personal data are mentioned in a judicial decision, a judicial file or a judicial investigation of a criminal procedure, the rights based on the GDPR have to be exercised to comply with the judicial code, the code of criminal procedure and other legislation applicable to these specific procedures; and
- The Privacy Act provides for a prohibitory injunction procedure where data subject rights are not respected, as well as administrative and criminal fines.



HOME

GDPR
OVERVIEW

COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Belgium

In Detail

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant’s personal data in your jurisdiction?

The recruitment and selection of employees is regulated in Belgium by the Collective Bargaining Agreement no. 38, dated December 6, 1983 (“**CBA no. 38**”), applicable to the private sector. It foresees that all information regarding the applicant must be processed confidentially by the employer (Article 12, CBA no. 38).

Regarding background checks, their processing is mainly limited by the three anti-discrimination Acts. They prohibit any discrimination based on age, sexual orientation, marital status, birth, wealth, religious or philosophical conviction, political conviction, union conviction, language, current or future health status, disability, a physical or genetic characteristic, social origin, sex, nationality, race, skin color, pedigree and national or ethnic origin.

For other grounds, the GDPR rules apply. This means notably that the principles relating to processing of personal data under Chapter II of the GDPR must be respected (lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, accountability; Article 5 of the GDPR). Furthermore, the applicant must be informed of (a) the identity and contact details of the controller, (b) the contact details of the data protection officer, (c) the purposes and legal basis of the processing, (d) the possible legitimate interests pursued by the controller or a third party, (e) the recipients of the personal data, (f) the possible transfer to a third country or organization and the applicable safeguards, (g) the retention period of the data, (h) the existence of the rights of access, rectification, erasure, restriction of or objection to processing and the right of data portability, (i) the right to withdraw consent at any time, (j) the right to lodge a complaint with a supervisory authority, (k) whether the provision of personal data is a statutory or contractual requirement, and the possible obligation to provide the data and the consequences of failure to provide the data and (l) the existence of automated decision-making, including profiling, and its consequences (Article 13 of the GDPR).

Regarding the transfer of applicant data abroad, the GDPR rules also apply (chapter V of the GDPR). This means that there is no problem in the case of transfer between the countries of the EEA, or the countries which the EU Commission has decided provide an adequate level of protection. For other countries, appropriate safeguards must be in place (please see question 6).





Belgium

In Detail

3. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee's personal data in your jurisdiction?

In general, the GDPR applies (please see summary of key provisions in question 2), with the provisions mentioned under question 1 regarding the Privacy Act implementing the GDPR in Belgium.

The protection of employee privacy regarding the control of electronic online communication data is regulated by the CBA no. 81, dated April 26, 2002 ("**CBA no. 81**"), applicable to the private sector. It contains a purpose principle, meaning that the control has to aim for (a) the prevention of illegal or defamatory facts, (b) the protection of confidential, economical or financial interests of the company, (c) the security and good working of the computer system of the company or the technical installations of the company and (d) respecting the good faith of the principles and rules of use of the networked technologies of the company (Article 5, CBA no. 81). The second principle is the one of proportionality, meaning that interference in the privacy of the employee must be limited to a minimum (Article 6, CBA no. 81). Furthermore, information on the control system has to be provided to the works council and each employee (Article 7 and 8, CBA no. 81). Finally, direct individualization of the data (allowing the identification of the concerned employee) is only possible for the purposes under (a) to (c) above. An indirect individualization (i.e., an individualization in two steps: first, providing information to all employees that there is a problem and, secondly, individualization to the concerned employee if the problem reoccurs) applies for the purpose under (d). For instance, if the employer finds that too much data have been downloaded in comparison with the needs of the business, it will inform all the employees that there is a problem with the data downloaded and that it will seek the original source of the problem if the excessive downloading does not cease.

The protection of employee privacy in relation to video surveillance is regulated by the CBA no. 68, dated June 16, 1998, applicable to the private sector. It contains finality and proportionality principles. Video surveillance is only allowed to ensure (a) security and safety, (b) protection of the goods of the company, (c) control of the production process, i.e., machines and employees, and (d) control of the work done by the employees. Decisions and appraisals may not be based solely on data collected by video surveillance. The works council must be informed before video surveillance is implemented. Furthermore, the works council must be consulted if video surveillance has an impact on the privacy of at least one employee, so it can consider how to minimize interference with the employees' privacy.





Belgium

In Detail

4. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee's personal data?

An employer must ensure that employees are informed about their rights as data subjects, as required by Articles 12 and 13 of the GDPR (please see question 2). This can take the form of a privacy policy or an addendum to the works rules or to the individual employment contract.

Furthermore, an employer is required to have a data register (i.e., a record of processing activities as required under Article 30 of the GDPR).

5. For how long must an employer retain an employee's personal data? What is best practice?

Generally, the GDPR requires that personal data should be kept for no longer than necessary for the purpose for which the personal data are processed.

The retention period must comply with Article 13(2)(a) of the GDPR. This requires the data subject to be informed of the period for which the personal data will be stored or, if that is not possible, the criteria used to determine that period.

Best practice is for employers to determine how long data has to be retained on the basis of objective criteria. For example, job applicant data must not be retained for as long as employee data. For employees, data on which a dismissal is based, or data related to remuneration, have to be kept for at least five years after the end of the employment contract, as this is the limitation period for a claim based on the employment contract. Appraisals relating to a specific function must not be kept for longer than necessary for the appraisal of this specific function, e.g., after the employee moves to another function. Data that will be taken into account for the calculation of employees' pensions should be kept for a longer period (i.e., 10 years after the last payment of the employee's pension).

6. What are the legal restrictions on transferring employees' personal data outside your jurisdiction?

The restrictions on transferring data outside Belgium are set out in Chapter V of the GDPR. In brief, there is no problem transferring data between countries of the EEA or countries considered to be safe by the EU Commission. For other countries, appropriate safeguards must be in place, such as standard data protection clauses as validated by the EU Commission or a supervisory authority, approved mechanisms of certification, corporate binding rules or other mechanisms (Articles 44-47 of the GDPR).



HOME

GDPR
OVERVIEW

COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Belgium

In Detail

7. What are the legal restrictions on transferring employees' personal data to a third party?

If the employer transfers employee data to a third party to process on its behalf, the employer has to ensure that the third party processor provides sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR and protect the rights of the data subject (Article 28 of the GDPR).

This means that the employer has to conclude a binding written contract (or equivalent) with the processor stipulating in particular that the processor: (a) processes the personal data only on documented instructions from the employer, (b) ensures the confidentiality duty of the persons authorized to process the personal data, (c) takes all necessary measures to ensure an appropriate level of security for the processing, (d) respects the conditions of sufficient guarantees and liabilities if it engages another processor, (e) assists the employer for the fulfillment of the employer's obligation to respond to requests for exercising the data subject's rights, (f) assists the employer in ensuring compliance with the obligations of security of personal data and data protection impact assessment and prior consultation, (g) at the choice of the employer, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and (h) makes available to the employer all information necessary to demonstrate compliance with the obligations under the GDPR.

8. What are the consequences of breaching privacy laws in your jurisdiction?

Depending on the nature of the breach, there are substantial fines for non-compliance with the GDPR:

- (a) Up to EUR 10 million or, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher; and
- (b) Up to EUR 20 million or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

The Privacy Act provides for a prohibitory injunction before the civil court of first instance in the case of a breach of the obligations under the GDPR and the Privacy Act.

The classical damages in the case of civil liability also apply, which means proving a causal relationship between the fault and the damage. Belgian law does not recognize punitive damages. Therefore, the employee has to prove the real damage he/she has suffered.





Belgium

In Detail

Finally, the Privacy Act provides for criminal fines that can be imposed by a court, from EUR 800 to EUR 240,000, depending on the type of infringement of the GDPR or of the Privacy Act. These criminal fines are in addition to the administrative fines foreseen by the GDPR, provided that the same infringement cannot be sanctioned twice, i.e., by an administrative fine and by a criminal fine. Therefore, most of the time, the infringement will be sanctioned by an administrative fine imposed by the supervisory authority. If a court finds that there has been an infringement of the GDPR or the Privacy Act that has not yet been sanctioned by an administrative fine, the court will impose a criminal fine as foreseen in the Privacy Act.

9. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee's personal data?

The employer must ensure that it can prove that the employee is properly informed about his/her rights under the GDPR. Best practice is to ask the employee to sign for receipt of the document mentioning his/her rights.

For each type of data, it is important to specify the retention period (using the data register is helpful).

Finally, employers must be aware that it may be difficult to use data not collected in compliance with the GDPR to justify actions taken in relation to employees. This is particularly the case when employers have to prove the reasons for dismissing employees.

Contributed by: **Nicolas Simon**, Van Olmen & Wynant



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Czech Republic



Contributed by: **Havel & Partners**



In Brief



In Detail

Contributed by: **Petra Sochorová & Richard Otevřel**, Havel & Partners



[Link to biography >](#)



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Czech Republic

In Brief

1. Does employee data privacy law in your jurisdiction go beyond the GDPR?

Yes.

2. Is there a law regulating applicant personal data?

Yes. In addition to the GDPR, the Czech Labor Code and the Act on Employment (Act No. 435/2004 Coll.) apply.

3. Is there a law regulating employee personal data?

Yes, as above.

4. Do I need to have a privacy statement or agreement?

It is highly recommended to have at least one policy in place (in light of the information obligation under the GDPR).

5. How long must I retain employee data? What is best practice?

There are different regulations requiring data retention for different periods of time.

6. Can I transfer employee data overseas?

Yes, subject to the requirements of the GDPR.

7. Can I transfer employee data to a third party?

Transfers to third parties are allowed only in limited circumstances.

8. What are the consequences of breach?

A breach of the GDPR could lead to significant penalties. There may also be civil liability and, in serious cases, criminal liability.

9. What are the main pitfalls?

Issues may arise in connection with the transfer of data overseas or to third parties.

Other issues may occur in connection with the lack of provision of appropriate safeguards, the implementation of privacy policies and/or the inappropriate or excessive collection of personal data.





Czech Republic

In Detail

1. To what extent does employee data privacy law in your jurisdiction go beyond the GDPR?

Under the Czech Labor Code (Act No. 262/2006 Coll.), the employer is generally not allowed to ask for and process information on pregnancy, family and property situations, sexual orientation, origin, trade union membership, membership of political parties, membership of the Church or religious communities and criminal history. Exceptions may apply to information about pregnancy, family and property situations and criminal history depending on the nature of the work to be performed, when the requirement for provision of the information is appropriate or when such a requirement is stated in another Act. This restriction is an example of legislation anticipated by Article 9(2)(a) of the GDPR (i.e., when the prohibition on processing special categories of data may not be lifted by the employee's consent).

A similar restriction is set out in the Act on Employment (Act No. 435/2004 Coll.), which prevents employers from requesting (and thus processing) information from the applicant on his/her nationality, race or ethnic origin, political opinions, trade union membership, religion or philosophical belief, sexual orientation, and other such information in certain circumstances. Employers are obliged to prove the need for the required personal data on request from the applicant/employee.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant's personal data in your jurisdiction?

Please see response to question 1. Generally, employers may not require or process information that is not necessary for the fulfillment of the employment contract, the requirements set out for employers in legal regulations and/or if it is restricted information that does not relate to the work performed.

Once applicant data are collected in accordance with laws, they might be transferred overseas and/or to a third party under the same conditions as any data legally obtained. For further details, please see response to question 6 below.

3. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee's personal data in your jurisdiction?

Please see responses to questions 1 and 2 above. In addition to the GDPR, the Labor Code and Act on Employment apply.





Czech Republic

In Detail

4. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee's personal data?

Labor law states that employers must prove they have informed employees that their personal data will be collected and processed. There is no rule specifically stating that employers are obliged to issue a privacy policy or personal information collection statement, but due to the above requirement and the information obligation under the GDPR, all of the mentioned forms of informing employees about the handling of their personal data are highly recommended.

5. For how long must an employer retain an employee's personal data? What is best practice?

Generally, the GDPR requires that any personal data must be stored and kept only for the period that is necessary for the purpose of personal data processing. As a result, it is important to distinguish between what data are relevant and necessary only in the course of the employment relationship and what data may be stored after the termination of employment.

In relation to the personal data stored after termination of employment, the following specific retention periods apply under Czech law:

- Five years beginning from the end of the fiscal year to which the documents relate: accounting documents and records (except for the documents with longer retention periods as stated below);
- 10 calendar years after the year to which the documents relate: payroll or accounting records containing data necessary for the purposes of pension insurance concerning persons who are beneficiaries under a retirement pension scheme;
- 10 years after the date of execution: record on work attendance;
- 30 calendar years after the year to which the documents relate: payroll sheets of accounting records containing data necessary for the purpose of pension insurance; and
- 30 years after the date of issue: reports on work injuries, etc.





Czech Republic

In Detail

6. What are the legal restrictions on transferring employees' personal data outside your jurisdiction?

There are no specific rules under the labor law; therefore, the GDPR rules on general transfers of personal data apply.

In particular, an adequate level of protection is required. This will not present any problem for countries in the EU/EEA. For other countries, if the European Commission has not already decided that they provide an adequate level of protection, appropriate safeguards must be in place. These include binding corporate rules, standard data protection clauses, approved certification mechanisms or other mechanisms. In the absence of these safeguards, data transfers may still take place in specific situations (e.g., where the data subject has explicitly consented after being informed of the possible risks).

7. What are the legal restrictions on transferring employees' personal data to a third party?

Any transfer to a third party must be based on one of the legal bases in Article 6 of the GDPR.

If employee data will be shared with a processor (e.g., a payroll provider), a data processing agreement should be entered into (Article 28 of the GDPR).

8. What are the consequences of breaching privacy laws in your jurisdiction?

A breach of the GDPR could lead to penalties of up to EUR 20 million, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

These penalties may be imposed by the Office for Personal Data Protection and it may initiate the proceedings either on the basis of the complaint or of its own volition (for example, based on a finding in a random inspection) and, in addition to the penalties, blocking or liquidation of personal data may be required.

As well as the Office for Personal Data Protection, the State Labor Inspection Office may, in accordance with the Act on Inspection (Act No. 251/2005 Coll.), also impose a penalty of up to CZK 1 million (for example, for interfering in the employee's privacy in the workplace or for requiring information that is prohibited (please see response to question 1)). The State Labor Inspection Office may initiate proceedings in the same way as the Office for Personal Data Protection as described above.



HOME

GDPR
OVERVIEW

COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Czech Republic

In Detail

Moreover, the Penal Code (Act No. 40/2009 Coll.) recognizes several crimes related to a breach of the Act on Employment: the criminal offense of unlawful dealing with personal data either collected in the course of public service operation or violating the confidentiality provided for in the laws or regulation and the criminal offense of willful damage or misuse of information kept in secrecy and violations of this secrecy. The punishment may be up to eight years' imprisonment, a financial penalty or prohibition from conducting business, depending on the severity of the offense.

Finally, the employee may seek civil liability claims for violation of his/her right to human dignity, personal honor, good reputation or name, equal treatment and non-discrimination.

9. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee's personal data?

Multinational companies often need to address the situation when a unified model of data collection and processing is to be applied to employees in the Czech Republic. Usually, the employee personal data processing would not pose any major legal issues, but these unified models frequently require collection of inappropriate (restricted) categories of data; therefore, the set of personal data collected by the employer should always be localized.

Another issue connected with multinationals relates to central databases and access to these databases being granted to managers from different branches of the holding structures (e.g., the parent company). Unless properly substantiated and/or based on the specific holding structure and, for example, the manager's authorizations, such free circulation of the employees' personal data within the holding structure would not be permitted without the existence of a legitimate interest of the controller (employer) or another recognized ground of lawfulness of processing. However, taking into account Recital 48 of the GDPR, such transfers for administrative purposes within the group of companies should now be possible, but this has not been tested in practice and the term "internal administrative purposes" could be subject to clarification in the future.

Finally, implementing an appropriate privacy policy in a growing company is often overlooked. What suffices for a small company with a few employees would often be found inadequate for larger companies with hundreds of employees and its IT systems processing the employees' personal data, but the standards of protection of privacy of individuals obviously remain the same.

Contributed by: **Petra Sochorová & Richard Otevřel**, Havel & Partners



[Link to biography >](#)



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Denmark



Contributed by: **Kromann Reumert**



In Brief



In Detail

Contributed by: **Tina Brøgger Sørensen**, Kromann Reumert



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Denmark

In Brief

1. Does employee data privacy law in your jurisdiction go beyond the GDPR?

Yes, the Danish Data Protection Act (“**DPA**”) includes certain provisions on processing employee data that go beyond the GDPR, e.g., the DPA includes a provision under which the employer can process employee data based on the employee’s consent, if it is necessary to fulfill employment law obligations, or if such processing is necessary for the purposes of the legitimate interests of the employer or a third party. In addition, the employer can process the employee’s social security number (*CPR-nummer*) subject to certain requirements.

Further, the DPA also includes a provision that limits the data subject’s rights under Articles 13, 14 and 15 of the GDPR.

2. Is there a law regulating applicant personal data?

No specific Danish law regulates applicant personal data. Thus, the processing of applicant personal data is regulated by the GDPR and the DPA.

3. Is there a law regulating employee personal data?

No specific Danish law regulates employee personal data. The processing of employee personal data is regulated by the GDPR and the DPA.

4. Do I need to have a privacy statement or agreement?

Certain information must be provided in connection with the collection of personal data under Article 13 of the GDPR.

5. How long must I retain employee data? What is best practice?

There are no specific provisions that regulate the employee data retention period. Generally, employee personal data must not be kept in a form that makes it possible to identify the employee for a period that is longer than necessary for the legitimate purposes for which the data are processed.

6. Can I transfer employee data overseas?

Yes, subject to the requirements under the GDPR.

7. Can I transfer employee data to a third party?

Yes, subject to the requirements under the GDPR.

8. What are the consequences of breach?

- Complaint by an employee to the Danish Data Protection Agency (“**the Agency**”);
- Investigation by the Agency;
- Formal criticism by the Agency;
- Enforcement notice issued by the Agency;
- Fines and imprisonment; and
- Compensation claim from the data subject.

9. What are the main pitfalls?

- Long retention periods without a legitimate ground;
- Inappropriate legal basis for processing personal data;
- Where consent is used as the legal basis for processing personal data, non-compliance with the mandatory requirements to ensure valid consent; and
- Disclosure of personal data within a group of companies is considered as internal processing instead of disclosure subject to the requirements under the GDPR.





Denmark

In Detail

1. To what extent does employee data privacy law in your jurisdiction go beyond the GDPR?

In Denmark, the Danish Data Protection Act (“**DPA**”) supplements the GDPR and includes certain provisions on processing employee data that go beyond the GDPR.

Please note that the provisions mentioned below are supplements to the legal basis for processing personal data under Articles 6 and 9 of the GDPR.

The employer’s processing of employee personal data

Section 12 of the DPA includes a provision that regulates the employer’s processing of employee personal data under certain circumstances. Under section 12(3) of the DPA, the employer can process employee personal data based on the employee’s consent in accordance with the requirements under Article 7 of the GDPR.

Further, section 12(1) explicitly states that the employer may process employee personal data subject to Article 6(1) and 9(1) of the GDPR, if such processing is necessary for the employer’s and/or the employee’s compliance with legal employment obligations to which the employer and/or the employee is subject, or to which the employer and/or the employee is subject under other provisions and/or collective bargaining agreements.

Finally, section 12(2) explicitly states that the employer may process employee personal data as stated in section 12(1), if such processing is necessary for the purposes of the legitimate interests pursued by the employer or by a third party, and such interests follow from other provisions and/or collective bargaining agreements to which the employer or a third party is subject, except where such interests are overridden by the interests or fundamental rights and freedoms of the employee.

With this said, the employer’s processing of employee personal data may also take place under the general provisions of Articles 6(1) and 9(1) of the GDPR (cf. sections 5 and 7 of the DPA).

The employer’s processing of the employee’s social security number

Under section 11(2) of the DPA, the employer can process the employee’s social security number based on the employee’s consent in accordance with the requirements under Article 7 of the GDPR, or when such processing is required by law. Further, the employer may process the employee’s social security number in accordance with the legal basis stated in Article 9 of the GDPR.





Denmark

In Detail

The employer may disclose the employee’s social security number when such disclosure is a natural element of the employer’s ordinary operations and the disclosure is of decisive importance for an unambiguous identification of the employee (for example, when disclosing the social security number to the employer’s or employee’s insurance company, bank, pension fund, etc.).

Specific limitations on the data subject’s rights

The data subject’s rights under Articles 13(1)-(3), 14(1)-(4) and 15 of the GDPR (relating to information to be provided to data subjects and their access to personal data) do not apply if the data subject’s interest in obtaining the information is found to be overridden by the essential considerations of private interests, including the interests of the data subject her/himself.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant’s personal data in your jurisdiction?

No specific law/Code or similar document regulates applicant personal data. The processing of applicants’ personal data is therefore regulated by the GDPR and the DPA. Whenever personal data are being processed, the fundamental principles under the GDPR must be observed, regardless of the type of data processed.

The employer may only collect, use, handle and/or request an applicant’s personal data that is *relevant* in order for the employer to assess whether the applicant is qualified for the job. In relation to the employer’s right to request any health information from the applicant, please see response to question 3 below.

3. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee’s personal data in your jurisdiction?

No specific law/Code or similar document regulates the processing of employee personal data. The processing of employee personal data is therefore regulated by the GDPR and the DPA. Whenever employee personal data are being processed, the fundamental principles under the GDPR must be observed, regardless of the type of data processed.

Special rules on employee/applicant health information

Certain restrictions may apply in connection with the employer’s processing of employee health data. The employer’s collection and use of health information is governed by the Danish Health Information Act (“**DHIA**”). The purpose of the





Denmark

In Detail

DHIA is to ensure that there is no unauthorized use of health information that would limit employees' possibilities of obtaining or retaining employment.

The underlying principle of the DHIA is that, although employers are entitled to select the best qualified person for the job, health information may only be used in the selection process if it can be established that such information is of relevance to the person's ability to perform the job. In other words, employers are generally not allowed to ask applicants health-related questions before employment. This prohibition applies to illness as well as to absence due to illness.

Under the DHIA, employers may request health information *before* and *during* an employee's employment only for the purpose of discovering whether the employee suffers from or has suffered from an illness, or has or has had symptoms of an illness that will materially affect the employee's fitness for work. Thus, the illness must have progressed, so that clinically the employee is no longer only susceptible to the illness.

Also, an employer may only ask about specific illnesses materially affecting the employee's fitness for work. For instance, an employer may not ask if a job applicant suffers from epilepsy unless this would materially affect the specific job, as in the case of drivers.

Employers may not ask general questions about an applicant's health, but only questions about specific functional limitations affecting the applicant's ability to perform the work. The key factor is whether the illness makes the person unable to perform the job. An employer may not, for instance, ask if an employee suffers from a successfully treated illness that does not make the employee unfit for work.

4. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee's personal data?

There is no legal requirement under the GDPR or the DPA for an employer to provide any particular form of document to an employee before the collection of personal data from an individual. However, the employer is bound by the obligation to provide information on the collection/processing of the personal data under Article 13 of the GDPR, which is typically set out in a general employee handbook or IT/HR privacy policy.





Denmark

In Detail

5. For how long must an employer retain an employee’s personal data? What is best practice?

Generally, under the GDPR, employee personal data may not be kept in a form that makes it possible to identify the employee for a period that is longer than necessary for the purposes for which the data are processed.

Applicant personal data may typically be stored for six months after collection for documentation purposes without consent from the applicant. If the purpose of the retention is future recruitment, longer retention (for example, two years) can be used, but the applicant must specifically consent to this.

Personal data regarding employees may typically be retained during employment and for five years after termination of the employment, which is also considered best practice. Please note that the employer must, in any event, on an ongoing basis assess whether it is still necessary to retain the collected personal data. If it is not, the personal data must be deleted.

In cases where retention for a longer period is required for the fulfillment of a legitimate purpose, for example, during an ongoing dispute or in order to comply with the employers’ statutory duties, applicant/employee personal data may be retained for longer than the above-mentioned periods.

6. What are the legal restrictions on transferring employees’ personal data outside your jurisdiction?

The transfer of employees’ personal data outside of Denmark is subject to the requirements under the GDPR, as no specific local rules regulate this matter.

An adequate level of data protection is required in the relevant country – this will not be an issue for EU/EEA countries. For other countries, standard data protection clauses, corporate binding rules or other mechanisms will be required to provide appropriate safeguards.

7. What are the legal restrictions on transferring employees’ personal data to a third party?

The transfer of employees’ personal data to a third party is subject to the requirements under the GDPR as no specific Danish rules regulate this matter.





Denmark

In Detail

Accordingly, the transfer of employees' personal data to a processor must be regulated in a written contract between the controller and the third party (Article 28 of the GDPR). This obligation must also be observed when third parties host or provide other services in relation to the operation of the systems on which employee personal data are processed.

If a disclosure to a third party takes place for the third party's own purposes (e.g., as a controller), there must be a legal basis for the disclosure, either in accordance with the rules of the GDPR or the DPA.

8. What are the consequences of breaching privacy laws in your jurisdiction?

Data subject may make a complaint

A disgruntled employee may make a complaint to the Danish Data Protection Agency ("**the Agency**").

Investigation by the Agency

The Agency may carry out a formal investigation. There is no obligation on it to follow a certain mediation process. If the investigation confirms a contravention of the DPA, the Agency may serve an enforcement notice that will set out steps that need to be taken.

Criticism by the Agency

If the employer is found to have violated the DPA, the Agency may choose to issue formal criticism against the processing involved with or without taking further measures. The criticism is usually published on the Agency's website.

Enforcement notice

The Agency may investigate any allegations of contravention of the DPA and serve an enforcement notice on the employer prescribing, among other things, remedial action to be taken by the employer.

Fines and imprisonment

In addition to the potential penalties under the GDPR (depending on the infringement, up to EUR 20 million or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher), the employer may also be liable to pay a fine under the DPA. Further, the sanction can be imprisonment of up to six months for any individual responsible for the breach (or longer according to Danish Penal Code, if applicable).





Denmark

In Detail

Employee compensation

In addition to the above, any data subject who suffers damage (including injury to feelings) by reason of a contravention of any requirement under the DPA may claim compensation from the employer for the damage.

9. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee’s personal data?

Long retention periods without a legitimate ground

Whereas most Danish employers under the former regulation have been aware of the general principles for processing personal data, few employers have been aware of the obligation to delete employee personal data when such data are no longer necessary. As a consequence of the major press coverage of the GDPR, more employers are aware of the obligation to delete personal data and more employers in general are expected to comply with the obligations under the GDPR, including deletion.

Inappropriate legal basis for processing personal data

It is our experience that many Danish employers have made use of an inappropriate legal basis for processing personal data. For instance, the employer chooses to obtain the employee’s consent even though the legal basis for processing the employee’s personal data is the employer’s legitimate interest. In this case, the employer uses unnecessary resources to obtain the employee’s consent and risks withdrawal of consent in situations where the processing cannot be ceased.

Where consent is used as legal basis for processing personal data, non-compliance with the mandatory requirements to ensure valid consent

Further, it is our experience that the Danish employers that choose to obtain the employees’ consent do not always do so in accordance with the (former) requirements. Mostly, the consent is not given in accordance with the requirements to be specific and informed, or, for instance, is implicitly given in the employment contract, and is too broad, and/or not comprehensive, etc. which is not in compliance with the (former) requirements. With this said, it is our impression that more employers are aware of the consent requirements under the GDPR and that the employers will strive to be compliant.





Denmark

In Detail

Disclosure of personal data within the group of companies

Finally, there are Danish employers that are not aware that transfer of employee personal data within the group is considered to be a disclosure of personal data to a third party rather than internal processing. Such disclosure is subject to the requirements of the GDPR.

Contributed by: **Tina Brøgger Sørensen**, Kromann Reumert

 [Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Egypt



Contributed by: **Shalakany Law Office**



In Brief



In Detail

Contributed by: **Sharif Shihata**, Shalakany Law Office



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Egypt

In Brief

1. Is there a law regulating applicant personal data?

No.

2. Is there a law regulating employee personal data?

Yes, Egyptian Labor Law No. 12 for 2003.

3. Do I need to have a privacy statement or agreement?

No.

4. How long must I retain employee data? What is best practice?

By law, one year from the date the employment contract terminates or expires.

5. Can I transfer employee data overseas?

Yes, to related companies.

6. Can I transfer employee data to a third party?

Except for those legally authorized to do so, an employer may not transfer an employee’s data to a third party.

7. What are the consequences of breach?

The employer will be liable to pay a fine.

8. What are the main pitfalls?

Employers failing to maintain employee files.





Egypt

In Detail

1. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant’s personal data in your jurisdiction?

No.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee’s personal data in your jurisdiction?

The Egyptian Labor Law No. 12 for 2003 (“**Labor Law**”), which governs nearly all employees working in Egypt regardless of their nationality, addresses in a few articles privacy restrictions and collection of employees’ personal data.

Pursuant to Article 77 of the Labor Law, an employer must keep a file for each employee that includes personal and private information, such as an employee’s name, address, job, skill level, marital status, date of hiring, salary, job development (appraisals), disciplinary sanctions, vacation dates, date of end of service and reason for termination of employment.

3. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee’s personal data?

There is no legal requirement to have a privacy statement or agreement.

4. For how long must an employer retain an employee’s personal data? What is best practice?

Pursuant to Article 77 of the Labor Law, an employer must retain an employee’s file for at least one year from the date the employment contract terminates or expires.

5. What are the legal restrictions on transferring employees’ personal data outside your jurisdiction?

Employers are prohibited from allowing access to employees’ personal data. The employer may not allow anyone to review the employee’s files except for those legally authorized to do so. Persons who are legally authorized to review employee files include governmental authorities, courts, employees in the employer’s human resources department, and the employer’s subsidiaries and affiliates (whether in Egypt or abroad).





Egypt

In Detail

It should be noted that the employer may obtain the employee’s approval to pass his/her data to related companies or third parties. In practice, nearly all employment contracts in Egypt include a clause stating that the employer is entitled to transfer the employee’s personal data to its subsidiaries and affiliates, whether in Egypt or abroad.

6. What are the legal restrictions on transferring employees’ personal data to a third party?

Please see response to question 5 above.

7. What are the consequences of breaching privacy laws in your jurisdiction?

Pursuant to Article 249 of the Labor Law, if an employer fails to comply with the obligations under Article 77 of the Labor Law, it will be liable to pay a fine of not less than EGP 100 and not exceeding EGP 200 per employee. It should be noted that this does not prevent the employee from filing a civil case against the employer.

8. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee’s personal data?

The main pitfall is employers not maintaining employees’ files as required by the Labor Law.

Contributed by: **Sharif Shihata**, Shalakany Law Office



France



Contributed by: **Mayer Brown**



In Brief



In Detail

Contributed by: **Julien Haure & Régine Goury**, Mayer Brown



[Link to biography >](#)



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



France

In Brief

1. Does employee data privacy law in your jurisdiction go beyond the GDPR?

Yes. The French Data Privacy Law dated June 20, 2018 has updated, in accordance with the GDPR provisions, the previous French Data Privacy Law dated January 6, 1978 and goes beyond the GDPR on specific matters, including biometric data, territorial scope and the ability to suspend the transfer of personal data to third countries.

2. Is there a law regulating applicant personal data?

The regulation of applicant personal data is governed by Articles L. 1221-6 to L. 1221-9 of the French Labor Code, non-discrimination laws, the GDPR and French data privacy provisions.

3. Is there a law regulating employee personal data?

Yes. In addition to the general provisions of the GDPR, the French Data Privacy Law dated June 20, 2018 also applies to employee data.

4. Do I need to have a privacy statement or agreement?

The employment relationship itself justifies the collection and processing of personal data without any need for a prior statement or agreement. However, the Social and Economic Committee (“SEC”) (i.e., the new version of the works council) may have to be consulted in advance and the employees should be formally informed, notably when the processing aims at monitoring their activity.

Under the GDPR, employees must be provided with specific information about the personal data being collected from them.

5. How long must I retain employee data? What is best practice?

This depends on the type of personal data. Some personal data should be deleted fairly promptly, whereas other personal data may be retained even beyond the end of the employment relationship.

6. Can I transfer employee data overseas?

Yes, in accordance with the general rules under the GDPR.

7. Can I transfer employee data to a third party?

Yes, in accordance with the general rules under the GDPR.

8. What are the consequences of breach?

A breach can lead to criminal, civil and administrative sanctions.

9. What are the main pitfalls?

Any information collected and used for employee monitoring purposes, without informing and consulting the SEC in advance and informing the employees in advance, could not lawfully form the basis of any sanction against the employee and/or be used as a valid evidence.





France

In Detail

1. To what extent does employee data privacy law in your jurisdiction go beyond the GDPR?

On June 20, 2018, the French Data Privacy Law (“**2018 French Data Privacy Law**”) updated the French Data Privacy Law of 1978 in accordance with the provisions of the GDPR, and has added some specific local provisions that go beyond the GDPR’s requirements. For example:

- Sensitive data: On top of the exceptions provided by the GDPR to process sensitive personal data, the 2018 French Data Privacy Law provides that biometric data may be processed by the employer for professional premises access control purposes or for the use of professional devices/applications.
- Territorial scope: French data privacy provisions are applicable to any individual residing in France, whatever the location of the processor.
- Transfers of personal data to third countries: The French data protection authority (the “**CNIL**”) is entitled to request from the Administrative Supreme Court the suspension of a transfer of personal data to third countries or international organizations (in order to protect the rights and freedoms of a person with regard to the processing of his/her personal data, notably in the case of a complaint from the individual).
- Right to lodge a complaint: Class actions are authorized before or against the CNIL.
- Supervisory authority’s powers: The CNIL has the right to access any premises of the controller and/or the processor from 6 a.m. to 9 p.m., excluding private residences.

It is expected that the 2018 French Data Privacy Law will be completed by some decrees and ordinances, which may contain additional local specific provisions.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant’s personal data in your jurisdiction?

Under French labor law, the applicant’s personal data collection, use and/or handling must comply with the general principles as set out in:

- Article L. 1221-6 of the French Labor Code, which limits the data that can be requested from the applicant to those enabling the employer to assess the applicant’s ability to perform the offered position and related professional skills;





France

In Detail

- Article L. 1221-8 of the French Labor Code, which requires the employer to inform the applicant of any means for selection processes;
- Article L. 1221-9 of the French Labor Code, which requires the employer to inform the applicant of any personal data collection;
- Article L. 1121-1 of the French Labor Code, which relates to the protection of civil rights within the company;
- Article L. 1132-1 of the French Labor Code, which prohibits discrimination during the recruitment process based on origin, sexual orientation, gender, habits (i.e., behaviors driven by customs/tradition), family situation, age, pregnancy, health, disability, family name, political opinion, DNA, physical appearance, belonging or not belonging to an ethnic group, a nation, a race, a religion or a trade union organization;
- The GDPR; and
- Data privacy law as updated by the 2018 French Data Privacy Law.

A CNIL recommendation (#02-017 dated March 21, 2002) specifies the information that it is lawful to collect during the recruitment process. To date, this recommendation remains in force even under the GDPR and the 2018 French Data Privacy Law.

In this respect, and unless justified by the specifics of the position to be filled, the examples of information/data listed below are likely to be considered irrelevant in the context of a recruitment and, as such, non-collectable:

- credit checks (e.g., payment failure, loans contracted, bank domiciliation, etc.);
- criminal background; and
- employment history (e.g., reasons for leaving).

Regarding the transfer of applicant personal data, the GDPR provisions apply in France (please see question 6 below). However, a specific procedure was introduced by the 2018 French Data Privacy Law under which the CNIL is entitled to request from the Administrative Supreme Court the suspension of transfers of personal data to third countries or international organizations.





France

In Detail

3. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee's personal data in your jurisdiction?

The processing of employee personal data falls within the scope of the 2018 French Data Privacy Law. The law incorporates the principles of the GDPR and redefines the tasks and powers of the CNIL (please see question 1).

4. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee's personal data?

There is no such legal requirement. Indeed, no data protection agreement requiring the employee's consent has to be signed as long as the processing of personal data is necessary for the hiring and/or the employment relationship.

However, employees must be informed by whatever means of the processing of their personal data. In accordance with Articles 13 and 14 of the GDPR, French law reiterates that, where personal data relating to a data subject (i.e., the employee) are collected, the employer has to provide him/her with all of the following information:

- the identity and the contact details of the controller;
- the contact details of the data protection officer ("DPO"), where applicable;
- the purposes of the processing for which the personal data are intended, as well as the legal basis for the processing;
- the legitimate interests pursued by the controller or by a third party;
- the recipients or categories of recipients of the personal data, if any;
- where applicable, the fact that the controller intends to transfer personal data to a third country or international organization;
- the period for which the personal data will be stored;
- the existence of the rights to access, rectify and/or erase personal data or to restrict the processing or to object to the processing, as well as the right to data portability;
- the existence of the right to withdraw consent at any time;





France

In Detail

- the right to complain to a supervisory authority;
- the existence of automated decision-making, including profiling; and
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.

In terms of best practice, the implementation of a charter is recommended in order to inform the employees of the data processing and their rights in this respect.

Article L 2312-38 of the French Labor Code requires a consultation of the staff representatives prior to the implementation or modification of certain automated processing. Staff representatives should also be informed of the appointment of a DPO.

5. For how long must an employer retain an employee's personal data? What is best practice?

In accordance with the provisions of the GDPR, the CNIL considers that personal data should be kept for no longer than is necessary for the purposes for which the personal data have been processed. Therefore, as long as the employee does not need to keep the data of its employees or former employees, the data should be erased.

Exceptions

Some employment documents containing employees' personal data have to be stored by the employer for a five-, three- and one-year period (notably in the event of labor authorities' audits and/or litigation with the employees), even following the termination of the employment contract:

- Five years
 - pay slips;
 - employment contracts and related amendments;
 - documents related to the retirement scheme;





France

In Detail

- dismissal letters;
 - employees’ working accidents records; and
 - final payments sheets.
- [Three years](#)
 - documents related to social contributions payment/declaration; and
 - time sheets for employees under working time arrangement in days per year.
 - [One year](#)
 - time sheets for employees working under working time arrangement in hours. However, in France, best practice requires employers to keep such information for a three-year period in case of a claim for unpaid overtime, for instance, which is subject to a three-year limitation period.

Regarding all other data, as per the GDPR, the employer may be allowed to archive them (but only for a defined and limited period of time, and ensuring the employee is aware of the relevant period).

The CNIL provides guidance on the various types of archival storage and distinguishes three main archives:

- (a) The active database (or current archive), which includes data that has just been processed or is likely to be processed in the near future;
- (b) The intermediate archive, which is an intermediate step requiring restricted access before deleting the data; and
- (c) The definitive archive, which is reserved for data that are likely to be kept for a while. This category can only contain data that need to be archived in the public interest, for scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organizational measures in order to safeguard the rights and freedoms of the data subject.





France

In Detail

6. What are the legal restrictions on transferring employees' personal data outside your jurisdiction?

The general rules under the GDPR apply. In particular, an adequate level of data protection is required in the country where the recipient is located. This will not present any problems in the EU and the EEA.

However, if the employer discloses employees' personal data to third countries where the level of protection is not similar to the one required by the GDPR, appropriate safeguards must be in place. These include binding corporate rules, standard data protection clauses, approved certification mechanisms or other mechanisms. In the absence of these safeguards, transfers may still be possible in specific situations (e.g., if the data subject has explicitly consented after being informed of the possible risks).

7. What are the legal restrictions on transferring employees' personal data to a third party?

Any transfer to a third party must be based on one of the legal bases of Article 6 of the GDPR.

If employees' personal data shall be shared with a processor (e.g., a payroll provider), it is important to enter into a proper data processing agreement that meets the requirements set forth in Article 28 of the GDPR.

8. What are the consequences of breaching privacy laws in your jurisdiction?

The CNIL has wide powers to investigate the employer's premises from 6 a.m. to 9 p.m. in order to ensure the proper application of personal data provisions (Art 44 of the 2018 French Data Privacy Law).

A breach of data privacy law can lead to civil, criminal and administrative sanctions:

- From a civil perspective: The affected employee can file an action for payment of damages. If several employees are involved, a class action is also possible.
- From an administrative perspective: Significant administrative penalties may be imposed on the employer. Under the GDPR, administrative fines may, depending on the infringement, amount to a maximum of EUR 20 million, or, if this is a higher amount, 4% of the company's worldwide annual turnover of the preceding financial year. Practically, there would be an undefined period of tolerance during which, before taking sanctions, the CNIL will first inform the employer of the need to comply with the regulations via a formal notice.





France

In Detail

- From a criminal perspective: Articles 226-16 to 226-22 of the French Criminal Code provide that the employer may be subject to three to five years' imprisonment and/or a fine of up to EUR 300,000 in the following situations: retention of data beyond the necessary retention limit, lack of precautions regarding the security of information with a risk of disclosure or distortion, use of fraudulent methods in the collection of data or failure to respect the legitimate opposition right of the employee, misappropriation of data, and/or illegal communication of data to a third party.

Moreover, it should be noted that the employer's failure to inform the Social and Economic Committee ("SEC") of the implementation of a data processing is a criminal offense, punishable by a maximum of EUR 7,500 for natural persons (i.e., the employer's legal representative) and EUR 37,500 for legal entities.

9. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee's personal data?

Personal data collected and used in order to monitor employees without informing and consulting the SEC and informing the employees in advance cannot be used as valid evidence before the labor court and/or lawfully form the basis of a sanction.

Therefore, if the employer monitors the employees (e.g., via access control cards, a video surveillance system, a monitoring system in the employees' computers, etc.) without first consulting the SEC and informing the employees, the employer could not sanction any failure/breach by the employee discovered via the monitoring system.

Contributed by: **Julien Haure & Régine Goury**, Mayer Brown



[Link to biography >](#)



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Germany



Contributed by: **Mayer Brown LLP**



In Brief



In Detail

Contributed by: **Dr. Guido Zeppenfeld, Björn Vollmuth & Vanessa Klesy, Mayer Brown LLP**



[Link to biography >](#)



[Link to biography >](#)



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Germany

In Brief

1. Does employee data privacy law in your jurisdiction go beyond the GDPR?

Yes.

2. Is there a law regulating applicant personal data?

Yes, in addition to the general provisions of the GDPR, section 26 of the Federal Data Protection Act (*Bundesdatenschutzgesetz*, “BDSG”) applies.

3. Is there a law regulating employee personal data?

Yes, in addition to the general provisions of the GDPR, section 26 of the BDSG applies.

4. Do I need to have a privacy statement or agreement?

A specific data protection agreement with the employee (or his/her consent) is not required to the extent that the handling of personal data is “necessary” for the hiring decision or, after hiring, for carrying out or terminating the employment contract. However, in some cases, details of the processing of employee personal data need to be agreed with the works council. In light of the documentation, transparency and accountability rules under the GDPR, a privacy policy or statement forms part of proper corporate governance.

5. How long must I retain employee data? What is best practice?

This depends on the type of personal data. Some personal data are to be deleted fairly promptly, whereas other personal data may be kept even beyond the end of the employment relationship.

6. Can I transfer employee data overseas?

Yes, in accordance with the general rules under the GDPR. In particular, an adequate level of data protection equivalent to the one in the EU is required, and, where this does not exist, appropriate safeguards must be in place before the employee data may be transferred.

7. Can I transfer employee data to a third party?

Yes, in accordance with the general rules under the GDPR. In particular, a legal basis within the meaning of Article 6 of the GDPR for the transfer is required.

8. What are the consequences of breach?

- Civil action brought by an employee for damages.
- Substantial fines.
- Criminal law punishment, including imprisonment.

9. What are the main pitfalls?

- It is unclear where the scope of “necessity,” according to section 26 of the BDSG, ends.
- Transfers among group companies and outside the EEA need to be approached with care.
- Works council participation may be required.





Germany

In Detail

1. To what extent does employee data privacy law in your jurisdiction go beyond the GDPR?

Pursuant to Article 88(1) of the GDPR, Member States may, by law or by collective agreements, provide for “more specific rules” to ensure the protection of the rights and freedoms in respect of the processing of employees’ personal data in the employment context. Germany has made use of its right to provide for more specific rules by introducing the new section 26 of the Federal Data Protection Act (*Bundesdatenschutzgesetz*, “**BDSG**”) that deals with data processing for employment-related purposes.

The term “employee” within the meaning of the BDSG includes:

- dependently employed workers (i.e., those in a traditional employer-employee relationship), including temporary workers contracted to the borrowing employer;
- persons employed for occupational training purposes;
- persons who should be regarded as equivalent to dependently employed workers because of their economic dependence; these include persons working at home and their equivalents; and
- applicants for employment and persons whose employment has been terminated.

Employee personal data may be processed for employment-related purposes where necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract or to exercise or satisfy rights and obligations of employees’ representation laid down by law, collective agreements or other agreements between the employer and staff council. Employees’ personal data may be processed to detect crimes only if there is a documented reason to believe the employee has committed a crime while employed, the processing of such data is necessary to investigate the crime and is not outweighed by the employee’s legitimate interest in not processing the data, and, in particular, the type and extent of processing are not disproportionate to the reason.

If employee personal data are processed on the basis of consent, then the employee’s level of dependence in the employment relationship and the circumstances under which consent was given shall be taken into account in assessing whether such consent was freely given. Consent may be freely given in particular if it is associated with a legal or economic advantage for the employee, or if the employer and employee are pursuing the same interests. Consent shall be given in written form, unless a different form is appropriate because of special circumstances. The employer shall inform the employee in text form of the purpose of data processing and of the employee’s right to withdraw consent





Germany

In Detail

pursuant to Article 7(3) of the GDPR.

By derogation from Article 9(1) of the GDPR, the processing of special categories of personal data as referred to in Article 9(1) of the GDPR (e.g., including data revealing racial or ethnic origin, political opinions and religious or philosophical beliefs) for employment-related purposes shall be permitted if it is necessary to exercise rights or comply with legal obligations derived from labor law, social security and social protection law, and there is no reason to believe that the employee has an overriding legitimate interest in not processing the data. If special categories of personal data shall be processed based on consent, such consent must explicitly refer to these data.

The processing of personal data, including special categories of personal data of employees for employment-related purposes, is also permissible on the basis of collective agreements, such as collective bargaining agreements or works council agreements. However, the negotiating partners must comply with Article 88(2) of the GDPR, and hence the collective agreements may not fall short of the data protection standards established by the GDPR.

Different from Article 2(1) of the GDPR, section 26 of the BDSG also applies when employee personal data, including special categories of personal data, are processed without forming or being intended to form part of a filing system.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant's personal data in your jurisdiction?

In addition to the general provisions of the GDPR, applicants for employment are regarded as employees within the meaning of section 26 of the BDSG and hence the general rules outlined in question 1 apply.

In relation to background checks, collected data may only be used to the extent necessary for the decision to appoint an applicant. The use of an applicant's personal data is only permitted up until the employer decides to make the job offer. As of an applicant's rejection, access to data has to be blocked until it is clear that no legal action will be taken; thereafter, data must be destroyed, deleted or returned to the applicant.

The transfer of an applicant's personal data to a third party (inside the EU or outside) will typically not be "necessary" within the meaning of section 26 of the BDSG. Thus, any such transfer will usually only be permissible if one of the legal bases set forth in Article 6 of the GDPR applies, e.g., if the transfer is necessary for the purposes of the legitimate interests pursued by the employer or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the applicant. A transfer to a recipient outside the EU must, furthermore, meet the requirements set forth in Chapter V of the GDPR, which means that the employer may have to implement certain





Germany

In Detail

safeguards in order to establish an adequate level of data protection at the recipient before the transfer may take place (please see question 6).

3. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee's personal data in your jurisdiction?

Yes, in addition to the general provisions of the GDPR, section 26 of the BDSG applies. Please refer to the response to question 1.

4. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee's personal data?

A specific data protection agreement with the employee (or his/her consent) is not required to the extent that the handling of their personal data is “necessary” for the hiring decision or, after hiring, for carrying out or terminating the employment contract. However, in some cases, the details of the processing of employee personal data need to be agreed with the works council, if any; this applies, in particular, to the introduction and use of technical means (such as devices or software) that would enable the employer to monitor the employees’ conduct and/or performance, even if such monitoring is not intended.

In light of the documentation, transparency and accountability rules under the GDPR, a privacy policy or statement forms part of proper corporate governance. Also, pursuant to Articles 13 and 14 of the GDPR, the employer shall, at the time when personal data are obtained, provide the employee with certain information, including the identity and the contact details of the employer, the contact details of the data protection officer, the purposes of the processing for which the personal data are intended as well as the legal basis for the processing, the recipients or categories of recipients of the personal data and, where applicable, the fact that the employer intends to transfer personal data to a third country and the appropriate safeguards that were implemented in order to establish an adequate level of data protection at the recipient.

5. For how long must an employer retain an employee's personal data? What is best practice?

Under the GDPR, an employee's personal data may be kept for no longer than is necessary for the purposes for which the personal data are processed. Hence, a distinction should be made between different categories of personal data.



HOME

GDPR
OVERVIEW

COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Germany

In Detail

For instance, an applicant's personal data must be deleted fairly shortly after the employer has declined the application. An explicit warning must be deleted from the personnel file after approximately two or three years, provided that the employee has not committed any similar breaches in the meantime.

Employee master data (such as name and contact details), however, must be retained for the duration of the employment relationship. Some personal data may also be retained even after the end of the employment relationship, for instance, personal data concerning occupational pension promises or post-termination restrictive covenants. In addition, various statutory provisions require the employer to retain certain data for a specified period of time: for example, documents containing information on overtime have to be retained for two years, in order for the relevant authorities to check if the requirements of the Working Time Act (*Arbeitszeitgesetz, ArbZG*) are met, and due to obligations under German tax laws, the employer must keep certain payroll documents for six years.

6. What are the legal restrictions on transferring employees' personal data outside your jurisdiction?

The general rules under the GDPR apply. In particular, an adequate level of data protection is required in the country where the recipient is located. This will not present any problems in the EU and the EEA. Most third countries, however, do not provide an adequate level of data protection (except where the European Commission has assessed a third country as adequate). If the country where the recipient is located does not guarantee an adequate level of data protection, the employer must implement certain further safeguards for the employees' personal data. These include binding corporate rules, standard data protection clauses and certification mechanisms. In the absence of these safeguards, data transfers may still take place in specific situations (e.g., with the employee's explicit consent once informed of the risks).

7. What are the legal restrictions on transferring employees' personal data to a third party?

It is important to bear in mind that there is no "group privilege"; this means that other group companies, including the parent company, are considered third parties, and hence any transfer to another group company must be based on one of the legal bases within the meaning of Article 6 of the GDPR.

If employees' personal data shall be shared with a processor (e.g., a payroll provider) it is important to enter into a proper data processing agreement that meets the requirements set forth in Article 28 of the GDPR.



HOME

GDPR
OVERVIEW

COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Germany

In Detail

8. What are the consequences of breaching privacy laws in your jurisdiction?

The affected employee can bring a civil action for damages. Moreover, significant financial penalties may be imposed on the employer. Depending on the nature of the breach, there are substantial fines for non-compliance with the GDPR, e.g., up to EUR 20 million or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

In terms of procedure, the rules stipulated in the Law on Regulatory Offences (*Ordnungswidrigkeitengesetz, OWiG*) and the general criminal law rules, namely the Code of Criminal Procedure (*Strafprozessordnung, StPO*) and the Code on Court Constitution (*Gerichtsverfassungsgesetz, GVG*) apply.

Furthermore, the BDSG contains an additional criminal law provision that could be relevant for employers: pursuant to section 42(1) of the BDSG, deliberately and without authorization transferring the personal data of a large number of people that are not publicly accessible to a third party, or otherwise making them accessible for commercial purposes, shall be punishable with imprisonment of up to three years or a fine.

9. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee's personal data?

The first obstacle is the inherent element of uncertainty when it comes to interpreting the generically phrased provisions of the BDSG and the GDPR. For instance, it can be quite difficult for an employer to determine whether the processing of an employee's personal data is "necessary" for the employment relationship pursuant to section 26 of the BDSG, or if the transfer of personal data to a third party, such as a service provider, is warranted by "legitimate interests."

Furthermore, there are issues of concern for multinationals who operate worldwide matrix structures with independent legal entities in different countries to handle their HR affairs in an integrated way, namely:

- the strict regulations on data transfers to third countries, i.e., outside the EU/EEA; and
- the fact that data privacy law regards affiliated companies (including the parent company) as third parties, which means that every transfer of employees' personal data requires a legal justification and must also comply with the various other restrictions, such as the data minimization principle whereby the disclosed data must be limited to what is necessary in relation to the purposes for which they are processed.





 In Brief

 In Detail

Germany

In Detail

Another area of concern is the far-reaching co-determination rights of the works council with regard to the collection and processing of employee personal data by means of technical devices or systems that would enable the employer to monitor the employees' conduct and/or performance, even if such monitoring is not intended. These co-determination rights are triggered if the employer wishes to introduce a new (or change an existing) system, such as a time recording device, GPS tracking, video surveillance or software, e.g., a new or upgraded operating system or a personnel management software such as PeopleSoft, Workday or SAP. In these cases, a written works agreement between the employer and the works council is required before the system may be rolled out.

Contributed by: **Dr. Guido Zeppenfeld, Björn Vollmuth & Vanessa Klesy**, Mayer Brown LLP



[Link to biography >](#)



[Link to biography >](#)



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



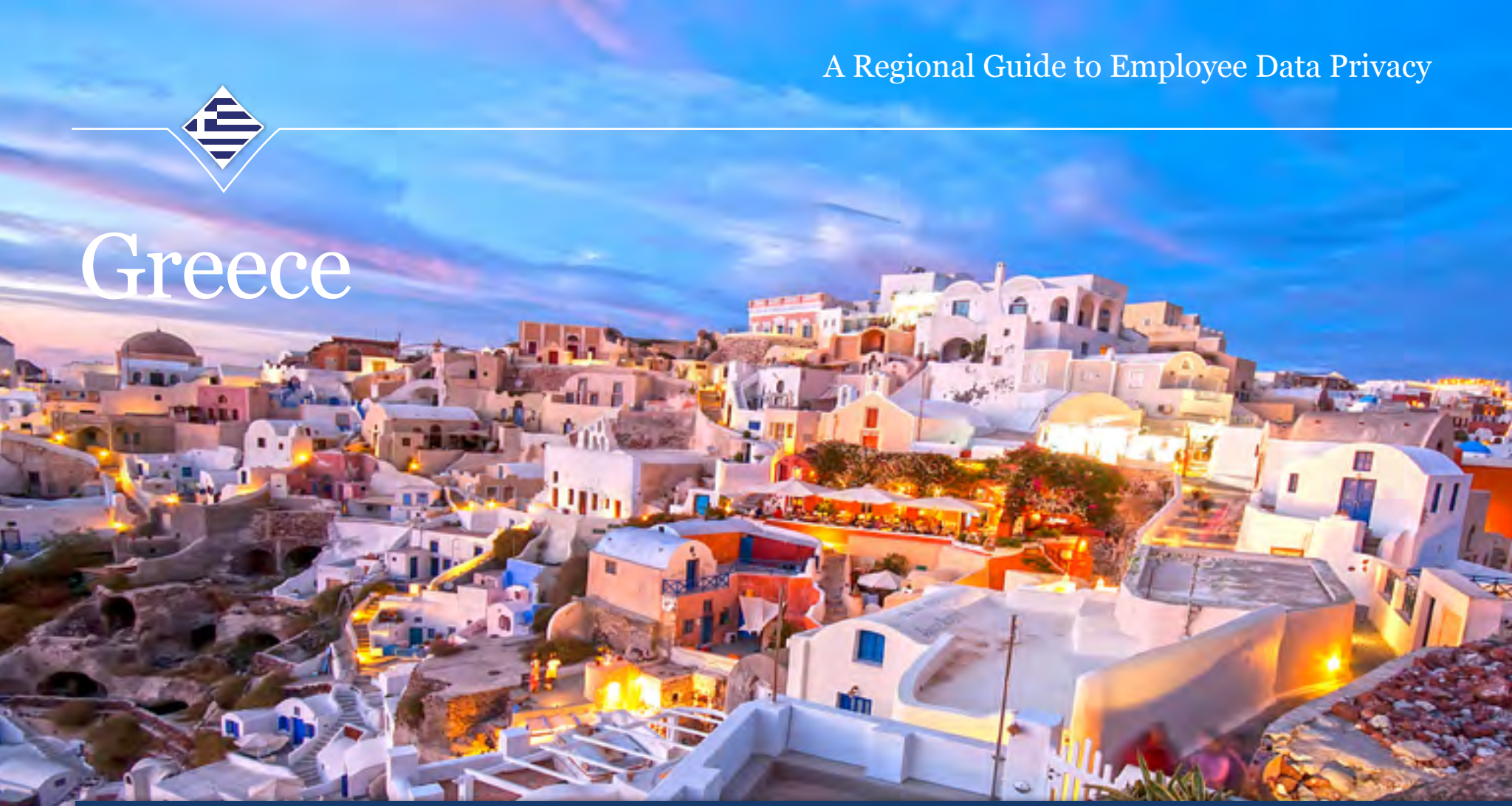
DIRECTORY

August 2018

SCROLL DOWN 



Greece



Contributed by: **Bernitsas Law**



In Brief



In Detail

Contributed by: **Tania Patsalia**, Bernitsas Law



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Greece

In Brief

1. Does employee data privacy law in your jurisdiction go beyond the GDPR?

In Greece, a draft bill implementing certain provisions of the GDPR (“**Draft Bill**”) – *inter alia* with regard to the processing of employee data in the employment context – was put into public consultation in early March 2018. Following this, an updated draft (not publicly available yet) is expected to be introduced soon to the Greek Parliament for discussion and adoption.

2. Is there a law regulating applicant personal data?

Under the Draft Bill, applicants are also treated as employees. In addition, and pending adoption of the Draft Bill, Directive 115/2001 of the Hellenic Data Protection Authority (“**HDP**A”), governing processing of personal data in the context of employment, includes provisions that are applicable to candidates. The general provisions of the GDPR also apply.

3. Is there a law regulating employee personal data?

Yes, apart from the Draft Bill and HDP A’s Directive (please see above), the current Greek Data Privacy Act is, until its replacement by the Draft Bill, the main legislation applicable to the protection of personal data in Greece. The general provisions of the GDPR also apply.

4. Do I need to have a privacy statement or agreement?

Employees must be properly informed in advance about the processing of their data in the employment context, in accordance with the GDPR requirements.

5. How long must I retain employee data? What is best practice?

Employee data should be kept for no longer than is necessary.

6. Can I transfer employee data overseas?

Yes, subject to appropriate safeguards being provided by the employer, in accordance with the GDPR requirements.

7. Can I transfer employee data to a third party?

The transfer of employee data to a third party is subject to the GDPR requirements and, under HDP A’s Directive, is permitted only for purposes directly related to the employment relationship or if the transfer arises from a statutory provision.

8. What are the consequences of breach?

Administrative and criminal sanctions may be imposed in the event of a breach. Damages may also be awarded.

9. What are the main pitfalls?

Draft Greek legislation has been formulated to cover the latest practices adopted/intended to be adopted by employers, such as processing of employees’ biometrics data, operation of CCTV in the workplace and use of geolocation tracking systems, which are permitted only under strict restrictions. There are also restrictions related to the processing of communications and monitoring employee use of the Internet.





Greece

In Detail

1. To what extent does employee data privacy law in your jurisdiction go beyond the GDPR?

In Greece, a draft bill implementing certain provisions of the GDPR (“**Draft Bill**”) was put into public consultation in early March 2018. Following this, an updated draft (not publicly available yet) is expected to be introduced soon to the Greek Parliament for discussion and adoption.

As the GDPR is directly applicable in Greece (as in all EU Member States), the Draft Bill applies to the processing of personal data in parallel with the GDPR, specifying, *inter alia*, the rules applicable to employees’ data processing and, in this regard, incorporating in essence the provisions laid down in existing guidelines issued by the Hellenic Data Protection Authority (“**HDP**A”) on those topics.

In particular, the Draft Bill specifies, among others, that:

- (a) employees also include candidates and former employees;
- (b) processing may, *inter alia*, be justified for the fulfillment of the employment relationship or on grounds of contract or law while, if the basis of the processing is employees’ consent, such consent must be in writing and given separately from the employment contract and employees must be free to revoke their consent without adverse effects;
- (c) special categories of data may only be processed based on contract or law;
- (d) data on criminal prosecutions, security measures and offenses may be processed where this is necessary to assess the employee’s qualifications for the specific job or to take a specific decision in the context of the employment;
- (e) CCTV in the workplace may be installed but only as an exception;
- (f) geolocation devices are allowed only for the protection of goods and persons or to ensure that the job has been performed where this is justified by the nature of the employment; and
- (g) monitoring employees’ communications in the workplace is permitted only where necessary for the protection of goods and persons or the organization and monitoring of the fulfillment of the employment, including checking expenses.

Employees must be individually and in writing informed about the processing of their data and the employer must have in place an internal regulation for the use of electronic communications in the workplace that should be made available





Greece

In Detail

to the employees (and the employer must be able to prove this). It is noted, for the sake of completeness, that the relevant provisions under the Draft Bill essentially elaborate and expand further on the rules already set out in Directive 115/2001 of the HDPa governing processing of personal data in the context of employment (“**Directive**”).

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant’s personal data in your jurisdiction?

The general provisions of the GDPR apply. Under the Draft Bill, applicants are also treated as employees. In addition, and pending adoption of the Draft Bill, the Directive also includes provisions that are applicable to candidates. The purpose of these provisions is to set out the boundaries within which the employer shall be entitled to lawfully collect, use and process employees’ as well as applicants’ data.

In this respect, the Directive provides that the employer, in its capacity as a controller, should collect the applicant’s personal data directly. If the applicant’s personal information is intended to be requested by a third party for the purpose of conducting a pre-employment check, the applicant must be informed in advance and must provide his/her explicit consent.

In any event, it is explicitly provided that the collection of applicant’s data should be restricted to what is absolutely necessary for the assessment of his/her suitability for the particular position. With regard to modern methods of personnel selection, such as through medical tests, it is stated that these should be performed only in exceptional cases and only if strictly necessary and appropriate for the fulfillment of a specific purpose directly related to the particular employment relationship in accordance with the principle of proportionality, and may be collected only following the applicant’s written consent, after he/she has been properly informed about the method, criteria, purposes and recipients of such data.

As regards the collection and further processing of information related to applicants’ criminal prosecutions and convictions, this is legally permissible only when justified by the particular job position (i.e., the employee will be handling money, etc.), as long as this is collected directly by the applicant.

Finally, with respect to the legal restrictions on the transfer of the applicant’s personal data overseas and/or to a third party, including to countries outside the EU/EEA, the GDPR provisions on the adoption of appropriate safeguards apply (please see question 6).





Greece

In Detail

3. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee's personal data in your jurisdiction?

Apart from the Draft Bill, which is expected to be introduced soon to the Greek Parliament for adoption, and the Directive (please see analysis above), the current Greek Data Privacy Act (i.e., Law 2472/1997 on the protection of individuals with regard to the processing of personal data, as in force, implementing Directive 95/46/EC into Greek law) is, until its replacement by the Draft Bill, the main legislation applicable to the protection of personal data in Greece. There is also secondary regulation in the form of decisions and directives of the HDP. The general provisions of the GDPR also apply.

4. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee's personal data?

Employees, as data subjects, must be provided with adequate information, in clear and plain language, regarding the processing of their personal data in the employment context, in accordance with the GDPR requirements.

In addition, under the Draft Bill, the employer, as the controller, is under an obligation to set up internal regulations governing the use of communication and other electronic means by employees in the workplace or for business purposes. Such regulations should be disclosed to employees, and the employer should be in a position to prove that all employees have been made aware of the regulations.

5. For how long must an employer retain an employee's personal data? What is best practice?

Data should not be kept for longer than is necessary for the purposes for which the data are processed, in accordance with the GDPR principles. Therefore, if an employment relationship is terminated or the employee has not been recruited, the information should be kept in a form that permits identification of data subjects only for the period that is necessary for defending a claim before a court or a public authority. Holding information on a candidate whose application has been rejected should be at the candidate's request and with a view to the company considering the candidate for a position at a later stage.





Greece

In Detail

6. What are the legal restrictions on transferring employees' personal data outside your jurisdiction?

The transfer of data outside the EU/EEA is subject to the legal restrictions under the GDPR. In this respect, the transfer of employees' personal data outside Greece, and, in particular, outside the EU/EEA, is subject to appropriate safeguards being provided by the employer, such as putting in place binding corporate rules or standard contractual clauses and on the condition that enforceable employees' rights and effective legal remedies for them are available.

7. What are the legal restrictions on transferring employees' personal data to a third party?

Under the Draft Bill, the collection and processing of employee personal data are only allowed for purposes directly related to the employment relationship or for purposes arising from a statutory provision. With regard to, in particular, the transfer of employees' data to a third party, this is only permitted for purposes directly related to the employment relationship or if the transfer is provided for under the law (subject also to the EU rules on the transfer of data to third countries) (please see Directive, p.20). As such, any transfer to a third party would need to be justified for specified purposes. Other members of the same group are also considered as third parties.

If employees' personal data shall be shared with a processor (e.g., a payroll provider), the employer should enter into a binding contract with the processor that meets the requirements set out in Article 28 of the GDPR.

8. What are the consequences of breaching privacy laws in your jurisdiction?

In the case of infringement of privacy laws in Greece, the administrative fines as provided for under the GDPR (i.e., amounting to up to EUR 20 million or up to 4% of the undertaking's total worldwide annual turnover of the preceding financial year, whichever is higher, depending on the type of infringement) may be imposed by the HDPa. In addition, the HDPa may also impose other administrative sanctions, such as warnings, reprimands or a ban on processing pursuant to the GDPR provisions.

Under the current Greek Data Privacy Act (until replaced by the Draft Bill), criminal sanctions, including fines and imprisonment, may also be imposed, and there are varying levels of fines and periods of imprisonment depending on the breach committed. The company's representative is liable to criminal sanctions where the controller is a legal entity. The infringer may be also liable to compensation for damages suffered, including moral damages.





Greece

In Detail

9. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee's personal data?

With the coming into effect of the GDPR, rules and principles established by the HDPa in its directives or case law to date have been elaborated on and further expanded by means of the Draft Bill which is expected to be adopted soon.

Also, draft Greek legislation has been formulated to cover the latest practices adopted/intended to be adopted by employers, such as processing of employees' biometrics data, operation of CCTV in the workplace and use of geolocation tracking systems, which are permitted only under strict restrictions (i.e., when absolutely necessary for the protection of persons and goods in the workplace, taking into account the nature of the work, etc.).

There are also restrictions related to the processing of communications and monitoring employee use of the Internet. In particular, the collection and processing of data regarding communications in the workplace, including email, are only permitted where absolutely necessary for the protection of persons and goods in the workplace and for organizing and monitoring the completion of a particular task or cycle of work and especially for cost control purposes. The communication data processed should be restricted to that which is absolutely necessary and relevant in order to achieve these specified purposes. In this respect, employers are obliged to put in place internal regulations, of which the employees must acquire knowledge (in a proven manner).

In any event, an employer's obligation to provide employees with information regarding all aspects of the processing of their data in the employment context is taken particularly seriously by the HDPa, and compliance should be ensured in a proven manner at all times.

Contributed by: **Tania Patsalia**, Bernitsas Law

 [Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Hungary

Contributed by: **Bán, S. Szabó & Partners**



In Brief



In Detail

Contributed by: **Péter Szemán, Bán, S. Szabó & Partners**



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Hungary

In Brief

1. Does employee data privacy law in your jurisdiction go beyond the GDPR?

The amended Hungarian Data Protection Act (the “**Data Protection Act**”) has now been harmonized with the GDPR and does not contain special rules that would go beyond the GDPR. The proper interpretation is that both the Data Protection Act and the GDPR have to be applied in parallel.

2. Is there a law regulating applicant personal data?

In addition to the GDPR, the Data Protection Act and the Labor Code contain general rules regarding the processing of the applicant’s personal data, in particular, what kind of information and what kind of tests/examinations may be requested from the applicant.

3. Is there a law regulating employee personal data?

In addition to the GDPR, the Data Protection Act and the Labor Code regulate employee personal data.

4. Do I need to have a privacy statement or agreement?

A privacy policy is not a requirement; however, it is advisable. Informing employees about the processing of their personal data is a requirement under the GDPR.

5. How long must I retain employee data? What is best practice?

Generally, personal data should be kept for no longer than necessary for the purposes for which the personal data are processed. Although there are no explicit rules in Hungary, retention periods may be governed by the relevant limitation periods for the applicable data and/or eligibility requirements for pension/social security benefits.

6. Can I transfer employee data overseas?

Yes, subject to conditions.

7. Can I transfer employee data to a third party?

Yes, subject to conditions.

8. What are the consequences of breach?

Alongside the penalties under the GDPR, under local data protection laws, the data protection authority may impose a fine of up to HUF 20 million/EUR 65,000.

9. What are the main pitfalls?

The monitoring of employees during work is a hot topic in Hungary, and it is only legal in certain circumstances. A workplace may only be monitored by cameras subject to the following conditions:

- (a) employees must receive information about the camera surveillance;
- (b) visitors to the site should be reminded that camera surveillance is taking place; and
- (c) internal rules should regulate how the cameras are placed and the recordings are stored, reviewed, used and deleted.





Hungary

In Detail

1. To what extent does employee data privacy law in your jurisdiction go beyond the GDPR?

The key legislation in Hungary regulating data protection issues is Act CXII of 2011 on the Information Self Determination Right and Freedom of Information (the “**Data Protection Act**”). The Data Protection Act has now been harmonized with the GDPR with the most recent amendment containing rules that are compatible with the GDPR. The Data Protection Act does not go beyond the GDPR. According to the interpretation of the Hungarian Data Protection Authority, the two laws have to be applied in parallel. The specific local regulations required by the GDPR (e.g., codes, requirement to carry out data protection assessments) are not yet available.

According to the amended Data Protection Act, the Hungarian Data Protection Authority is appointed as the supervisory authority in Hungary within the meaning of the GDPR. Regarding fines, the Data Protection Act provides that the Data Protection Authority will sanction a possible breach of the GDPR first by giving a warning to the controller.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant’s personal data in your jurisdiction?

There is no specific law regulating the applicant’s personal data. The general rules of the GDPR, Data Protection Act and the Labor Code have to be applied.

Act I of 2012 on the Labor Code (the “**Labor Code**”) provides specific rules regarding the protection of the employees’ personal data that should be taken into account when processing an applicant’s personal data. According to the Labor Code, an employee may be required to make a statement or to disclose certain information only if it does not violate his/her privacy rights and, if deemed necessary for the conclusion, fulfillment or termination of the employment relationship. An employee may be required to take an aptitude test if this is prescribed by employment regulations, or if deemed necessary with a view to exercising rights and discharging obligations in accordance with employment regulations.

As a general labor law principle, the rights relating to the personality of employees may be restricted if deemed strictly necessary for reasons directly related to the intended purpose of the employment relationship and if proportionate for achieving its objective. The means and conditions for any restriction of rights relating to personality, and the expected duration, should be communicated to the affected employees in advance.





Hungary

In Detail

When an applicant wishes to apply for a position at the employer, he/she has to provide his/her personal data. Before sending the personal data, the applicant has to receive detailed information about the processing of his/her data, including:

- the legal title of the data processing, its purpose and duration;
- the possible data transfer to third parties; and
- the rights and remedies of the applicant in connection with the data processing.

The above information sheet has to be available to the applicant, and he/she has to approve it before consenting to send the personal data to the employer.

Applicant data may be stored and processed only when it is strictly necessary for the given purpose. So, if the position is filled and the applicant is refused, his/her personal data has to be deleted, unless the applicant specifically consented to store and process his/her personal data for the purpose of information about future open positions. If the applicant initiates a legal dispute against the employer because of the refusal (e.g., breaching equal treatment rules), the data may be processed until the legal procedure is completed with a final and non-appealable court decision.

For the transfer of applicant data overseas or to a third party, please see responses to questions 6 and 7.

3. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee’s personal data in your jurisdiction?

The Data Protection Act was harmonized with the Directive 95/46/EC of the European Parliament and Council of October 24, 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Data. The Data Protection Act has also been harmonized with the GDPR. So currently in Hungary, both the GDPR and the Data Protection Act have to be applied in parallel.

The provisions of the Data Protection Act shall apply if the main establishment (within the meaning of the GDPR) of the controller is in Hungary or, if the main establishment of the controller is not in Hungary, but the data processing activity carried out by controller or processor is connected to the provision of products or services provided to data subjects





Hungary

In Detail

residing in Hungary, or it is connected to the monitoring of the data subjects in Hungary. The provisions of the Data Protection Act shall not apply to data processing of natural persons for their own personal purposes. According to the definition of the Data Protection Act, “personal data” shall mean any information relating to the data subject.

The Data Protection Act provides that “processing of data” shall mean any operation or set of operations that is performed upon data, whether or not by automatic means, such as in particular collection, recording, organization, storage, adaptation or alteration, use, retrieval, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, and blocking them from further use, photographing, sound and video recording, and the recording of physical attributes for identification purposes (such as fingerprints and palm prints, DNA samples and retinal images).

The Labor Code provides specific rules regarding the protection of the employees’ personal data. As noted above, the rights relating to the personality of employees may be restricted if deemed strictly necessary for reasons directly related to the intended purpose of the employment relationship and if proportionate for achieving its objective. The means and conditions for any restriction of rights relating to personality, and the expected duration, should be communicated to the affected employees in advance.

Employers shall be allowed to monitor the behavior of employees only to the extent pertaining to the employment relationship. The employers’ actions of control, the means and methods used, may not be at the expense of human dignity. The private lives of employees may not be monitored. Employers have to inform their employees in advance concerning the technical means used for the surveillance of employees.

4. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee’s personal data?

There is no requirement in Hungary to have a privacy policy or other data protection internal regulation; however, it is standard in Hungary that a data privacy policy regulates all issues in connection with the data processing. The amended Data Protection Act, in compliance with the GDPR, provides that the controller and processor shall keep records about all data processing activities, personal data breaches and the actions carried out in connection with access to personal data. Such records shall contain, in particular, the name and contact details of the controller and processor, the purpose of the data processing, the transfer of data, the scope of the data subjects and data processed, the legal title of processing, and the date of the deletion of data. Maintaining such records is obligatory for employment-related databases as well.





Hungary

In Detail

In connection with the GDPR, it is now also common that employees are informed about all details of the processing of their personal data, including the hiring process, the data transfer to third parties, the various data retention periods, engagement of processors acting on behalf of the employer (controller), transfer of data within the company group for internal administration/HR purposes, camera recording at the workplace, use of GPS in the company cars and application of whistleblowing systems. In the case of camera recording, this has to be regulated in detail. The whistleblowing system generally also needs detailed internal rules. The company car policy may contain the rules for the application of the GPS system and monitoring the employee's route during daily work which would also have privacy implications.

As a general principle, the employee has to be notified of all circumstances regarding the processing of his/her personal data in connection with the employment. Therefore, it is advisable to implement an employee data processing information sheet that is available to all employees (e.g., on the internal intranet). This information sheet/policy has to detail:

- the legal title and purpose of the data processing;
- the types of data that the employer processes about the employees;
- the duration of processing of the various scopes of data;
- the transfer of data to third parties (within the group, for accounting or payroll purposes);
- camera recording in the workplace or other technical equipment used to monitor the employees (GPS used in the company cars);
- rules of web usage and monitoring of emails;
- rules of using entrance cards; and
- the rights and remedies available in case of unlawful data processing.

5. For how long must an employer retain an employee's personal data? What is best practice?

According to the general "data minimization" and "storage limitation" principles of the GDPR, personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, and shall not be stored for longer than it is strictly necessary for the given purpose. According to the amended Data Protection





Hungary

In Detail

Act, if the storage period is not regulated by legal regulation or binding EU law, the controller has to review whether the given data processing is still necessary for the given purpose at least every three years. The result of this review has to be documented and stored for 10 years and, in the case of any request, has to be provided to the Data Protection Authority. This periodic review could be required in the case of labor law data processing as well. The first review has to be completed by May 25, 2021 for data processing started prior to May 25, 2018.

In Hungary, there are no clear and explicit rules for how long HR data may be stored. The general labor law statute of limitation period is three years; for claims for breach of privacy rights and claims for compensation the statute of limitation is five years. So, as a general approach, after the five-year statute of limitation period from the end of the employment has passed, the HR data has to be deleted. Those data that are required for tax returns may be processed until the expiry of the tax statute limitation period (which is five years from the end of the year when the tax return is due). The data required for financial returns have to be stored for eight years.

Although not explicitly regulated by law, employee data that are required for the eligibility to pension or other state benefit cannot be deleted because they might be necessary when the employee reaches the pension age or even thereafter (e.g., potentially 50 to 70 years after termination of employment). Such data may include the name, tax number, start and end of the employment, and the salary paid to the employee which form the basis of the pension entitlement.

It is advisable to regulate the retention deadlines in an internal policy or in the information letter available to the employees with the details of the HR data processing.

6. What are the legal restrictions on transferring employees' personal data outside your jurisdiction?

According to the Data Protection Act, personal data may be transferred to a controller or processor located in a third country (outside of the EU/EEA) if (a) the data subject expressly consented to the data transfer or (b) the data transfer is required for the purpose of the data processing and, in this regard, the general requirements of the data processing are fulfilled, and in the third country or at the controller or processor in the third country the adequate level of protection is fulfilled.

An adequate level of protection is required. This will not present any problem for countries in the EU/EEA. For other countries, if the European Commission has not already decided that they provide an adequate level of protection, appropriate safeguards must be in place. These include binding corporate rules, standard data protection clauses, approved certification mechanisms or other mechanisms. In the absence of these safeguards, data transfers may





Hungary

In Detail

still take place in specific situations (e.g., where the data subject has explicitly consented after being informed of the possible risks, it is necessary for the essential interests of the data subject or another person, it is necessary to remedy a significant danger or is in the public interests of an EEA or third country).

7. What are the legal restrictions on transferring employees' personal data to a third party?

The data transfer qualifies as a type of data processing, so the transfer of employee data to a third party is possible if there is a general legal title for the processing as provided by Article 6 of the GDPR (consent of the data subject, legitimate interest, performance of a contract).

In addition to the general requirements of the GDPR, the Data Protection Act provides that, prior to the data transfer, the controller or the processor has to double-check the accuracy of the data. If the controller or processor finds that the data are inaccurate, not up to date or deficient, such data may be transferred only if the transfer is indispensably necessary for the purpose of the data processing, and the controller or processor informs the transferee of the accuracy of the data.

As a general principle, the Labor Code provides that the employer has to inform its employees about the processing of their personal data. The employer is permitted to disclose facts, data and opinions concerning an employee to third persons in the cases specified by law or upon the employee's consent.

In the interests of fulfilling the obligations stemming from an employment relationship, the employer is authorized to disclose the personal data of an employee to a controller as prescribed by law, indicating the purpose of disclosure, of which the affected employee shall be notified in advance.

Based on these rules, employee data may be transferred to a payroll agent for further processing with a notification sent to the employees. This can be made in the general employee data protection information letter that all employees receive.

8. What are the consequences of breaching privacy laws in your jurisdiction?

Depending on the nature of the breach, there are substantial fines for non-compliance with the GDPR:

- (a) Up to EUR 10 million or, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher; and





Hungary

In Detail

- (b) Up to EUR 20 million or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.
- The Data Protection Authority may also initiate an administrative procedure itself or based on the request of an applicant. During such investigation, the Authority reviews the employer’s compliance with the data protection laws.
- In its resolution adopted in administrative proceedings for data protection, the Authority may:
- (a) impose all those sanctions that are provided in the GDPR;
 - (b) establish the unlawful handling or processing of personal data;
 - (c) order the revision of any personal data that is deemed inaccurate;
 - (d) order the blocking, erasure or destruction of personal data handled or processed unlawfully;
 - (e) prohibit the unlawful handling or processing of personal data;
 - (f) prohibit the cross-border transmission or disclosure of personal data;
 - (g) order the information of the data subject, if it was refused by the controller unlawfully; and
 - (h) impose a financial penalty on the controller or processor.
- The Authority may also issue an order to have its resolution published, including the controller’s particulars, if the case concerns a large segment of the population, is connected to the activity of a body with public service functions or if public disclosure appears justified on account of the gravity of the infringement.
- The amount of the financial penalty imposed shall be between HUF 100,000 and HUF 20 million (between EUR 300 and EUR 65,000). This fine is in addition to the sanctions and fines imposed by the GDPR.
- The Authority shall decide whether or not to impose a penalty, and the amount of the penalty, by taking into account all circumstances of the case, in particular the number of data subjects affected by the infringement, the gravity of the infringement and whether it is a repeat offense.





Hungary

In Detail

9. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee’s personal data?

A hot topic and a pitfall could be video recording/camera surveillance/voice recording during work that all qualify as data processing. This practice is legal if special conditions are fulfilled.

For example, the employer has to give information about camera surveillance to the employees. This information has to include the following:

- the legal title of the recordings (e.g., the relevant provision of the Data Protection Act or the EU Data Protection Directive that makes the data processing possible);
- the position of the cameras and the purpose of the camera positioning (e.g., monitoring those assets which are protected);
- the purpose of the surveillance (e.g., the protection of assets);
- the name of the entity that operates the recordings;
- the duration and place of storing the recordings;
- the data security measures taken by the operator in connection with storing the recordings;
- the scope of people entitled to review the recordings (e.g., only authorized employees at the employer);
- the rules of reviewing the recordings and for what purposes the employer may use the recordings; and
- the rights and remedies available to the employees (e.g., they can turn to the compliance or HR officer if they believe that their privacy rights have been violated and then turn to the data protection commissioner).

The information must be simple, clear and understandable for the employees and must include all the above topics. A general notification that “camera surveillance is taking place at the work site” is not sufficient. The employer must also be able to prove that the employees received the information about the camera surveillance.





Hungary

In Detail

The monitoring should have a legitimate purpose. As an example, asset protection can be a legitimate purpose for camera monitoring. However, monitoring of the employee's work performance or his/her behavior are not permitted purposes of the monitoring.

No cameras may be placed in places that might breach the privacy of the employees or other individuals (e.g., a dressing room, shower room, toilet). If, however, no one is authorized to enter the site (e.g., on public holidays, rest days), the whole area of the site may be monitored.

The records have to be deleted within three working days unless the film has to be used for a specific purpose, especially in criminal proceedings or other investigation.

In addition to the above, an on the spot brief information sheet must be made available for all those persons (e.g., third parties, customers, visitors) who visit the site, confirming that camera surveillance is taking place (e.g., at the entrance of the site, in the corridors, at the most important points of the site). Pictograms must also warn the employees and other persons that camera surveillance is taking place.

It is advisable that the employer regulates in internal rules the above issues relating to camera recordings.

Contributed by: **Péter Szemán, Bán, S. Szabó & Partners**



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Iceland



Contributed by: **LOGOS Legal Services**



In Brief



In Detail

Contributed by: **Áslaug Björgvinsdóttir**, LOGOS Legal Services



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Iceland

In Brief

1. Does employee data privacy law in your jurisdiction go beyond the GDPR?

Yes, special provisions apply in relation to electronic surveillance in the workplace.

2. Is there a law regulating applicant personal data?

Yes, the Data Protection Act and the GDPR.

3. Is there a law regulating employee personal data?

Yes, the Data Protection Act and the GDPR.

4. Do I need to have a privacy statement or agreement?

Employees must be provided with certain information when their personal data are processed.

5. How long must I retain employee data? What is best practice?

This depends on the data and the purpose for which they were collected. Some data must be retained for up to 14 years.

6. Can I transfer employee data overseas?

Yes, if that country provides an adequate level of personal data protection.

7. Can I transfer employee data to a third party?

Yes, but such transfer must be based on one of the legal grounds of processing.

8. What are the consequences of breach?

Fines of up to ISK 2.4 billion or 4% annual worldwide turnover, daily fines, imprisonment and compensation to data subjects.

9. What are the main pitfalls?

The main pitfalls for employers include retaining data for too long, collecting too much information, failing to provide the necessary information to data subjects and not complying with electronic surveillance rules.





Iceland

In Detail

1. To what extent does employee data privacy law in your jurisdiction go beyond the GDPR?

The legislation implementing the GDPR came into effect on July 15, 2018 by Act No 90/2018 (the “**Data Protection Act**”). According to the Data Protection Act, special provisions on electronic surveillance in the workplace apply. According to Article 14, paragraph 4 of the Act, electronic surveillance in the workplace shall be clearly labelled and identify the controller. The Data Protection Authority has also implemented rules on electronic surveillance (No. 837/2006) that include special provisions on employees’ email and Internet use and monitoring employees’ work performance.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant’s personal data in your jurisdiction?

The Data Protection Act, which implements the GDPR, applies equally to the collection, use and handling of applicants’ and employees’ personal data in Iceland.

Personal data can only be processed based on one of the legal grounds of processing, but the processing of applicants’ personal data is primarily processed based on the applicant’s request to enter into a contract with the employer, therefore based on Article 6, paragraph 1(b) of the GDPR (please see Article 9, item 2 of the Data Protection Act).

If an employer wishes to conduct background checks during the application process, and obtain records from applicants on their criminal convictions and offenses, the processing must furthermore comply with Article 12 of the Data Protection Act. According to Article 12 of the Data Protection Act, a private party cannot process information on data relating to criminal convictions and offenses unless the applicant has given his/her explicit consent for the processing, or if the processing is necessary for the purposes of the employer’s legitimate interests, where such interests are not overridden by the fundamental rights and freedom of the applicant. Whether an employer is warranted in conducting a background check on applicants must also be evaluated on grounds of the nature of the job. Furthermore, in certain instances, an employer may have a legal obligation to obtain records from applicants on their criminal convictions and offenses.

According to the Data Protection Act, all processing of personal data must also comply with the principles relating to processing of personal data, pursuant to Article 5 of the GDPR and Article 8 of the Data Protection Act. An employer must thus only process personal data that are necessary in order to achieve the recruitment/selection purpose. The employer must also inform all job applicants how their data will be processed and for what purposes, before applicants submit their application.





Iceland

In Detail

Finally, personal data of applicants can only be stored as long as necessary for the purpose of their collection. The retention time for unsuccessful applications (job vacancies) is often six months after the relevant deadline.

3. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee's personal data in your jurisdiction?

Yes, the Data Protection Act, which implements the GDPR.

Personal data can only be processed based on one of the legal grounds of processing according to Article 6 of the GDPR and Article 9 of the Data Protection Act. Personal data collected on employees are primarily processed for the performance of an employment contract (such as for the purpose of salary payments) in accordance with Article 6, paragraph 1(b) of the GDPR and Article 9, item 2 of the Data Protection Act. Processing of an employee's personal data can also be carried out to comply with the controller's legal obligation (e.g., tax law) or based on the employer's legitimate interests (such as for security purposes), in accordance with Article 6, paragraph 1(c) and (d) of the GDPR and Article 9, items 3 and 6 of the Data Protection Act.

The processing must also comply with the general principles of the Data Protection Act and the GDPR (please see Article 5 of the GDPR and Article 8 of the Data Protection Act). This means in practice that employee personal data can only be retained for as long as necessary in relation to the purpose for which they are processed, unless otherwise permitted or obligated by law. Employees must also be informed on how their personal data are processed, and special rules must be implemented regarding electronic surveillance at the workplace. An employer must therefore keep all personal data safe and accurate.

4. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee's personal data?

Under the Data Protection Act, employees (as well as other data subjects) must be provided with certain information when their personal data are processed. The information shall be provided in writing or by other means, including, where appropriate, by electronic means (Article 12 of the GDPR and Article 17 of the Data Protection Act).





Iceland

In Detail

The information to be provided is detailed in Articles 13 and 14 of the GDPR and Article 17 of the Data Protection Act. It includes the identity and contact details of the employer, the contact details of the data protection officer where applicable, the purposes of the processing for which the personal data are intended as well as the legal basis for the processing, the recipients or categories of recipients of the personal data and, where applicable, the fact that the employer intends to transfer personal data to a third country and the appropriate safeguards implemented.

5. For how long must an employer retain an employee's personal data? What is best practice?

An employer must retain employee data only for as long as necessary to fulfill the purposes for which the personal data were collected.

In order to be able to defend an employer against any legal claims that may arise after the exit process of a former employee, an employer may keep personal data that relates to its salary decisions for a maximum of 14 years after the completion of the exit process (Act No. 10/2008 on equal status and equal rights of women and men).

Pay slips and other book-keeping records are kept for seven years, in accordance with requirements of the Accounting Act No. 145/1994.

Other data, such as absences for sickness and information necessary for salary processing, shall be retained for a maximum of four years after the completion of an exit process of the employee, unless the data are necessary to establish, exercise or defend against legal claims (Act No. 150/2007 on the limitation periods for claims).

In relation to personal data collected and processed via electronic surveillance, personal data can be kept for no longer than 90 days, unless they are necessary to establish, exercise or defend against legal claims (the Data Protection Authority's rules on electronic surveillance No. 837/2006). However, logging data collected via the use of entrance cards and traffic logging may be kept for a longer period.

6. What are the legal restrictions on transferring employees' personal data outside your jurisdiction?

The GDPR does not prohibit the transfer of employees' personal data; however, there must be an adequate level of data protection in the country to which data are transferred that is equivalent to the level required in the EU. If the country where the recipient of the data is located does not guarantee an adequate level of data protection, an employer must implement certain additional safeguards for the employees' personal data before it may be transferred.





Iceland

In Detail

This will not present problems in the EU and the EEA, given the application of the GDPR; however, most other countries are not considered to provide an adequate level of data protection. Generally, in the absence of an adequacy decision from the EU Commission, one of the legal safeguards or derogations must apply to ensure the legality of transferring data outside the EU/EEA. These include standard contract clauses, EU model clauses, binding corporate rules, explicit consent in limited circumstances, and, in respect of the United States, the Privacy Shield.

7. What are the legal restrictions on transferring employees' personal data to a third party?

An employer can only transfer employee personal data to a third party if one of the conditions on lawfulness of processing, set out in Article 6 (and Article 9 as applicable) of the GDPR, is met (please see also Articles 9 and 11 of the Data Protection Act).

The employer and the third party also need to enter into a data processing contract according to Article 28 of the GDPR (please see also Article 26 of the Data Protection Act).

8. What are the consequences of breaching privacy laws in your jurisdiction?

If an entity does not comply with the instructions of the Data Protection Authority regarding (a) a temporary or definitive limitation, including a ban on processing, (b) rectification or erasure of personal data or restriction of processing and the notification of such actions to recipients to whom the personal data have been disclosed, or (c) suspension of data flows to a recipient in a third country or to an international organization, the Authority can decide to impose daily fines upon the entity until it concludes that necessary improvements have been made. Fines can amount up to ISK 200,000 for each day that passes without the Data Protection Authority's instructions being observed.

Breaches of the Data Protection Act, which implements the fines set out in the GDPR, can lead to fines from ISK 100,000 to ISK 2.4 billion or up to 4% of the annual worldwide turnover, whichever is higher (please see also Article 46 of the Data Protection Act). Major breaches can also lead to imprisonment of up to three years and a breach of confidentiality by a data protection officer can lead to fines or imprisonment of up to one year and in severe cases up to three years (Article 48 of the Data Protection Act).

The data subject can also claim compensation from a controller or a processor.





Iceland

In Detail

9. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee's personal data?

In practice, the main pitfalls that employers have fallen into regarding the processing of their employees' personal data concern retention periods (data not deleted), too much information collected and electronic surveillance in the workplace that is not in accordance with the Data Protection Authority's rules on electronic surveillance, which apply to CCTV, monitoring/viewing of emails and Internet use.

Contributed by: **Áslaug Björgvinsdóttir**, LOGOS Legal Services

 [Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Ireland



Contributed by: **A&L Goodbody**



In Brief



In Detail

Contributed by: **Ailbhe Dennehy**, A&L Goodbody



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Ireland

In Brief

1. Does employee data privacy law in your jurisdiction go beyond the GDPR?

Yes, in addition to the GDPR, requirements apply to the processing of employee personal data arising from the Data Protection Act 2018 (the “**2018 Act**”) which implements the GDPR in Ireland; the Law Enforcement Directive (as transposed by the 2018 Act; the Data Protection Acts 1988 and 2003 (the “**1988 and 2003 Acts**”)); and the E-Privacy Regulations 2011.

2. Is there a law regulating applicant personal data?

Yes, the above legislation also applies to applicants as they fall within the definition of “data subjects.” The guidance issued by the Irish Data Protection Commission from time to time should also be followed in processing personal data, including processing applicant personal data.

3. Is there a law regulating employee personal data?

Yes, the above legislation also applies to the processing of employee personal data in Ireland. The guidance issued by the Irish Data Protection Commission from time to time should also be followed when processing the personal data of employees.

4. Do I need to have a privacy statement or agreement?

Under both the GDPR and the 2018 Act, it is necessary to provide information on the processing activity to affected employees at the time of processing. This is generally done by means of a data privacy notice or privacy statement.

5. How long must I retain employee data? What is best practice?

The GDPR provides that personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

There is no blanket retention period that covers all employee data, and employers must determine how long to retain personal data in accordance with other statutory retention periods, limitation periods for legal claims, individual business needs and data quality principles.

6. Can I transfer employee data overseas?

Yes, although the transfer is subject to the employer complying with certain conditions under the GDPR.

7. Can I transfer employee data to a third party?

Yes, however, the employer must be satisfied that adequate safeguards are in place to ensure that the third party also complies with data protection requirements.

8. What are the consequences of breach?

There are potential fines for controllers and processors who contravene the provisions of the GDPR and who are prosecuted for data protection breaches. There is also potential for the criminal sanction of imprisonment and/or a fine under the 2018 Act.

9. What are the main pitfalls?

- Unreliable nature of employee consent;
- New rules around data subject access requests; and
- Demonstrating compliance with the GDPR.





Ireland

In Detail

1. To what extent does employee data privacy law in your jurisdiction go beyond the GDPR?

In addition to the GDPR, the Data Protection Act 2018 (the “**2018 Act**”), the Law Enforcement Directive (Directive (EU) 2016/680) (the “**Law Enforcement Directive**”), and the Data Protection Acts 1988 and 2003 (the “**1988 and 2003 Acts**”) apply to the processing of employee personal data in Ireland.

The 1988 and 2003 Acts will apply to a data protection complaint or infringement of law that relates to an incident that occurred pre-commencement of the GDPR on May 25, 2018.

The Law Enforcement Directive, as transposed into law by the 2018 Act, applies with regard to the processing of personal data by competent authorities for the purpose of prevention, investigation or prosecution of criminal offenses. A competent authority is any public authority competent for the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. To the extent that an employee’s data may be processed in the context of an investigation/prosecution by a public authority, the Law Enforcement Directive applies in addition to the provisions of the GDPR.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant’s personal data in your jurisdiction?

The processing of applicant personal data is governed by the GDPR, the 2018 Act and the Law Enforcement Directive.

Applicants are considered to be data subjects under the GDPR, and, as a data subject, the applicant will be entitled to the same information as employees regarding processing activity concerning their personal data. This information can be provided in the form of a Data Privacy Notice or Privacy Statement.

Under the GDPR, employers must be able to demonstrate that data are collected for a specified, explicit and legitimate purpose and not processed beyond that purpose. This can pose difficulties for employers that carry out background checks on job applicants. Similarly, requesting information on an applicant’s credit history may be regarded as excessive data processing and a breach of the GDPR.

The Irish Data Protection Commission (the “**DPC**”) has previously issued guidance that outlines that an employer should only be concerned about an applicant’s history of criminal offenses where this information is relevant to a particular job offer. For example, if a conviction relates to a driving offense where driving is a function of the job, then the conviction history will be relevant to the job application process. Under the GDPR, the processing of personal data relating to





Ireland

In Detail

criminal convictions or offenses is substantially restricted. Reliance on the explicit consent of applicants as the basis for conducting such criminal background checks is not recommended, due to the imbalance of power in the employment relationship. In most cases, employers that conduct criminal background checks will need to rely on an alternative legal basis for processing employee criminal conviction data, for example, compliance with a legal obligation. In the absence of further guidance from the DPC, the current recommended practice is for an employer to request an employee to voluntarily self-certify if they have any previous criminal convictions that may impact their suitability for a particular job offer. Where an employer is relying on self-certification, the employee should be informed that they are not required to declare spent convictions and that the self-certification disclosure is an entirely voluntary one.

The rules governing the transfer of personal data under the GDPR as outlined at questions 6 and 7 below apply in respect of an applicant’s personal data. However, it may be more difficult for an employer to demonstrate a legitimate legal basis for transferring the applicant’s personal data to third parties/non-EEA countries.

3. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee’s personal data in your jurisdiction?

The processing of employee personal data will be governed by the GDPR, the 2018 Act and may be governed by the 1988 and 2003 Act and the Law Enforcement Directive.

Personal data are defined as “any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”

The GDPR introduces a number of substantial changes to the processing of personal data that will impact the employee/ employer relationship. Traditionally, Irish-based employers have relied on blanket consent provisions within the contract of employment for processing personal data; however, under the GDPR, this may no longer be reliable in circumstances where the GDPR provides a right to employees to withdraw their consent and halt data processing, at any time.

The GDPR sets out the six lawful bases for processing personal data (including employee personal data):

- (a) The data subject consents to the processing;





Ireland

In Detail

- (b) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering the contract;
- (c) Processing is necessary for compliance with a legal obligation;
- (d) Processing is necessary to protect the vital interests of the data subject or another person;
- (e) Processing is necessary in the public interest or for the exercise of an official authority; and
- (f) Processing is necessary for the purposes of legitimate interests pursued by the controller or third party, except where such interests are overridden by the rights of the data subject.

Going forward, most employers will move away from “consent” as a basis for processing and identify an alternative ground for processing the majority of employee personal data. It is anticipated that most employers will rely on the legitimate interest of the business ground (for example, the monitoring of office space for security purposes), the performance of the contract (for example, processing bank details for payroll purposes) and compliance with a legal obligation (for example, Revenue reporting).

The processing of special category data (i.e., data concerning racial, ethnic origin, political opinions, religious/philosophical beliefs, trade union membership, genetic data, biometric data, health/sexual data) is prohibited unless one of the following grounds applies:

- (a) The data subject explicitly consents;
- (b) Processing is necessary for the employer to carry out obligations/exercise rights under employment, social security or social protection law or pursuant to a collective agreement, provided there are appropriate safeguards in place;
- (c) Processing is necessary to protect the vital interests of the data subject or another person where the data subject is not capable of consenting;
- (d) Processing relates to personal data that are manifestly made public by the data subject;
- (e) Processing is necessary for establishment, exercise or defense of legal claims;
- (f) Processing is necessary for reasons of substantial public interest; or





Ireland

In Detail

(g) Processing is necessary for the purposes of occupational health/assessment of the working capacity of the employee.

In the context of employment, the processing of special category data can occur in a range of circumstances, including in the context of assessing an employee's capacity to work.

As referred to at question 2 above, further restrictions apply to the processing of criminal conviction data. Under the 2018 Act, the processing of criminal conviction data is prohibited unless one or more of the following conditions is satisfied:

- (a) The processing is under the control of an official authority;
- (b) The data subject explicitly consents;
- (c) The processing is necessary and proportionate for the performance of the contract with the data subject;
- (d) The processing is for the purpose of obtaining legal advice or exercising or defending legal rights;
- (e) The processing is necessary to protect the vital interests of the data subject or another person; or
- (f) The processing is otherwise authorized by law.

4. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee's personal data?

The GDPR widens the scope of mandatory information that must be provided to employees to ensure that the processing of their personal data is fair and transparent. Under Article 13 of the GDPR, the data subject must be provided with certain information at the time his/her personal data are collected. In addition, Article 30 obliges the controller to maintain a detailed record of the processing activity. This essentially obliges an employer, as a controller, to provide a privacy statement or notice to all employees/contractors/applicants, etc. when their data are processed. The information to be provided to data subjects must include the following:

- (a) The purpose for processing a data subject's personal data, as well as the legal basis for such processing and any legitimate interest pursued by the controller;
- (b) The fact that a controller intends to transfer personal data to a third country or an international organization;





Ireland

In Detail

- (c) The period for which the data will be stored;
- (d) A statement of the data subject’s right to access and rectify any personal data stored;
- (e) A statement of the data subject’s right to withdraw consent at any time;
- (f) A statement of the data subject’s right to lodge a complaint with a supervisory authority;
- (g) Whether the provision of personal data is a statutory or contractual requirement or obligation, and the consequences of failure to provide such data; and
- (h) Details of automated decision-making, including profiling and logic involved, as well as the significance and consequences of such processing for the data subject.

Where an employer is seeking to rely on its own legitimate interest as the basis for processing, it must be able to demonstrate that their interest in processing the data is not overridden by the rights/interests of the data subject. This balancing exercise should be documented by means of a legitimate interest assessment.

In addition, depending on the scale and nature of the employer’s processing activity, there may also be a mandatory obligation on employers to carry out and document a data protection impact assessment that is intended to identify and mitigate any data protection risks arising from a processing activity that may impact on the data subjects.

5. For how long must an employer retain an employee’s personal data? What is best practice?

The GDPR does not set out specific retention periods for personal data but requires that personal data should be kept for no longer than is necessary for the purposes for which they are processed.

Under the GDPR and associated data protection legislation, employers should determine how long to retain personal data in accordance with other statutory retention periods, limitation periods for legal claims, individual business needs and data quality principles. Best practice will vary according to the nature of the data and purpose for processing. For example, in circumstances where the data may be relevant to defending a claim of breach of contract (which carries a statute of limitation period in Ireland of six years), employee data should be retained for seven years post-termination to allow for an additional year within which the proceedings can be served. In the case of unsuccessful job applicants, records of the recruitment process should only be kept for 12 months after the process has concluded.





Ireland

In Detail

6. What are the legal restrictions on transferring employees' personal data outside your jurisdiction?

The GDPR acknowledges that the transmission of personal data within a group of undertakings for internal administrative purposes, including the processing of employee data, constitutes a legitimate interest of the controller. However, where personal data are being transferred outside of the EEA, certain restrictions apply.

Under the GDPR, an employer, as controller, may only transfer employee personal data to a non-EEA country where one of the following conditions applies:

- (a) The non-EEA country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights. For example, the Privacy Shield certification will usually suffice for transfers to United States-based recipients. However, the legitimacy of the Privacy Shield as a data transfer mechanism is under scrutiny in a legal challenge referred by the Irish courts to the Court of Justice of the European Union.
- (b) Safeguards, such as the model clauses, binding corporate rules, an approved code of conduct or approved certification mechanism, are in place with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.
- (c) The transfer is lawful pursuant to one of the derogations in the GDPR, such as the data subject has given their explicit consent, the transfer is necessary for the performance of a contract, for public interest reasons, authorized by law, necessary for the defense of legal claims, or to protect the vital interests of the data subject.
- (d) Where none of the above safeguards or derogations applies, a transfer to a non-EEA country may take place if the transfer is not repetitive, concerns only a limited number of data subjects, and is necessary for the legitimate interests of the controller which are not overridden by the rights of data subjects. The controller must inform the Data Protection Commission and the data subject of such a transfer, and the legitimate interests pursued.

7. What are the legal restrictions on transferring employees' personal data to a third party?

To ensure that such sharing of information is compatible with fair processing, employers should inform employees that their personal data will be shared with a third party, the purpose for which the data are being shared, and ensure that adequate safeguards are in place to guarantee that the third party also complies with the applicable data protection legislation. As the GDPR is now in operation, this information should typically be found in the employer's privacy notice.





Ireland

In Detail

To ensure the protection of the employees' personal data in this context, the employer should enter into an agreement with the third party, placing obligations on that party to ensure the confidentiality and security of the personal data being shared and further include a commitment from that party to comply with the Irish legislation and the GDPR.

8. What are the consequences of breaching privacy laws in your jurisdiction?

Under the GDPR, there are significant penalties for breach of data protection laws. Depending on the nature of the breach, there are substantial fines for non-compliance with the GDPR:

- (a) Up to 2% of annual worldwide turnover of the preceding financial year or up to EUR 10 million (whichever is greater); and
- (b) Up to 4% of annual worldwide turnover of the preceding financial year or up to EUR 20 million (whichever is greater).

The GDPR and the 2018 Act have enhanced the investigative, corrective, advisory and enforcement powers of the Irish Data Protection Commission.

Under the 2018 Act, a person who obtains or discloses personal data, without authority from the controller or processor, will be guilty of a criminal offense that can give rise to a maximum prison sentence of five years and/or a fine of up to EUR 50,000. Where the offenses are committed by a corporate body, personal liability can attach to the directors/officers of the company.

In addition to the above, there will also be significant reputational risks associated with a perceived or actual failure to comply with data protection requirements. The risk of litigation being brought by data subjects, such as employees, has also substantially increased now that civil actions can be brought for breaches of the GDPR, even where no financial loss has been suffered by the data subject concerned.

9. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee's personal data?

Consent

Employers should be mindful to cease relying on employee consent as a lawful basis for processing personal data (except in cases where explicit consent may be required for the processing of personal data), as the guidance from the





Ireland

In Detail

relevant data protection authorities is that employee consent is inherently unreliable given the imbalance of power in the employee-employer relationship. In particular, the ability of an employee to withdraw consent may pose difficulties in the context of a medical assessment where the relevant health practitioner will refuse to release a report without the consent of the data subject. This may result in an employer being unable to obtain updated medical information on a data subject's capacity to return to work, thereby leaving them with a difficult decision on whether to terminate in the absence of such information.

Data privacy by default and design

The GDPR introduces the concept of data privacy by default and design. This means that employers should ensure they have appropriate technological safeguards in place to ensure any data processed is adequately protected. This will usually require at a minimum restricting access to personal data within a business and employing encryption software and pseudonymization where possible.

Transfer of data to third parties and non-EEA countries

As outlined above, there are heightened obligations on controllers where processing involves the transfer of data to third parties and outside of the EEA (including where this is to an employer group company). Employers must ensure that, where such transfers are taking place, they have identified the purpose for the transfer of such data, the data subjects are informed of the transfer and the process and that the appropriate safeguards are in place to secure the data being transferred.

Data subject access requests

The obligations on employers in responding to a data subject access request have increased under the GDPR. In particular, the time limit for responding to a request has decreased from 40 days to one calendar month (with scope to extend it for an additional two months in the case of a complex request). Perhaps most significant for employers is that a complaint arising from an inadequate response to a data subject access request can give rise to a breach of data protection laws and expose the employer to potential fines/sanctions, including those referred to above.

Demonstrating compliance with the GDPR

The GDPR requires an employer's processing activity to be both fair and transparent. To ensure compliance, employers must ensure they provide data subjects with the information outlined in question 4 above.





 In Brief

 In Detail

Ireland

In Detail

Demonstrating compliance can be a particularly onerous task for employers. It is important that staff are adequately trained on their data protection obligations and that the business has documented legitimate interests assessments and data protection impact assessments (where applicable). By conducting these assessments, it can demonstrate how it balanced the interests of the business against the rights of the data subjects and also identified and mitigated against the risks of infringing the data subjects' rights under data protection legislation.

Contributed by: **Ailbhe Dennehy**, A&L Goodbody

 [Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Israel



Contributed by: **Goldfarb Seligman**



In Brief



In Detail

Contributed by: **Revital Shprung-Levy & Gal Sion, Goldfarb Seligman**



[Link to biography >](#)



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Israel

In Brief

1. Is there a law regulating applicant personal data?

There are various laws regulating applicant personal data. These include the Criminal Register and Rehabilitation Law, 5741-1981, the Genetic Information Law, 5761-2000 and the Equal Opportunities in Employment Law, 5748-1988.

The Guideline 2/2012 – Screening of Job Applicants and the Operation of Screening and Evaluation Centers, which sets out rules regarding screening and evaluation of candidates, also applies.

The Basic Law: Human Dignity and Liberty, 5752-1992; the Protection of Privacy Law, 5741-1981 (the “PPL”) and the regulations promulgated thereunder, and the Guidelines of the Privacy Protection Authority (“PPA”) apply to applicants as well.

2. Is there a law regulating employee personal data?

The Criminal Register and Rehabilitation Law, 5741-1981, the Genetic Information Law, 5761-2000 and the Equal Opportunities in Employment Law, 5748-1988, apply.

The Basic Law: Human Dignity and Liberty, 5752-1992, the PPL and the regulations promulgated thereunder and the Guidelines of the PPA all apply to employees as well.

3. Do I need to have a privacy statement or agreement?

Yes. There are also specific requirements for certain types of data.

4. How long must I retain employee data? What is best practice?

Employee data should only be retained for as long as they are needed for the purpose for which they were collected or as required by law.

5. Can I transfer employee data overseas?

Yes, but consent from the data subjects and a data transfer undertaking from the transferee are required.

6. Can I transfer employee data to a third party?

Yes, subject to consent and outsourcing requirements.

7. What are the consequences of breach?

Criminal penalties, monetary damages and/or administrative fines.

8. What are the main pitfalls?

Failure to comply with the main legal requirements (e.g., consent, proportionality and treatment of special types of data).





Israel

In Detail

1. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant's personal data in your jurisdiction?

Yes. Rules concerning the protection of privacy and data protection of job applicants are dispersed throughout dozens of Israeli statutes. The principal statutes are outlined below:

- The Criminal Register and Rehabilitation Law, 5741-1981 ("**Criminal Register Law**"), provides that accessing or requesting access to an applicant's or employee's criminal records is a criminal offense, even if this was done with the consent of the data subject. It was ruled by the Israel Supreme Court that applicants may be requested to provide a declaration regarding their convictions and outstanding criminal investigations (which may not include criminal records). Such requests should be limited to a list of specific offenses that are relevant to the applicant's future role. The following information may not be requested: investigations that were terminated, convictions that were reversed and any proceedings to which the statute of limitations applies.
- Under the Genetic Information Law, 5761-2000, an employer may not request genetic information from an employee or a job applicant for any purpose, including hiring, employment conditions or dismissal.
- The Equal Opportunities in Employment Law, 5748-1988, provides that an employer is prohibited from discriminating between employees or job candidates due to many matters, including personal information such as pregnancy, fertility treatments and IVF treatments. Moreover, according to this law, the Israel Defense Forces ("**IDF**") profile may not be requested from applicants or employees.
- Guideline 2/2012 – Screening of Job Applicants and the Operation of Screening and Evaluation Centers (the "**Screening Guidelines**"), which was published by the Israel Privacy Protection Authority (formerly known as the Israeli Law, Information and Technology Authority) ("**PPA**"), sets forth the rules for processing job applicants' information in connection with the screening and evaluation process, for example, regarding consent, retention periods, the applicant's access rights and outsourcing.

Israeli courts have set forth various restrictions on employers' use of information collected from candidates for screening and evaluation.

All of the laws, regulations, codes and guidelines set out in question 2 below also apply to job applicants.





Israel

In Detail

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee’s personal data in your jurisdiction?

The laws that govern employee privacy and data protection in Israel are:

- the Basic Law: Human Dignity and Liberty, 5752-1992;
- the Protection of Privacy Law, 5741-1981 (the “**PPL**”) and the regulations promulgated thereunder, especially the Privacy Protection Regulations (Transfer of Data to Databases Abroad), 5761 2001 (“**Data Transfer Regulations**”), and the Privacy Protection Regulations (Data Security), 5777-2017 (“**Data Security Regulations**”); and the guidelines of the PPA.

The draft bill of amendment no. 13 of the PPA has passed its first reading in the Knesset (Israeli Parliament) and is now in preparation for its second and third readings. If the amendment passes these readings it will be published and then enter into force. The most significant change that is relevant to employee data and is introduced in the amendment is an increase in monetary fines for violations to up to NIS 3.2 million.

The Criminal Register Law, the Genetic Information Law, 5761-2000, and the Equal Opportunities in Employment Law 5748-1988, outlined in question 1 above, also apply to employees.

3. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee’s personal data?

Yes. While this requirement is not explicitly set forth in the PPL, the PPA requires employers to have in place consent forms for processing employee personal data. This requirement has also been determined by Israeli courts on several occasions in respect of the use of security cameras, monitoring of computer usage and biometric attendance systems. In respect of computer usage and email communications, the requirement to obtain written consent is also set forth in the Collective Agreement between the Coordinating Bureau of Economic Organizations and the General Federation of Laborers in Israel. The following PPA guidelines set out specific requirements in respect of how employee consent should be obtained and how the applicable policy should be drafted: Guideline 5/2017 – Use of Surveillance Cameras in the Work Place and as part of the Employment Relationship and Guideline 2/2012 – Screening Guidelines.





Israel

In Detail

Consent has to be informed and freely given. The PPL requires that the following will be disclosed when seeking the data subjects' consent: (a) whether there is a legal requirement to provide the information, or if the information is provided at the data subjects' volition; (b) the purpose for which the information is requested; and (c) if the data will be transferred, the transferees of the data and the purpose of the transfer.

4. For how long must an employer retain an employee's personal data? What is best practice?

An employer must limit the retention period to the time that is required for the fulfillment of the purpose for which the data were collected. For example, the Screening Guidelines provide that, absent a legal obligation for a longer retention period or a specific justification arising from the screening process (e.g., for defense against claims in litigation), the employer is required to destroy applicant information (e.g., test scores) if the applicant is not accepted as an employee. Please note that the general statute of limitations in Israel is seven years.

In addition, according to certain specific employee-related laws (such as Work and Rest Hours Law 1951, Wage Protection Law 1958 and Annual Leave Law 1951), an employer is obliged to retain internal records regarding its employees. These records include personal data such as: name, father's name, surname, ID number, work starting date, work hours, weekly rest hours, additional work hours, payment for additional work hours, dates of leave days, payment for leave days, etc.

5. What are the legal restrictions on transferring employees' personal data outside your jurisdiction?

The transfer of personal data abroad is subject to the Data Transfer Regulations, pursuant to which personal data may be transferred abroad only to the extent that:

- (a) the laws of the country to which the data are transferred ensure a level of protection that is no less than the level of protection of data provided for by Israeli Law; or
- (b) one of the following conditions is met:
 - (i) the data subject has consented to the transfer;
 - (ii) the consent of the data subject cannot be obtained and the transfer is vital for the protection of his/her health or physical wellbeing;
 - (iii) the data are transferred to a corporation under the control of the owner of the database from which





Israel

In Detail

the data are transferred, provided that such corporation has guaranteed the protection of privacy after the transfer;

- (iv) the data are transferred to an entity bound by an agreement with the database owner, to comply with the conditions governing the use of the data as applicable under Israeli Laws, *mutatis mutandis*;
- (v) the data were made available to the public or were opened for public inspection by legal authority;
- (vi) the transfer of data is vital for public safety or security;
- (vii) the transfer of data is required by Israeli Law; or
- (viii) the data are transferred to a database in a country:
 - that is a party to the European Convention for the Protection of Individuals with Regard to Automatic Processing of Sensitive Data;
 - that receives data from Member States of the European Community, under the same terms of acceptance; or
 - in relation to which the Registrar of Databases announced, in an announcement published in the Official Gazette, that it has an authority for the protection of privacy, after reaching an arrangement for cooperation with that authority.

When transferring personal data abroad, the database owner is required to enter into a data transfer agreement with the data recipient, pursuant to which the recipient undertakes to apply adequate measures to ensure the privacy of the data subjects and guarantees that the data shall not be further transferred to any third party.

The aforementioned data transfer agreement must also comply with additional restrictions, to the extent that the recipient provides outsourcing services, as set forth in PPA Guideline 2/2011 – Use of Outsourcing Services for Processing Personal Data (“**Outsourcing Guidelines**”) and the Data Security Regulations.





Israel

In Detail

6. What are the legal restrictions on transferring employees' personal data to a third party?

Such a transfer and the processing permitted thereunder must be in accordance with the scope of consent obtained from the employees and with the general principles of privacy protection, i.e., legitimate purpose, purpose limitation, proportionality and transparency.

Retaining outsourcing services for the processing of personal information is subject to the Outsourcing Guidelines. The Outsourcing Guidelines include, *inter alia*, factors to be taken into consideration when deciding to use outsourcing services, specific provisions to be included within the data transfer agreement and data security requirements. The Data Security Regulations provide additional requirements such as performing a risk assessment and defining the following in the outsourcing agreement: the data that may be processed and the permitted processing purposes, the permitted processing activities and the database systems that the transferee may access.

7. What are the consequences of breaching privacy laws in your jurisdiction?

Violations of the PPL may result in criminal penalties (one to five years' imprisonment) and/or monetary damages:

- (a) violation of the restriction on requesting an applicant's or employee's IDF profile may result in criminal fines (this option is rarely applied) and/or administrative fines;
- (b) violation of the restriction on requesting an applicant's or employee's criminal records may result in criminal penalties (one to two years' imprisonment); and
- (c) violation of the restriction on requesting an applicant's or employee's genetic information may result in criminal penalties (six months to one year of imprisonment or a fine that is rarely applied) and/or administrative fines.

There are statutory damages of up to NIS 50,000, which can be increased to NIS 100,000 if it is established that the defendant intended to harm the data subjects. The court may award statutory damages without evidence of actual damages. As these amounts are not caps, larger amounts may be awarded if the plaintiff can establish in evidence that the actual damages were greater than the statutory damages. Except in severe circumstances, criminal offenses usually result in administrative fines. The PPA may also order that data will be destroyed.

Material obtained in violation of the PPL is deemed as inadmissible evidence.





Israel

In Detail

8. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee's personal data?

The pitfalls primarily consist of failure to comply with legal requirements, such as:

- Purpose and proportionality principles: use and processing of personal data should be only for the purposes for which the data were obtained (including those set forth in the applicable privacy statement/agreement) by applying a test of reasonableness of measure and good faith.
- Failure to comply with the requirements for obtaining consent of the data subjects in an adequate manner.
- Processing special types of information without complying with the specific rules that apply to such processing (e.g., biometric, security cameras, use of computers and location data).
- Collection of data that may give rise to claims of discrimination (e.g., personal status, age, religion).

Contributed by: **Revital Shprung-Levy & Gal Sion**, Goldfarb Seligman



[Link to biography >](#)



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Italy

Contributed by: **Quorum Studio Legale e Tributario Associato**



In Brief



In Detail

Contributed by: **Francesco D'Amora**, Quorum Studio Legale e Tributario Associato



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Italy

In Brief

1. Does employee data privacy law in your jurisdiction go beyond the GDPR?

No.

2. Is there a law regulating applicant personal data?

Aside from the general provisions of the GDPR, there is no specific law regulating applicant personal data.

3 Is there a law regulating employee personal data?

Aside from the general provisions of the GDPR, the Italian Data Protection Code provides general rules for personal data processing, including employee data.

4. Do I need to have a privacy statement or agreement?

Yes, under Italian law, a privacy statement is needed for legal data processing.

5. How long must I retain employee data? What is best practice?

It may be possible to keep data for five or ten years, depending on the purpose for retention.

6. Can I transfer employee data overseas?

Yes, subject to the requirements of the GDPR.

7. Can I transfer employee data to a third party?

Yes, subject to the requirements of the GDPR.

8. What are the consequences of breach?

The majority of breaches are punished with fines but, in some cases, breaches may have criminal consequences.

9. What are the main pitfalls?

Information obtained through illegal means cannot be used in trials. Sensitive data processing may also be risky. Providing inadequate information to data subjects and processing data without proper consent are also common pitfalls.





Italy

In Detail

1. To what extent does employee data privacy law in your jurisdiction go beyond the GDPR?

The Italian Data Protection Code (L. decree of June 30, 2003 no. 196) (“**Italian Data Protection Code**”) does not go beyond the GDPR. Nevertheless, the Italian Parliament is working on a new privacy law draft that is likely to go beyond the GDPR provisions.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant’s personal data in your jurisdiction?

No, applicants’ personal data are subject to general data protection provisions, including under the GDPR.

3. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee’s personal data in your jurisdiction?

Yes, the Italian Data Protection Code provides general rules for personal data processing, including employees’ data. The Italian Data Protection Authority’s Deliberation of December 7, 2006 no. 53 provides a set of specific mandatory rules for employees’ personal data. In addition, Law 300/1970 provides for special restrictions on employer investigation rights. As noted above, the Italian Parliament is working on a new privacy law draft. The GDPR also applies to employees’ personal data processing in Italy.

4. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee’s personal data?

Yes, under Italian law, a personal information collection statement must be provided to the employee before processing starts. Pursuant to the GDPR, such document must include mandatory information. Further, the employee must give his/her specific consent to the data processing unless another ground under Article 6 applies (e.g., processing is necessary for compliance with a legal obligation, to protect the vital interests of the data subject or for the performance of a task carried out in the public interest).

In the case of sensitive data processing, this can be done with the employee’s explicit consent.



HOME

GDPR
OVERVIEW

COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Italy

In Detail

5. For how long must an employer retain an employee's personal data? What is best practice?

As a general principle set forth in the Italian Data Protection Code and in the GDPR, data may be kept for no longer than is necessary for the purposes for which the personal data were collected/processed. The data must then be deleted or made unavailable (or anonymized), unless a different provision of the law has different requirements for retaining the document containing the data.

Generally, the employer retains data for as long as they are necessary to prove wage payments, which could be five or ten years but potentially longer if a lawsuit is pending.

6. What are the legal restrictions on transferring employees' personal data outside your jurisdiction?

Pursuant to the GDPR, it is possible to transfer employees' personal data within the EU/EEA. Transmission to third countries or to an international organization shall take place only on the basis of an adequacy decision, if the transfer is subject to appropriate safeguards or if other mechanisms, such as binding corporate rules, exist.

7. What are the legal restrictions on transferring employees' personal data to a third party?

Employee's personal data may be disclosed to third parties if the disclosure was previously and clearly described with the information notice submitted to employees. Processing is lawful only if and to the extent that at least one of the following applies:

- (a) the data subject has given consent to the processing of his/her personal data for one or more specific purposes;
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- (e) 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 controller;





Italy

In Detail

- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

If employees' personal data will be shared with a processor (e.g., a payroll provider), a data processing agreement should be entered into, meeting the requirements of Article 28 of the GDPR.

8. What are the consequences of breaching privacy laws in your jurisdiction?

There are several consequences. Fines are provided by the GDPR: they go from a minimum of up to EUR 10 million or, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher, to up to EUR 20 million or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Under the Italian Data Protection Code, a civil sanction (compensation for the so-called "damage arising from processing of personal data") may be imposed by the competent authority, such as a "criminal condemnation" (up to three years' imprisonment).

9. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee's personal data?

In general, it must be taken into consideration that breach of any privacy rule is the first ground on which Italian employees usually base their claims within the labor relationship.

Processing employees' sensitive (and, in particular, health) data and/or judicial data is an issue of particular risk.

Providing inadequate information to data subjects and carrying out data processing without proper consent are also common pitfalls.

Contributed by: **Francesco D'Amora**, Quorum Studio Legale e Tributario Associato

[HOME](#)[GDPR
OVERVIEW](#)[COUNTRIES](#)[DIRECTORY](#)

August 2018

SCROLL DOWN



Netherlands



Contributed by: **Loyens & Loeff**



In Brief



In Detail

Contributed by: **Hermine Voûte**, Loyens & Loeff



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Netherlands

In Brief

1. Does employee data privacy law in your jurisdiction go beyond the GDPR?

No.

2. Is there a law regulating applicant personal data?

The GDPR.

3. Is there a law regulating employee personal data?

The GDPR.

4. Do I need to have a privacy statement or agreement?

The GDPR requires that an employer provides specific information to its employees in relation to its collection of their personal data.

5. How long must I retain employee data? What is best practice?

The general rule is that data cannot be retained for longer than necessary in relation to the purposes for which they were collected. There are certain statutory retention periods for HR matters. The old Exemption Decree, which was abolished due to the entry into force of the GDPR, provides rules of thumb.

6. Can I transfer employee data overseas?

Under the GDPR, as a general rule, transfers of personal data to EEA countries are allowed.

Transfer of personal data to countries outside the EEA may take place if these countries have an “adequate” level of data protection or if the controller or processor exporting the data has itself provided for “appropriate safeguards.”

7. Can I transfer employee data to a third party?

The GDPR requires that an employer concludes a data processing agreement in case the third party can be considered a processor.

8. What are the consequences of breach?

Potentially significant administrative fines. Other consequences could be a complaint to a supervisory authority or liability for damages.

9. What are the main pitfalls?

First, the employee’s consent in principle does not provide a legal ground for data processing due to the imbalance of power in the employer-employee relationship. Secondly, all policies that concern the processing of employee data are subject to the works council’s consent. Thirdly, employers should be aware that data transfers to other group companies, e.g., parent companies, require a separate legal ground. Lastly, employers should be aware that, as of January 1, 2016, data controllers (e.g., employers) are required to notify the Dutch Data Protection Authority within 72 hours of any data security breaches that have or are likely to have serious adverse consequences for the protection of personal data.





Netherlands

In Detail

1. To what extent does employee data privacy law in your jurisdiction go beyond the GDPR?

The Dutch legislator is currently not using the room that the GDPR provides to introduce country specific rules for processing of personal data in the employment context (Article 88 of the GDPR). The Dutch legislator has decided to maintain the data privacy regime that was applicable before the GDPR entered into force as much as possible. The Minister for Legal Protection announced that he intends to submit a proposal with regard to data protection in the employment context for consultation in 2019.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant's personal data in your jurisdiction?

This topic is covered mainly by the GDPR. There are some other acts that touch upon this topic.

For instance, the Medical Examinations Act deals with pre-employment medical examinations. Under the Medical Examinations Act, pre-employment medical examinations may only be carried out with regard to functions for which special medical requirements or safeguards are required.

Another example is the Justice System Data Act, which deals with the certificate of conduct (in Dutch, *Verklaring omtrent gedrag* ("VOG")). Where it is necessary for a certain position that an employer is aware of the applicant's criminal background (e.g., a job involving confidential information, vulnerable people, or handling the employer's money), an employer can ask job applicants for the VOG. The VOG is a statement by which the Dutch Minister of Security and Justice declares that, following an investigation with respect to the behavior of the person concerned, he/she did not commit any criminal offenses that are relevant to the position for which the VOG has been requested. The VOG does not contain any other information. The VOG will be issued if the individual has no criminal record. If the individual does have a criminal record, the authorities will decide whether the offenses in question are relevant for the position concerned. For example, criminal offenses that are relevant to the teaching profession do not have to be relevant to the function of accountant. The application for a VOG is submitted by the applicant and so his/her cooperation is required. For some jobs, such as teachers and taxi drivers, the certificate is required by law. For positions for which a VOG is not a legal requirement, the employer can nonetheless request a VOG, provided that the request for the VOG is in line with the GDPR.





Netherlands

In Detail

The Dutch Association for Personnel Management and Organizational Development (“NVP”) has drawn up a code together with the Labor Foundation (*Stichting van de Arbeid*) that provides a standard for a transparent and fair selection procedure. The latest English version of the NVP Recruitment Code dates from June 2017 and is available on the NVP website: <https://nvp-plaza.nl/download/?id=7714>

3. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee’s personal data in your jurisdiction?

This topic is mainly covered by the GDPR. Please see also the response to question 1.

4. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee’s personal data?

The GDPR requires that an employer provides specific information to its employees in relation to its collection of their personal data, setting out which personal data are collected, what the legal grounds for the data processing are, for what purposes the data are collected and processed, how long the data are stored, etc. This document is subject to the consent of the works council. Most companies with more than 50 employees in the Netherlands are obliged to have a works council as a form of employee representation.

5. For how long must an employer retain an employee’s personal data? What is best practice?

For some data, such as data included in an employee file, there are no statutory retention periods. For these data, the rules as prescribed in the GDPR apply. The GDPR does not include specific retention periods, but stipulates that data cannot be retained for longer than necessary in relation to the purposes for which they were collected.

With the implementation of the GDPR as of May 25, 2018, the Dutch Data Protection Act (*Wet bescherming persoonsgegevens*) (“DPA”) has been abolished. As a result, the Exemption Decree, which was linked to the DPA, is also no longer applicable. The Exemption Decree included guidelines with respect to retention periods. So, in principle, the guidelines with regard to retention periods as stipulated in the Exemption Decree DPA can no longer be used. However, the general principles as stipulated in the GDPR will be the same as under the DPA, namely that personal data may not be retained for longer than necessary in relation to the purposes for which they were collected. Taking the aforementioned into account, we assume that the guidelines as indicated in the Exemption Decree DPA may still be used now that the GDPR has entered into force.





Netherlands

In Detail

Statutory retention periods

Data	Retention period	Trigger event	Legislation
Payroll records, including administration of wages, tax and social security records, wages earned, social security withheld, wage withholding tax, pay slips, overtime compensation, bonuses, expenses	Min. seven years	The year following the financial year to which the data relate	Section 28 Wages and Salaries Tax Act 1964 (<i>Wet op de Loonbelasting 1964</i>) Section 52(4) State Taxes Act (<i>Algemene wet inzake rijksbelastingen</i>)
Identification documents, including those of foreign nationals (copy)	Min. five years	After the employment ends	Section 15(4) Foreign Nationals (Employment) Act (<i>Wet arbeid vreemdelingen</i>) Sector 7.5 (4) Implementing Regulations to the Wages and Salaries Tax (<i>Uitvoeringsregeling Loonbelasting</i>)
Data and documents concerning pension schemes and related subjects	Min. seven years	The year following the financial year to which the data relate	Section 169 Pensions Act (<i>Pensioenwet</i>) Section 164 Occupational Pension Scheme (Obligatory Membership)





Netherlands

In Detail

Retention periods from the abolished Exemption Decree

Data	Retention period	Trigger event	Legislation
Data of (rejected) job applicants, including application letters, CVs, references, certificates of good conduct, job interview notes, assessment and/or psychological test results	Max. four weeks Max. one year with consent of the data subject	From the date the application procedure ends	Section 5 Exemption Decree DPA
Employment agreement, on-boarding documents, such as collection of personal information, bank account information, etc.	Max. two years – the data may, however, be kept for longer in cases where this would be necessary to fulfill other legal retention duties NB: If needed, the data may be retained for longer to uphold a legitimate interest, for instance in the event of a (possible) court proceeding. In such an event, it is advisable to retain the relevant data for a period of five years as employees in principle can claim entitlements for a period of five years.	Once the employment ends	Section 7 Exemption Decree DPA





Netherlands

In Detail

Reports on employee performance review meetings and assessment interviews and career counselling (e.g., evaluations, copies of academic or other training received, appraisals, promotions and demotions, sick leave reports)	Max. two years –the data may, however, be kept for longer in cases where this would be necessary to fulfill other legal retention duties	Once the employment ends	Section 7 Exemption Decree DPA
Data and documents concerning pension schemes and related subjects	Max. two years – the data may, however, be kept for longer in cases where this would be necessary to fulfill other legal retention duties NB: If needed, the data may be retained longer to uphold a legitimate interest for instance, in the event of a (possible) court proceeding. In such an event, it is advisable to retain the relevant data for a period of 20 years.	After the entitlement to a pension or benefit in connection with early retirement has ended	Section 10 Exemption Decree DPA NB: Pension and related subjects as mentioned in the Exemption Decree DPA mainly concern data about the calculation of pensions etc. The data as mentioned in the Pensions Act concerns the amounts of pensions etc. that have been paid. This distinction is relevant for the data retention period (which is different under both Acts).





Netherlands

In Detail

6. What are the legal restrictions on transferring employees' personal data outside your jurisdiction?

EEA countries

There are no specific requirements for transfers of personal data to EEA countries (i.e., the EU countries, plus Iceland, Liechtenstein and Norway).

Countries with an adequate level of protection

Under the GDPR, as a general rule, transfers of personal data to countries outside the EEA may take place if these countries ensure an “adequate” level of data protection. Third countries’ level of personal data protection is assessed by the European Commission through “adequacy findings,” which are binding in their entirety on all Member States. Once the “adequacy” of a third country has been recognized, personal data can be transferred to this country without having to take further protective measures. The rules that follow from the GDPR, however, apply unimpaired.

A novelty in the GDPR with respect to adequacy decisions is that they are subject to periodic review, at least every four years, taking into account all relevant developments in the relevant third country. The GDPR furthermore obliges the European Commission to monitor on an ongoing basis developments that could affect the proper functioning of existing adequacy decisions. The GDPR has also introduced the possibility of adequacy decisions being repealed, amended or suspended.

Countries without an adequacy decision

In the absence of an adequacy decision, personal data may in principle only be transferred to third countries (a) if the controller or processor exporting the data has itself provided for “appropriate safeguards” and (b) on the condition that enforceable data subject rights and effective legal remedies are available in the given country.

The most relevant “appropriate safeguards” are the following:

- binding corporate rules
- standard contractual clauses
- approved codes of conduct/certification mechanisms





Netherlands

In Detail

Exceptions/derogations for specific situations

In the absence of either an adequacy decision or the implementation of “appropriate” safeguards as listed above, a cross-border transfer may only take place in one of the following cases:

- the data subject has explicitly consented to the proposed transfer, after having been duly informed (and of the possible risks);
- the transfer is necessary for the performance of a contract;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defense of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons (where the data subject is incapable of giving consent);
- under certain conditions, when the transfer is made from a register that is intended to provide information to the public; or
- only if none of the other derogations listed above can be applied (and provided that the supervisory authority is informed of the transfer): if the transfer (a) is not repetitive, (b) concerns only a limited number of data subjects, (c) is necessary for the purposes of compelling legitimate interests pursued by the controller that are not overridden by the interests or rights and freedoms of the data subject and (d) the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data.

Transfers not authorized by EU law

Finally, the GDPR expressly confirms that, if no other legal ground is available, any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognized or enforceable if based on an international agreement (such as a mutual legal assistance treaty) in force between the requesting third country and the EU or a Member State. The exact scope of this provision still needs to be further clarified, but already promises to lead to an interesting debate.





Netherlands

In Detail

7. What are the legal restrictions on transferring employees' personal data to a third party?

Apart from the legal restrictions described in the answer to question 6, the GDPR requires that an employer concludes a data processing agreement in case the third party can be considered a processor. Note that third-party service providers, e.g., payroll administrators, are considered processors and must therefore comply with certain obligations under the GDPR and enter into data processing agreements.

8. What are the consequences of breaching privacy laws in your jurisdiction?

Administrative fines

One of the most discussed topics relating to the GDPR is the administrative fines that may be imposed by a supervisory authority in the event of non-compliance with the GDPR and not without reason. The administrative fines that may possibly be imposed are substantial.

Administrative fines may, depending on the infringed provision of the GDPR, amount to a maximum of EUR 20 million, or, if this is a higher amount, 4% of the total worldwide annual turnover of the preceding financial year of an organization. Such fines may be imposed on both the controller and the processor.

For example, a violation of requirements governing privacy by design and default is subject to a maximum fine of EUR 10 million or 2% of the total worldwide annual turnover. Violating the basic principles for processing, including the conditions for obtaining valid consent, as well as non-compliance with a supervisory authority's order, may result in the highest fine of EUR 20 million or 4% of the total worldwide annual turnover.

Fortunately, not all infringements of the GDPR will lead to those serious fines. Besides the power to impose administrative fines as described above, a supervisory authority also has the (corrective) power to (among others) issue warnings, reprimands and orders. When imposing an administrative fine, in addition to or instead of its other corrective powers, a supervisory authority is obliged to take into account the specifics of the case at hand. What exact fine will be imposed depends on (among others) the nature, gravity and duration, as well as the intentional or negligent character of the infringement. In short, the supervisory authority must ensure that the imposition of administrative fines is in each specific case effective, proportionate and dissuasive. The supervisory authorities are allowed to decide on their enforcement policy within the boundaries of the GDPR.





Netherlands

In Detail

A data subject's right to lodge a complaint and to an effective judicial remedy

Further, the GDPR provides data subjects with the explicit right to lodge a complaint with a supervisory authority, if they consider that any processing of their personal data infringes the requirements of the GDPR. Controllers are even obliged to explicitly inform the data subjects of this right.

Further to a complaint, a supervisory authority may decide to further investigate the company's processing activities (the scope of such an investigation may be broader than the complaint lodged). In the event that a supervisory authority does not inform a data subject of the progress or outcome of a complaint lodged within three months, a data subject shall have the right to an effective judicial remedy. Each data subject shall have the right to an effective judicial remedy against a controller or processor where he/she considers that his/her rights under the GDPR have been infringed.

In this respect, it should be pointed out that if a court of a Member State is addressed by a data subject regarding the non-compliant processing activities of a controller or processor and such court has information that proceedings concerning processing activities of the same controller or processor are already pending before a court in another Member State, the court that was addressed second may suspend its proceeding. Such court may also, if the proceedings are pending at the first instance, on request of one of the parties (for example, the controller) decline jurisdiction, but only to the extent that the first court seized has jurisdiction over both actions and its law permits consolidation of the proceedings.

Liability for damages

The GDPR also gives data subjects the right to compensation of any material and/or non-material damages resulting from an infringement of the GDPR.

Both controllers and processors are liable for any damages resulting from an infringement of the GDPR. However, processors shall only be liable for damages that are caused as a result of the processor's actions that were contrary to the controllers' instructions or a breach of the GDPR requirements particularly addressing processors, such as the data security obligations. A controller or processor will be exempted from liability if it can prove not to be in any way responsible for the event causing the damage.

The GDPR explicitly indicates that data subjects are entitled to have their rights to lodge a complaint or to claim damages exercised by a not-for-profit body, organization or association on their behalf. This opens the door for "mass-claims" in case of large-scale infringements.





Netherlands

In Detail

9. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee's personal data?

First, the employee's consent in principle does not provide a legal ground for data processing, because a genuine free choice is hardly ever present in an employee-employer relationship.

Secondly, employers in the Netherlands must take into account the works council's right to consent to any implementation, amendment or withdrawal of policies regarding the processing of employee data by the employer. Employers should therefore be aware that policies in that respect, such as an employee privacy policy, an acceptable use policy, a data breach policy or a retention policy, must not only comply with the GDPR's requirements but must also be consented to by the works council, prior to their implementation. All policies that concern the processing of employee data are therefore subject to the works council's consent.

Thirdly, employers should be aware that data transfers to other group companies, e.g., parent companies, require a separate legal ground.

Lastly, employers should be aware that as of January 1, 2016, data controllers (e.g., employers) are required to notify the Dutch Data Protection Agency within 72 hours of any data security breaches that have or are likely to have serious adverse consequences for the protection of personal data.=

Contributed by: **Hermine Voûte**, Loyens & Loeff



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Norway

Contributed by: **Advokatfirmaet Thommessen AS**



In Brief



In Detail

Contributed by: **Christopher Sparre-Enger Clausen**, Advokatfirmaet Thommessen AS



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Norway

In Brief

1. Does employee data privacy law in your jurisdiction go beyond the GDPR?

As Norway is a member of the European Free Trade Association (“EFTA”) and the EEA (but not the EU), the GDPR does not apply directly, but must be implemented through national legislation. The GDPR came into force in Norway on July 20, 2018. The national legislation contains derogations from the GDPR in certain areas.

2. Is there a law regulating applicant personal data?

Yes, in addition to the general provisions in the Personal Data Act and the GDPR, both the Working Environment Act and the Equality and Anti-Discrimination Act contain provisions limiting which personal data an employer may collect in a recruitment process. Further, there are limitations as to when an employer may obtain police certificates from applicants and employees.

3. Is there a law regulating employee personal data?

Yes, in addition to the general provisions in the Personal Data Act and the GDPR, the Working Environment Act contains provisions limiting which employee personal data an employer may collect and use.

4. Do I need to have a privacy statement or agreement?

Pursuant to Article 13 (and, where applicable, Article 14) of the GDPR, the employer must provide the employees with information concerning its processing of their personal data.

5. How long must I retain employee data? What is best practice?

There are legal obligations in the Bookkeeping Act obliging employers to retain certain employee data. The Working Environment Act also includes provisions obliging employers to keep records of sickness and accidents related to the workplace.

Best practice depends on which types of personal data are processed.

6. Can I transfer employee data overseas?

Yes, subject to the requirements of the GDPR.

7. Can I transfer employee data to a third party?

Yes, subject to the requirements of the GDPR.

8. What are the consequences of breach?

Administrative fines, orders, coercive fines and liability to pay compensation to data subjects.

Depending on the breach, a controller may also be obliged to notify the Norwegian Data Protection Authority and/or the data subjects of the breach.

9. What are the main pitfalls?

The main pitfalls are lack of legal basis for processing personal data, insufficient information provided to the data subjects, insufficient deletion/retention routines and practices and transfer of personal data made outside of the EU/EEA without complying with Articles 44-49 of the GDPR. Further, local derogations on employer’s access to employees’ email accounts, etc. are common pitfalls.





Norway

In Detail

1. To what extent does employee data privacy law in your jurisdiction go beyond the GDPR?

As Norway is a member of the European Free Trade Association (“EFTA”) and the EEA (but not the EU), the GDPR does not apply directly, but must be implemented through national legislation. The GDPR came into force on July 20, 2018.

The national legislation deviates and goes beyond the GDPR on a number of subjects. In relation to employees, the most noticeable deviations are the additional requirements for use of CCTV in the workplace, the additional requirements for use of control measures, restrictions on which personal data may be processed in relation to job candidates and employers’ access to employees’ email accounts, work computers, private area on the company’s server, and any other electronic equipment that the employer has provided to the employees for use in their work (e.g., mobile phones).

Use of CCTV in the workplace

If an employer would like to monitor a workplace using CCTV, there are additional requirements that must be met. First, the use of CCTV in the workplace, to which only a limited amount of people have access, is only allowed if it is necessary to prevent dangerous situations, ensure the interest or security of employees and others or there is another particular reason for the monitoring. The assessment must be made taking into consideration the type of business in question (e.g., a bank would be more likely to fulfill the additional requirements than a grocery shop or office location). Further, there are requirements to put up signs with warnings of the use of CCTV, which also provide information about the identity of the controller. There are also limitations on sharing the recordings and on the retention period of the recordings (usually no more than one week). The provisions for CCTV are located in the Regulation on Camera Surveillance in the Business.

When implementing control measures on employees (e.g., monitoring through the use of CCTV or the use of access control), the employer must have a valid reason for wanting to implement the control measure, discuss the need, use and purpose with the employees’ representatives and inform the affected employees.

Access to employees’ email accounts, etc.

An employer may only access employees’ email accounts, work computers, private area on the company’s server and any other electronic equipment that the employer has provided to the employees for use in their work (e.g., mobile phones), if:

- (a) the access is necessary to maintain the daily operations or ensure other legitimate interests of the business; or





Norway

In Detail

(b) there is a reasonable suspicion that the employee has used his/her email account or equipment in a way that constitutes a serious breach of the duties arising from the employment or that may constitute grounds for termination or summary dismissal.

Before accessing the above mentioned accounts/equipment, an employer must normally notify the employee prior to the access, give him/her the opportunity to give his/her views on the access and to be present at the time of the access. If the employee wants, he/she is also entitled to bring a counsel or employee representative.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant's personal data in your jurisdiction?

Yes, in addition to the general provisions in the Personal Data Act and the GDPR, both the Working Environment Act and the Equality and Anti-Discrimination Act have provisions limiting which personal data an employer may collect in a recruitment process. Among others, the provisions prevent an employer from collecting information about an applicant's pregnancy or plans to have or adopt children, religion or beliefs, ethnicity, disability, sexual orientation, gender identity or gender expression. Additionally, there are restrictions on the collection of health data and the use of medical examinations concerning applicants and employees.

There are several exceptions to the above. An employer may, for instance, make use of medical examinations where it is permissible by law or where the applicant is applying for a position that includes a particular risk for the safety of the applicant or others.

With regard to collecting police certificates, such documents are obtained by candidates in Norway, and the police will only provide the candidates with police certificates when applying for certain positions (e.g., a management position in a financial institution).

There are no provisions in national legislation restricting the transfer of applicant data overseas and/or to third parties. When transferring applicant data overseas and/or to third parties, the transferring entity must ensure that the general requirements under the GDPR are met. Among others, this includes ensuring a sufficient legal basis and transfer basis where required (please see our answers to question 6 and 7 below), that the transfer is in compliance with the principle of purpose limitation (that personal data collected for one purpose should not be used for another purpose incompatible with the original purpose) and that the applicants receive sufficient information about the transferring.





Norway

In Detail

3. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee's personal data in your jurisdiction?

Yes, please see our answer to question 2 above. The restrictions on the collection of health data and the use of medical examinations also apply for employees. In addition, the use of medical examinations will most likely be considered a control measure directed towards employees with the additional requirements this would impose (please see our answer to question 1 above).

4. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee's personal data?

Articles 13 and 14 of the GDPR require employers to provide specific information to employees about the collection and processing of their personal data. As long as the information is provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language, there are no particular requirements as to how employers make such information available to its employees. Normally, the employers establish a privacy policy for employees that they make available on the intranet or in the employee manual. Some employers also include a reference to the privacy policy in the employment agreement.

5. For how long must an employer retain an employee's personal data? What is best practice?

The general requirement is that the personal data must be deleted when they are no longer necessary for the purpose for which they were collected. In certain circumstances, an employer must retain the employee's personal data to comply with legal obligations, e.g., the provisions in the Bookkeeping Act. Among others, an employer is obliged to retain the employees' employment agreements (three years and six months), salary details (five years) and coverage of travel expenses (five years).

Best practice depends on which types of personal data are processed. Some of the general HR data may be processed for the duration of the employment, while police certificates, warnings, performance data, background checks, medical examinations, etc. should be retained for a more limited time.





Norway

In Detail

6. What are the legal restrictions on transferring employees' personal data outside your jurisdiction?

The transfer of employees' personal data outside Norway requires a legal basis in Article 6 of the GDPR. If the personal data transferred are special categories of personal data, additional requirements apply under Article 9 of the GDPR.

If the personal data are transferred outside of the EU/EEA, employers must also ensure that they have a basis for the transfer under Articles 44-49 of the GDPR. These include:

- an adequacy decision by the EU Commission, approving the level of data privacy offered by the non-EU/EEA state;
- the receiving party has certified that it follows the EU-US Privacy Shield and that the personal data are covered by the certification (where the receiving entity is located in the United States);
- appropriate safeguards, such as binding corporate rules (intra-company rules that require the entities in a group to ensure a satisfactory level of data privacy by obliging them to follow certain provisions of the GDPR); or
- derogations for special circumstances.

7. What are the legal restrictions on transferring employees' personal data to a third party?

The transfer of employee data to a third party is considered processing of personal data that requires a legal basis. If the personal data processed are considered to be special categories of personal data, additional requirements apply. If the employee data are transferred outside of the EU/EEA, employers must also ensure that they have a legal basis for the transfer as set out in Articles 44-49 in the GDPR (please see our answer to question 6 above).

If the third party receiving the personal data merely processes the data on the employer's behalf, the employer must also enter into a data processor agreement with the third party prior to transferring the personal data. The requirements for a data processor agreement are set out in Article 28 of the GDPR.





Norway

In Detail

8. What are the consequences of breaching privacy laws in your jurisdiction?

In accordance with Article 83 of the GDPR and the Personal Data Act, the Norwegian Data Protection Authority (“NDPA”) may issue administrative fines for breaching the GDPR. Depending on the nature of the breach, there are substantial fines for non-compliance with the GDPR:

- (a) Up to EUR 10 million or, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher; and
- (b) Up to EUR 20 million, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Additionally, the NDPA may issue orders and, in cases where entities do not comply with issued orders, coercive fines. Breaches may also make controllers and/or processors liable to pay compensation for economic and non-economic damages. Although the NDPA has avoided large administrative fines so far, it is believed that the NDPA will increase its levels of fines due to influence from other supervisory authorities and the European Data Protection Board.

Depending on the breach, a controller may also be obliged to notify the NDPA and/or the data subjects of the breach (e.g., where personal data have been disclosed to an outside party and the disclosure constitutes a high risk to the rights and freedoms of natural persons).

9. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee’s personal data?

The main pitfalls are processing personal data without a legal basis, not providing information to data subjects and transferring personal data outside of the EU/EEA without complying with Articles 44-49 of the GDPR. Further, local legislation adding additional requirements is likely to be a major pitfall for international employers without local HR (e.g., non-compliance with material and procedural requirements when accessing employees’ email accounts, etc., when implementing control measures or when using CCTV in the workplace).

Contributed by: **Christopher Sparre-Enger Clausen**, Advokatfirmaet Thommessen AS



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Poland



SOŁTYSIŃSKI
KAWECKI
SZLĘZAK

Contributed by: **Sołtysiński Kawecki & Szlęzak**

 In Brief

 In Detail

Contributed by: **Agata Szeliga & Katarzyna Paziewska**, Sołtysiński Kawecki & Szlęzak



[Link to biography >](#)



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 

Poland

In Brief

1. Does employee data privacy law in your jurisdiction go beyond the GDPR?

On May 25, 2018, regulations on employee monitoring in the workplace came into force in Poland. Apart from these regulations, there is currently no employee data privacy law that goes beyond the GDPR, although specific regulations on employee data privacy are expected soon.

The Polish government is working on an Act Implementing the Act on the Protection of Personal Data (“**Amending Act**”), which will amend numerous sector-specific provisions on personal data protection, including the Act of June 26, 1974, the Labor Code, which includes regulations on employee privacy. Work on the Amending Act is still in progress. On August 23, 2018, the Council of Ministers adopted the draft which will now be reviewed by the Parliament. Based on the latest draft dated June 15, 2018, it is likely that this Act will implement additional protection for employee personal data.

2. Is there a law regulating applicant personal data?

Yes, the Act of June 26, 1974, the Labor Code and the GDPR.

3. Is there a law regulating employee personal data?

Yes, the Act of June 26, 1974, the Labor Code and the GDPR.

4. Do I need to have a privacy statement or agreement?

There is no obligation to have a separate privacy statement or agreement in Poland; however, employers must inform employees about processing of their personal data under the GDPR.

5. How long must I retain employee data? What is best practice?

In Poland, an employer could, in principle, retain an employee’s personal data for a period of 50 years after

termination of the employment contract, depending on the nature of the data. However, a new law on the retention of personal documentation is scheduled to come into force on January 1, 2019, providing for a shorter retention period under specific circumstances.

6. Can I transfer employee data overseas?

As a general rule under the GDPR, a transfer of employee personal data to a third country (outside the EEA) may take place only if that country ensures an adequate level of personal data protection or there are appropriate safeguards.

7. Can I transfer employee data to a third party?

Employee personal data may be transferred to a third party, subject to the requirements of the GDPR.

8. What are the consequences of breach?

Under the GDPR, a breach may give rise to a financial penalty, imposed by the Polish Data Protection Authority. Additionally, any person who has suffered damage as a result of an infringement has the right to receive compensation for the damage suffered. Criminal liability may also arise under the Polish Act on Personal Data Protection.

9. What are the main pitfalls?

Applicants often provide, on their own initiative, additional data (which is outside the scope of data specified in the Labor Code), such as images or personal interests, to employers. If the employer has not obtained applicant consent to process such additional data, there is no legal basis for such processing.

Employers belonging to an international group of companies that transfer employee personal data to their affiliates should check if they have a legal basis for such transfers and comply with the GDPR provisions on transfer to third countries.



Poland

In Detail

1. To what extent does employee data privacy law in your jurisdiction go beyond the GDPR?

A new regulation on monitoring employees in the workplace came into force on May 25, 2018. Pursuant to the new provisions of the Labor Code, an employer is entitled to implement video monitoring, email monitoring and other forms of monitoring of employees. The regulations on monitoring are quite detailed as they specify, for instance, the purposes of monitoring, the area that can be monitored (in the case of video monitoring), the retention period, and certain formal conditions that must be met by the employer before monitoring starts, e.g., the way in which employees should be notified of such monitoring.

Pursuant to the expected changes to employee data privacy law, arising from the draft Act Implementing the Act on the Protection of Personal Data ("**Amending Act**"):

- The scope of personal data that an employer may request from an applicant or employee will be rigidly defined;
- An employer will be able to request that an applicant provide certain details, e.g., name and surname, date of birth, contact details, education, qualification and work experience. Information concerning education, qualification and work experience can be requested only if necessary for the job position;
- An employer may also request from an employee the place of residence, "PESEL" number (Polish identification number), or if the employee has no such number, type and number of ID, and other personal data, including personal data of the employee's children and other family members, if providing such data is necessary due to the employee's special rights provided for under the labor law;
- An employer will be able to demand from an applicant or employee the provision of personal data other than that specified above, which is necessary to fulfill the employer's obligation under the law; in addition, other data may also be made available to the employer upon the consent of the applicant or employee; and
- Lack of consent or withdrawal of consent for data processing should not be a basis for unfavorable treatment of the applicant or employee, and should not give rise to any negative consequences for them. In particular, this should not constitute a reason for refusal of employment or termination of employment contract.





Poland

In Detail

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant's personal data in your jurisdiction?

Pursuant to Article 22¹ §1 of the Labor Code, and as noted above, an employer may request from an applicant particular details including name, surname, date of birth, place of residence (address for correspondence), education and work experience. The employer may demand from the applicant the provision of personal data other than that specified above if permitted under the law. It is possible to process additional applicant personal data; e.g., the applicant's image, personal interests, etc. with the applicant's consent (please see comments on consent in question 3 below). Such consent has to be given freely and should meet the other requirements of Article 7 of the GDPR. The Polish Data Protection Authority states that separate applicant consent is required to process applicant personal data for future recruitment purposes. If such consent is not granted, applicant personal data can only be processed for the purposes of the recruitment process concerning the current job position.

It is not standard practice in Poland for employers to carry out background checks in relation to applicants. If the employer would like to verify information provided by the applicant, the employer should first require additional confirmation directly from the applicant. The Polish Data Protection Authority is of the opinion that employers have enough tools (e.g., the interview and reference letters) to verify applicants' qualifications and experience. If such confirmation is not provided by the applicant, the employer may check information using publicly available sources (but only within the scope of data that the employer may require under the law and by using proportionate tools). Employers therefore often need to assess whether background checks are appropriate and proportionate in the circumstances and to consider the implications of data protection and discrimination legislation. There are, however, exceptions that enable employers to carry out background checks; e.g., information about applicants' and employees' criminal records may be collected in relation to certain professions only, when the law clearly allows the employer to collect such information.

Transfers of applicant data overseas or to third parties are subject to the same rules as the transfer of employee data (please see questions 6 and 7 below).

3. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee's personal data in your jurisdiction?

Under Polish law, employers are entitled to process certain personal data of their employees for the purposes of establishing and maintaining the employment relationship. Under Article 22¹ § 1 and § 2 of the Labor Code, an employer may request from an employee the following personal data only: first and last names, parents' first names, date of





Poland

In Detail

birth, address, education and career path; other personal data, including the names and dates of birth of an employee's children, can be requested only to the extent it is necessary for the employee to enjoy the various rights granted to him/her under labor law. Employers may also request the identification number awarded by the authorities (the so-called "PESEL" number) and other personal data, if permitted under law. If there is no provision of law, other personal data, such as an employee's image, may only be collected and processed with the employee's consent.

A few years ago, the Supreme Administrative Court resolved the question of whether an employer may also process other types of employee personal data, not identified in the Labor Code, but given freely by the employees themselves. The Court ruled that relying on written consent to process this kind of data infringes the rights of the employee, as well as his/her freedom to express his/her will, due to the imbalance of power in the employer-employee relationship. This is thought to put the freedom of consent in doubt. On this basis, even the employees' written consent to an employer's demand to collect unspecified data under Article 22¹ of the Labor Code would be an evasion of the law. However, the Amending Act is to explicitly allow the processing of non-sensitive data of employees based on their freely given consent.

Under the GDPR, employee consent to process personal data has to meet requirements specified in Article 7 of the GDPR (i.e., employee consent must be freely given). The GDPR does not exclude the possibility of obtaining consent from an employee; however, due to the imbalance of power in the relationship between employee and employer, employers should be ready to prove that the employee did not consent due to employer pressure, in order to minimize the risk of the employee consent being challenged by the Polish Data Protection Authority.

4. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee's personal data?

There is no obligation to have a separate privacy statement or agreement; however, the employer has an obligation under Article 13 of the GDPR to notify and inform employees about the processing of their personal data. Such notification must include information about the identity and contact details of the controller, the contact details of the data protection officer, the purposes of and the legal basis for the processing, and the recipients or categories of recipients of the personal data.

The information may be provided in writing, orally at the request of the individual when the identity of that person is proven by other means or by electronic means where appropriate (e.g., via email). Employer must do so in a concise, transparent, intelligible and easily accessible way, in clear and plain language and free of charge.





Poland

In Detail

Information can be provided in the form of a privacy notice, can be included in the employment contract or can constitute a separate statement.

5. For how long must an employer retain an employee’s personal data? What is best practice?

Generally, the GDPR requires that personal data should be kept for no longer than necessary for the purpose for which the personal data are processed.

In Poland, employee personal data should be retained, in principle, for 50 years after termination of the employment contract. The 50-year period of HR and payroll records retention is counted differently depending on the type of documentation; i.e., for HR records (mainly employee files), the 50 years runs from the termination of the employment relationship with a given employer, and for payroll records, the 50 years runs from the date on which they were created. Nevertheless, the data retention period should cover 50 years from termination of the employment relationship, in particular due to the fact that the social security contributions payer is obliged to keep payroll details, payslips or other evidence on which the retirement or invalidity pension is assessed for 50 years following termination of the employment relationship of a given insured with a given payer.

On January 1, 2019, the amendment of the Act on Retirement and Disability Pensions from the Social Security Fund will come into force, requiring employers to keep payroll details, payslips or other evidence on which the insured person’s retirement or invalidity pensions basis is assessed for 10 years after the end of the calendar year in which: (a) the insured person ended his/her employment relationship with a given contributions payer, in the event of a person reported for insurance by a given contributions payer after December 31, 2018; and (b) the so-called information report, referred to in provisions applicable to the social insurance system, was submitted. These new rules will also apply to entities hiring self-employed persons or contracting personnel under agency or service agreements.

The remaining non-compulsory documentation in matters related to the employment relationship shall be stored in accordance with the limitation period for claims to which the documents relate or may relate; in the case of employee claims, the relevant period is no less than three years.





Poland

In Detail

6. What are the legal restrictions on transferring employees’ personal data outside your jurisdiction?

According to the GDPR, any transfer of personal data to a third country (non-EEA country) shall take place only if certain requirements are met.

A transfer of personal data to a third country may take place where the European Commission has decided that the third country, a territory or one or more specified sectors within that third country ensures an adequate level of protection. Such “adequacy decisions” have been issued with respect to, for example, Switzerland, Argentina, Israel, etc. Additionally, the EU-US Privacy Shield Framework is generally regarded as providing such level of protection.

In the absence of a European Commission decision, the transfer of personal data to a third country may take place only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. The appropriate safeguards may be provided for, without requiring any specific authorization from a supervisory authority, by, for example, binding corporate rules or standard contractual clauses adopted by the European Commission.

Even if the above safeguards are not applied, the transfer of personal data to a third country may take place if, for example, the data subject (employee) has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject or the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject (employee) between the controller and another natural or legal person.

7. What are the legal restrictions on transferring employees’ personal data to a third party?

Employee personal data may be transferred to a third party on the basis of a data processing agreement that authorizes the third party to process personal data for and on behalf of the controller (i.e., the employer). The third party would therefore act as a processor for the employer. Under Article 28 of the GDPR, the data processing agreement must contain a general description of the personal data processing, including subject matter and duration of the processing, the nature and the purpose of the processing, the type of personal data and categories of data subjects involved, and the rights and obligations of the controller (employer) and processor (third party). Furthermore, the data processing agreement should explicitly state that the processor ensures that people authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and may only process personal data on the controller’s documented instructions.





Poland

In Detail

If employee personal data are transferred to another controller (e.g., to an affiliate or parent company) who will process it for its own purposes and decide on the means of data processing, the parties must consider whether there is a legal basis for such data transfer. In principle, if personal data are transferred for the purposes of HR management and administration, this would be based on the legitimate interests of the employer and the affiliate; however, the legal basis and the purpose of the transfer should be decided on a case-by-case basis. A data sharing agreement is recommended to document the legal basis and purpose of the transfer in case of inspection or inquiries from the Polish Data Protection Authority.

8. What are the consequences of breaching privacy laws in your jurisdiction?

Under the GDPR, the consequences of breaching privacy laws are as follows:

- Compensation for damage: any person who has suffered material or non-material damage as a result of an infringement has the right to receive compensation from the controller (employer) or processor for the damage suffered. Pursuant to the Polish Act on Personal Data Protection, the liability for material and non-material damages resulting from a breach of the GDPR is based on the general principles of Polish civil law.
- Administrative penalties: the Polish Data Protection Authority may impose administrative penalties if the GDPR rules have been infringed. The gravity of penalties depends on, for example, the nature, gravity and duration of the infringement, the intentional or negligent character of the infringement, any action taken by the controller (employer) or processor (third party) to mitigate the damage, the degree of responsibility of the controller or processor taking into account technical and organizational measures, any relevant previous infringements, the degree of cooperation with the Polish Data Protection Authority, the categories of personal data affected by the infringement and other aggravating circumstances of the infringement. Under the GDPR there are mandatory penalties for violation of the GDPR regulations in the following amounts:
 - o Up to EUR 10 million or up to 2% of the total global annual turnover of the enterprise in the previous financial year (whichever is higher) in the case of a violation of the regulations relating to, for example, the data processing security;
 - o Up to EUR 20 million or up to 4% of the total global annual turnover of the enterprise in the previous financial year (whichever is higher) in the case of a violation of the provisions relating to, for example, the rights of persons whose data are processed, failure to provide the requested information to the data subject.





Poland

In Detail

The GDPR does not provide for criminal sanctions; however, the Polish Act on Personal Data Protection includes criminal provisions and sanctions for (a) processing of personal data if such processing is not allowed or the processing is carried out without authorization or (b) obstructing or hindering inspection of personal data processing.

9. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee’s personal data?

An employer is only entitled to process certain personal data (listed in the Labor Code and other provisions of labor law); however, in practice many Polish employers process more data than allowed. For instance, it is very common that applicants provide, on their own initiative, additional data such as personal images or interests. Consequently, an employer who receives such additional data has no legal basis for processing that data without consent. In practice, it is difficult to delete such “excessive” data from applications or to contact each applicant and request his/her consent to processing of additional personal data. It is recommended that employers review the application process to avoid collection of “excessive” data.

Additionally, many employers belong to an international group of companies that process and transfer employee personal data for administrative/management purposes. Such processing in principle can be based on the legitimate interest of the employer and companies from the employer group. However, employers should bear in mind that they need to observe provisions on personal data transfer outside the EEA to countries that do not provide an adequate level of personal data protection and should comply with the data minimization principle. Pursuant to guidance from the Polish Data Protection Authority, employee data transfers within the group of companies should be limited to the relevant data necessary for the purposes of processing.

Contributed by: **Agata Szeliga & Katarzyna Paziewska**, Sołtysiński Kawecki & Szlęzak



[Link to biography >](#)



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Russia

Contributed by: **Secretan Troyanov Schaer SA**



In Brief



In Detail

Contributed by: **Markus Schaer**, Secretan Troyanov Schaer SA



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Russia

In Brief

1. Is there a law regulating applicant personal data?

No, the general rules apply (please see question 2).

2. Is there a law regulating employee personal data?

Yes, the Labor Code and the Federal Law on Personal Data.

3. Do I need to have a privacy statement or agreement?

Yes. The employer must have internal regulations and each employee must sign off to confirm that the regulations were brought to his/her attention.

4. How long must I retain employee data? What is best practice?

Data must be destroyed (normally within 30 days) once processing becomes illegal, e.g., because the data subject withdrew his/her consent or the data are no longer necessary, unless the law (e.g., tax or accounting rules) requires the employer to retain the data for longer periods. Mandatory archiving periods also apply.

5. Can I transfer employee data overseas?

Yes, if the recipient country offers adequate data protection or the employee has provided his/her prior written consent.

6. Can I transfer employee data to a third party?

This can normally only be done with an employee's prior written consent (this also applies to group companies).

7. What are the consequences of breach?

Unauthorized processing and disclosure of data is a breach of labor law, an administrative offense and sometimes also a criminal offense. An employee can claim damages (financial damages and damages for emotional distress).

8. What are the main pitfalls?

- Insufficient documentation and failure to obtain the data subject's consent in the required form and scope; and
- Insufficient organizational and technical measures to prevent unauthorized access to, and disclosure of, personal data.





Russia

In Detail

1. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant's personal data in your jurisdiction?

As a general overview, although Russia is not part of the EU or EEA, Russian data privacy law was initially inspired by EU law, in particular Directive 95/46/EC of October 24, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Although we do not expect that the GDPR will be transposed into Russian law, we anticipate that it will influence the evolution, interpretation and enforcement of Russian privacy rules.

There are no specific rules in Russia that would regulate an applicant's personal data. Some rules have been formulated in explanations of the Russian Data Authority (in particular, the letter of Roskomnadzor of December 14, 2012). According to these explanations, the processing of an applicant's data normally requires the applicant's consent. If the candidate can apply by filling in a form on the company's website, the consent can be given by ticking a box except where the law requires written consent (e.g., sensitive data, biometrical data, cross-border transfers, disclosure to third parties). Written consents must have specific content (please see question 2 below) and be signed by hand or digitally. If an electronic form is used, it must comply with Government Resolution No. 687 of September 15, 2008 (please see question 3 below), and the company must further publish a privacy statement on its website. Moreover, the data must first be collected into a database located within Russian territory, at least to the extent it concerns Russian citizens.

The applicant's data can be stored during the recruitment process, but the data should be destroyed within 30 days thereafter if the applicant is not hired. Applicant data can be stored for future vacancies only with the applicant's specific consent. When providing consent, the applicant should be informed about the duration of the recruitment/selection process. Labor law requires that employers obtain data from the applicant personally (please see question 2 below). Where this is not possible, the applicant must be informed of the reasons, of the sources that will be used to obtain the information, of the manner in which the information will be procured and of its nature. The applicant must give his/her written consent in advance and also be informed in advance about the consequences of a failure to give such consent. Background checks are therefore not legally possible without the applicant's written consent. A prospective employer refusing to hire an applicant for an open position must give the reasons in writing. In this context, using the results of background checks is highly restricted.





Russia

In Detail

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee’s personal data in your jurisdiction?

The protection of employees’ personal data is regulated by chapter 14 of the Labor Code of December 30, 2001 and the Federal Law On Personal Data of July 27, 2006 (“**Personal Data Law**”). The Government, ministries and agencies responsible for implementing the Personal Data Law can issue regulations on specific aspects of data processing within their respective authority. The most important are:

- “List of Information of Confidential Character” approved by Presidential Decree No. 188 of March 6, 1997;
- “Regulation on the Particularities of Personal Data Processing Without the Use of Automated Means” approved by Government Resolution No. 687 of September 15, 2008 and “Requirements for the Protection of Personal Data During Their Processing in Personal Data Information Systems” approved by Government Resolution No. 1119 of November 1, 2012;
- “Composition and Content of Organizational and Technical Measures in Order to Ensure the Safety of Personal Data During Their Processing in Personal Data Information Systems with the Use of Tools for Data Protection by Encryption Necessary to Fulfill the Requirements Set by the Government of the Russian Federation for the Protection of Personal Data for Each Safety Level” approved by Order of the Federal Security Service No. 378 of July 10, 2010; and
- “Composition and Content of Organizational and Technical Measures in Order to Ensure the Safety of Personal Data During Their Processing in Personal Data Information Systems” approved by the Federal Service for Technical and Export Control No. 21 of February 18, 2013.

Article 23 of the Russian Constitution and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms protect the right to a private and family life (including personal data) and Article 24 of the Russian Constitution prohibits the use, collection, storage and dissemination of personal data relating to an individual’s private life without such individual’s consent. The Russian Federation is a party to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (effective since November 1, 2013). Russia also signed the Additional Protocol of November 8, 2001 regarding supervisory authorities and transborder data flows, but ratification of the Protocol is still outstanding.





Russia

In Detail

The Federal Law “On Information, Information Technologies and the Protection of Information” of July 27, 2006 classifies information of restricted access (including personal data) as confidential and defines the duties of the owner of confidential information or the operator of information systems (databases) containing confidential information to protect such information, in particular from unauthorized access and disclosure. The law can introduce a requirement to use certified equipment for data protection. The manufacturing, sale, installation and/or maintenance of encryption tools and devices for the technical protection of data may require a government license.

The Personal Data Law defines personal data as information relating to an identified or identifiable individual. Processing of personal data includes the collection, organization, compilation, storage, rectification (updating, alteration), use, dissemination (disclosure, transmission, access), anonymization, blockage, erasure and any other operations relating to personal data. Any operator processing personal data (by automated means or with the help of human labor) must, before any processing, notify the responsible government agency (Roskomnadzor). Employers exclusively processing the personal data of their employees are exempt from notification.

Employees’ personal data are defined by Article 85 of the Labor Code as information that the employer needs in relation to the employment and that concerns a specific employee (e.g., the employee’s full name, date of birth, address, family, social and financial situation, education, profession, salary). The Labor Code restricts the liberty of the employer to request information. In particular, the employer cannot request and process data on the employee’s political, religious or other beliefs or, unless permitted by federal law, his/her membership of non-government organizations or labor unions. Data on the employee’s private and family life can be obtained only if directly related to the employment. Medical information can be obtained only if required under the law or relevant to the performance of the specific duties of the employee. In general, the employer can process the employee’s personal data exclusively in order to ensure compliance with legislation, to assist the employee with a job search, training or career promotion, to ensure the personal safety of the employee, to control the quantity and quality of job performance and in relation to the preservation of property. The collection of data for any other purposes requires the employee’s written consent.

Personal data must be obtained from the employee personally. If this is not possible, it can be obtained from a third party, but the employee must be notified in advance and give his/her written consent. The employer must inform the employee what information it intends to obtain, why it is being obtained, the source(s) of the information and the manner in which it will be procured. The employee must also be informed of the consequences if he/she refuses to consent.





Russia

In Detail

There are precise requirements in relation to consents required under the Personal Data Law. The consent must be voluntary, specific, informed and conscious and can normally be withdrawn. As a rule, the consent can be given in any form, but it is for the operator to prove that consent was effectively given and that it originated from the data subject or from a duly authorized representative, or that the data can be processed without the data subject's consent, e.g., because the data subject has published the data so as to render it generally accessible. According to a recent court decision, data published on social media cannot be deemed generally accessible within the meaning of the law. Consent is also required after the death of the data subject and can then be given by the heirs if it was not given when the data subject was still alive.

Where the law requires written consent, the consent must include the name (family, middle and first name), address and relevant references of the identity document of the personal data subject, the name and address of the operator requesting the consent, the purpose of the data processing, the list of personal data for which the consent is given, the list of operations with personal data for which the consent is given, a description of the methods of data processing and the period for which the consent is given. The consent must indicate how it can be withdrawn (under the law it can be revoked at any time). It is generally recommended to use standard forms to obtain consents for data processing.

The employer must take the necessary organizational and technical measures to guarantee the protection of an employee's personal data against loss and unauthorized or accidental access and use. Personal data must be treated as confidential information. The employer must limit access to personal data to specially authorized staff, and such staff must have access only to the data it requires to perform specific functions. Hard copies of documents containing employees' personal data must be stored in a safe way excluding access from unauthorized persons (e.g., in a safe or at least under lock and key).

Personal data of Russian citizens must be collected through a database located within Russian territory. This also applies to foreign companies collecting data through websites, but should not exclude the cross-border transfer of data provided they originate from a database in Russia.

3. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee's personal data?

Under the Labor Code, the employer must set out rules for the storage, processing and protection of employee data, define the scope and content of the data processed and state the rights and obligations of the employees with respect to personal data. The relevant document(s) (typically but not necessarily called "regulation on personal data") is (are)





Russia

In Detail

treated under the Labor Code as a “local regulatory act” of the employer and is (are) compulsory for all employees of the company. The regulations must be brought to the attention of each employee, which must be acknowledged by the employee’s personal signature. The employees and their representatives are entitled to participate in the implementation of measures to protect employees’ personal data.

The law does not define the form or structure of the document regulating data protection, but such document would typically contain the following:

- (a) a general section (e.g., the purpose of data processing, the definition of data processed, how the data are collected, the requirements with respect to the data);
- (b) a section regulating the storage, use and transfer of data (e.g., procedures, place of storage, access);
- (c) a list of the staff responsible for processing data or having access to data;
- (d) the employee’s rights (e.g., the right to access his/her data);
- (e) the employer’s duties; and
- (f) the definition of liability in the event of unauthorized access or disclosure of an employee’s data.

4. For how long must an employer retain an employee’s personal data? What is best practice?

Under the Personal Data Law, personal data (on paper or in the form of electronic files) can be kept as long as needed for the purpose for which such data were collected or processed and must be destroyed (generally within 30 days) when they are no longer needed for such purpose unless the law requires the data to be retained for a longer period. The latter applies, in particular, to tax and accounting documents. As a rule, tax records must be kept for at least four full calendar years, accounting documents for at least five full calendar years and documents relevant for the calculation of social welfare contributions for at least six full calendar years.

The law further defines mandatory archiving periods. Article 22.1 of the Federal Law No. 125-FZ of October 22, 2004 “On Archives in the Russian Federation,” as amended by Federal Law 127-FZ of June 18, 2017, requires the storage of HR documents (documents reflecting the employment relationship between employer and employee) archived after January 1, 2003 for up to 50 years (previously 75 years) unless different archiving periods are defined by implementing regulations. Currently, the “List of Standard Management Documents Created in the Activity of State Authorities,





Russia

In Detail

Authorities of Local Self-Government and Organizations, With Indication of Their Storage Period,” approved by Order of the Ministry of Culture No. 558 on August 25, 2010, requires, for instance, that the personal files of the employees and employment agreements be kept for 75 years and, in some cases, permanently (the list has not yet been updated following the amendment of the law in 2017). Documents not included in the personal files (reports, explanations, documents related to business trips and holidays, etc.) must normally be kept for five years. Documents relating to unsuccessful job candidates (CVs, questionnaires, references, etc.) must be kept for three years. The destruction of archives must be documented. If the employer’s business is liquidated, documents should be transferred to a state or municipal archive. The Personal Data Law does not apply to archives.

5. What are the legal restrictions on transferring employees’ personal data outside your jurisdiction?

Transfers of personal data across the Russian border are permitted if the territory to which the data are transferred guarantees an adequate protection of the rights of the personal data subjects. Transfers to a third party (including other companies of the same group) are subject to the restrictions listed under question 6 below. If the recipient territory does not offer adequate protection, transfers are possible with the prior written consent of the data subject.

Under the Personal Data Law, countries having ratified the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (please see also Article 12 of the Convention) are deemed to offer adequate protection. The law further empowers the supervisory authority (Roskomnadzor) to define a list of additional jurisdictions that are considered to offer adequate protection. The current list dates from March 15, 2013 and was last amended on June 15, 2017. It includes Australia, Argentina, Israel, Canada, Morocco, Malaysia, Mexico, Mongolia, New Zealand, Angola, Benin, Cape Verde, South Korea, Peru, Tunisia, Chile, Costa Rica, Qatar, Mali, Singapore, South Africa, Gabon and Kazakhstan. The most important jurisdictions considered not to offer adequate protection are the United States, India and China. It is the responsibility of the operator to assess the level of protection offered by the domestic legislation of the territory to which the data are to be transferred before authorizing the transfer of data to such territory.

6. What are the legal restrictions on transferring employees’ personal data to a third party?

An employee’s personal data can be transferred inside the same legal entity as provided by the relevant local regulatory act (regulation on personal data). The data may not be transferred to a third party (including other group companies) without the employee’s prior written consent except in cases where such transfer is authorized or required under federal law (e.g., under tax or social welfare law) or necessary to prevent a threat to the employee’s life or health.





Russia

In Detail

The person to whom the personal data are communicated is authorized to use such data only for the purpose for which they were communicated. The employer communicating the data must obtain a confirmation that this requirement will be complied with.

The Labor Code does not specifically regulate the outsourcing of data processing. The Personal Data Law requires that the company outsourcing data processing obtain contractual covenants from its service provider guaranteeing the protection of the confidentiality and safety of the data during processing. The employee's prior written consent should also be obtained. This applies, in particular, where accounting and financial reporting is outsourced to a third-party service provider.

7. What are the consequences of breaching privacy laws in your jurisdiction?

The employer is liable for damages (including damages for emotional distress) in accordance with the Civil Code. The employee can further apply to court in relation to unlawful actions or the employer's failure to act in relation to the processing and protection of personal data.

If an employee breaches the duty to keep other employees' personal data confidential and such duty is properly defined by the employment contract and the employer's regulation on personal data, the employer can take disciplinary action against the employee at fault. The unlawful disclosure of employee personal data is a reason for immediate dismissal from employment. The employee disclosing personal data in breach of his/her duties can also be held materially liable for damages suffered by the employer as a result of the unlawful disclosure of employee data (excluding lost profit).

A breach of the provisions of the Labor Code relating to the protection of employees' personal data is considered a breach of labor law and constitutes as such an administrative offense. Officers of the employer can be fined up to RUR 5,000; legal entities up to RUR 50,000. Officers of employers who have already been sanctioned can be disqualified for a period from one to three years.

The processing of personal data in breach of the law, in particular without the data subject's consent where such consent is required, is sanctioned by fines of up to RUR 20,000 for officers of legal entities and up to RUR 75,000 for the legal entities themselves. The disclosure of information with restricted access by individuals having access to such information in connection with the performance of their job duties is sanctioned by a fine of up to RUR 5,000 for officers of legal entities and up to RUR 1,000 for other individuals.





Russia

In Detail

The unlawful disclosure and publication of data relating to the private life of an individual is a criminal offense. Officers of the employer can also commit a criminal offense if they do not provide the employee with documents and materials that they are obliged to provide under the law. Under the Labor Code, an employee has the right to obtain full information about his/her personal data and the processing of such data, to have free access to his/her data and to obtain copies of any records containing personal data except where the law provides otherwise.

Both Roskomnadzor and the labor inspection can audit compliance with personal data law on their own initiative or pursuant to individual complaints.

The Criminal Code further sanctions the unauthorized access to data stored on computers, breach of the rules relating to exploitation of tools for the storage, processing and transmission of electronic data, misuse of an IT network or end user equipment resulting in the destruction, blockage, alteration or copying of electronic data, and the creation, use and distribution of malicious software.

An individual may also demand the refutation of information defaming his/her honor, dignity or business reputation if such information is untrue. If the information has been published by mass media, the individual has the right to publish his/her reply in the same media where the inaccurate information was published.

8. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee's personal data?

Data protection law requires substantial paperwork. It is not sufficient to take adequate measures for the protection of personal data; such measures must also be correctly documented. This aspect is often neglected especially by small firms that do not have sufficient resources for a human resources department and the formal aspects of data protection tend to be overlooked. The approach of the courts and authorities also tends to be formal. It is therefore important to make sure that data processing complies with the letter of the law, i.e., that all conditions authorizing data processing in a specific case are strictly complied with. Theft or unauthorized use of data by employees is a major risk, and the remedies offered to the employer under the law are not necessarily as powerful in practice as they might appear on paper.

It is not always obvious what legal, organizational and technical measures an employer must take to comply with data protection law. Not all commentators' opinions appear realistic (e.g., keeping all employee files in a safe, not sending personal data through unsecured Internet connections, mandatory use of cipher technology, etc.). Following amendments to the Personal Data Law in 2011, it is the employer's duty to define the level of data protection required based on a risk assessment. However, the authorities still tend to regulate the technical aspects of data protection in





 In Brief

 In Detail

Russia

In Detail

excessive detail rather than use abstract concepts taking into account specific circumstances (e.g., standard of conduct, reasonable degree of care, good practice, etc.). This is likely to restrict the employer’s flexibility and to increase the financial and administrative burden of compliance.

Contributed by: **Markus Schaer**, Secretan Troyanov Schaer SA

 [Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Saudi Arabia



Contributed by: **Mayer Brown LLP**



In Brief



In Detail

Contributed by: **Tom Thraya, Jad Taha & Omar El-Khattabi, Mayer Brown LLP**



[Link to biography >](#)



[Link to biography >](#)



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Saudi Arabia

In Brief

1. Is there a law regulating applicant personal data?

There are currently no laws or regulations in Saudi Arabia that regulate applicant personal data.

2. Is there a law regulating employee personal data?

There are currently no laws or regulations in Saudi Arabia that regulate employee personal data.

3. Do I need to have a privacy statement or agreement?

There are no formal legal requirements for a privacy statement or agreement; however, in practice, confidentiality clauses are customarily included in employment agreements.

4. How long must I retain employee data? What is best practice?

Employees and employers can contractually agree on certain parameters that govern the retention of data. It is also best practice to retain employee data for at least one year following termination of employment.

5. Can I transfer employee data overseas?

Any transfer of employee data overseas must not be prohibited by the relevant employment agreement. Additionally, it is highly recommended that employers seek the relevant employee’s consent prior to the transfer of data.

6. Can I transfer employee data to a third party?

As noted above, any transfer of employee data to a third party must not be prohibited by the relevant employment agreement. Additionally, it is highly recommended that employers seek the relevant employee’s consent prior to the transfer of data.

7. What are the consequences of breach?

Any action that is deemed by a competent court in Saudi Arabia to constitute a breach of privacy rights could allow for the non-breaching party to terminate the relevant agreement. The non-breaching party could also potentially be entitled to damages, although the granting and extent of such damages is generally at the complete discretion of the court.

8. What are the main pitfalls?

The lack of relevant laws and regulations in Saudi Arabia is often a source of confusion for those seeking clarity on the limitations and restrictions relating to the management of personal data. Similarly, there is a lack of established customary practice that can be used as a reliable guide for the treatment of personal data.





Saudi Arabia

In Detail

1. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant’s personal data in your jurisdiction?

There are no specific personal data protection laws or regulations in Saudi Arabia and, therefore, no such laws or regulations regulate applicant personal data.

The Consultative Assembly (Shura Council) is reportedly working on drafting a new law for the protection of personal data, although no official commentary or information has been published at this time.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee’s personal data in your jurisdiction?

There is no law or regulation in Saudi Arabia that specifically regulates the use or handling of an employee’s personal data.

Please note, however, that courts in Saudi Arabia have a wide discretion to interpret Sharia Law principles as prohibiting the dissemination of personal information of employees, and have done so in the past. The concept of *stare decisis* (binding precedent) does not exist in Saudi Arabia.

3. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee’s personal data?

There is no legal requirement to have a document that deals with employee personal data; however, it is customary in Saudi Arabia to cover this type of personal data management as a stand-alone provision in the underlying employment agreement (e.g., in a confidentiality clause).

4. For how long must an employer retain an employee’s personal data? What is best practice?

There is no law regulating the retention period for employee data. The parties to an employment agreement are generally free to negotiate this type of restriction. Please note, however, that former employees can sue their former employers for up to one year following termination of employment. As such, it is advisable for employers to retain employee data for at least one year following termination.





Saudi Arabia

In Detail

5. What are the legal restrictions on transferring employees’ personal data outside your jurisdiction?

There are no laws or regulations in Saudi Arabia that govern the transfer of employee information outside of Saudi Arabia but any such transfer must not be prohibited by the relevant employment agreement. It is highly recommended that employers obtain an employee’s consent prior to the transfer of personal data.

6. What are the legal restrictions on transferring employees’ personal data to a third party?

There are no laws or regulations in Saudi Arabia that govern the transfer of employee information to a third party, but any such transfer must not be prohibited by the relevant employment agreement. It is highly recommended, as noted above, that employers obtain an employee’s consent prior to the transfer. Customary practice indicates that, in most cases, employees must consent to such a transfer of their personal data.

7. What are the consequences of breaching privacy laws in your jurisdiction?

In the case of a breach of an express privacy clause that is contractually agreed upon by the parties, the non-breaching party may freely terminate the agreement and sue for damages. Please note that courts have a wide discretion in assessing the consequences and/or the additional repercussions relating to such a breach.

8. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee’s personal data?

The absence of relevant laws and regulations is often a major source of confusion to those seeking to understand the treatment of personal data in Saudi Arabia. Employers should focus on maximizing protections through express contractual provisions, in addition to seeking express consent from employees as to the management of their data whenever possible, especially given the shifting legislative landscape on these issues in Saudi Arabia.

Contributed by: Tom Thraya, Jad Taha & Omar El-Khattabi, Mayer Brown LLP



[Link to biography >](#)



[Link to biography >](#)



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



South Africa



Contributed by: **ENSafrica**

 In Brief

 In Detail

Contributed by: **Ross Alcock**, ENSafrica

 [Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



South Africa

In Brief

1. Is there a law regulating applicant personal data?

Yes, the protection of an applicant’s personal information and data privacy in South Africa is regulated by the Protection of Personal Information Act 4 of 2013 (“**POPI**”).

2. Is there a law regulating employee personal data?

The personal information of an employee is also regulated by POPI.

3. Do I need to have a privacy statement or agreement?

Employers should obtain the consent of an employee (or an applicant) before processing their personal information.

4. How long must I retain employee data? What is best practice?

Records of personal information must not be retained for any longer than is necessary for achieving the purpose for which the information was collected and processed.

5. Can I transfer employee data overseas?

Generally speaking, a responsible party (such as an employer) may not transfer personal information about a data subject (an employee) to a third party who is in a foreign country.

6. Can I transfer employee data to a third party?

An employer should obtain consent from the employee before transferring any personal information to a third party.

7. What are the consequences of breach?

Depending on the nature of the breach, the consequences may be an administrative fine not exceeding R10 million, or, if the breach concerns Chapter 11 of POPI, a fine not exceeding R10 million, imprisonment, or both.

8. What are the main pitfalls?

Currently, the provisions of POPI relating to the processing of personal information are not fully effective. However, employers should ensure that their data collection and retention policies comply with the standards required by POPI.





South Africa

In Detail

1. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant’s personal data in your jurisdiction?

Yes, the protection of any natural person’s personal information and data privacy in South Africa is regulated by the Protection of Personal Information Act 4 of 2013 (“**POPI**”). While POPI has been enacted, the majority of the Act is not in force and still needs to be proclaimed by the President of the Republic of South Africa. It is, however, advisable that a responsible party (meaning any public or private body that processes personal information) takes the necessary measures to comply with the provisions of POPI sooner rather than later. This chapter has been prepared on the basis that POPI is fully proclaimed.

POPI applies to the pre-employment screening and vetting of applicants for employment in instances where the applicant’s personal information is accessed and processed. Such information includes, but is not limited to, employment history, criminal records, educational history, credit records and directorships.

In order to process the applicant’s personal information during the recruitment, selection, vetting and ultimate appointment of the applicant for employment, an employer should ensure that it processes personal information in accordance with POPI. In this regard, personal information may be processed in circumstances where the employee/prospective employee consents to the personal information being “processed” or the processing of personal information is necessary for the conclusion or the performance of the contract of employment.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee’s personal data in your jurisdiction?

Yes, POPI applies to the processing of an employee’s personal information. Employee data (i.e., personal information) must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless:

- retention of the record is required or authorized by law;
- the responsible party reasonably requires the record for lawful purposes related to its functions or activities;





South Africa

In Detail

- retention of the record is required by a contract between the parties thereto; or
- the data subject, or a competent person where the data subject is a child, has consented to the retention of the record.

3. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee’s personal data?

Under section 11 of POPI, personal information may lawfully be processed in circumstances where the data subject (the person to whom the information relates) consents to his/her information being processed. Accordingly, an employer should preferably obtain consent from an employee to process his/her personal information. There is no specific format that this consent should take. However, practically speaking, this should be clear written consent from the data subject. The employer is permitted to process an employee’s personal information without consent if that information is necessary for the conclusion or performance of the contract of employment.

4. For how long must an employer retain an employee’s personal data? What is best practice?

As noted in question 2, records of personal information must not be retained for any longer than is necessary for achieving the purpose for which the information was collected and processed. An employer must accordingly delete and destroy all of the personal information that is no longer the subject of prior consent or that is no longer necessary for the performance of the contract of employment. This must be done as soon as reasonably practicable.

5. What are the legal restrictions on transferring employees’ personal data outside your jurisdiction?

A responsible party (such as an employer) may not transfer personal information about a data subject (an employee) to a third party who is in a foreign country unless:

- (a) the third party is subject to a law, binding corporate rules or binding agreement which provides an adequate level of protection that effectively upholds principles for reasonable processing;
- (b) the data subject consents to the transfer;
- (c) the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject’s request;





South Africa

In Detail

- (d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or
- (e) the transfer is for the benefit of the data subject, provided that it is not reasonably practicable to obtain the consent of the data subject to that transfer and if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

6. What are the legal restrictions on transferring employees’ personal data to a third party?

Under section 10 of POPI, personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive. Personal information must therefore be purpose-specific and the dissemination of the personal information to third parties is generally prohibited. An employer would need to obtain consent from the employee before transferring any personal information to a third party.

7. What are the consequences of breaching privacy laws in your jurisdiction?

If a responsible party is alleged to have committed an offense under POPI, the Information Regulator (the regulatory body established in terms of POPI) may issue an administrative fine of the appropriate amount, but not exceeding R10 million.

When determining an appropriate fine, the Information Regulator will consider the nature of the personal information involved, the duration and extent of the contravention, the number of data subjects affected by the contravention, whether or not the contravention raises an issue of public importance, the likelihood of substantial damage or distress, including injury to feelings or anxiety suffered by data subjects, whether the responsible party or a third party could have prevented the contravention from occurring, any failure to carry out a risk assessment or a failure to operate good policies, procedures and practices to protect personal information, and whether the responsible party has previously committed an offense under POPI.

Offenses relating to Chapter 11 of POPI may attract a fine not exceeding R10 million, imprisonment for a period not exceeding 10 years, or both.





South Africa

In Detail

8. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee’s personal data?

POPI imposes rigorous standards for the collection and processing of personal information. While the majority of provisions are not yet fully effective, employers should take active steps to align their data policies with the provisions of POPI sooner rather than later.

Contributed by: **Ross Alcock**, ENSafrica

 [Link to biography >](#)



Spain



Contributed by: **Pérez-Llorca**



In Brief



In Detail

Contributed by: **Andrea Sánchez Guarido, Pérez-Llorca**



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Spain

In Brief

1. Does employee data privacy law in your jurisdiction go beyond the GDPR?

No, neither our current Constitutional Act 15/1999 of December 13 on Personal Data Protection nor the draft of the new Spanish Data Protection Act goes beyond the GDPR.

Please note that the draft is in the Parliamentary stage, so the text is not final and is subject to change.

2. Is there a law regulating applicant personal data?

There are no regulations specifically covering the processing of data relating to applicants. The processing of this data is regulated by the general provisions on data protection contained in the applicable Constitutional Act on Personal Data Protection and in the GDPR.

3. Is there a law regulating employee personal data?

Alongside the GDPR, the following laws apply in Spain: Organic Law 15/1999 and Royal Decree 1720/2007.

4. Do I need to have a privacy statement or agreement?

Under Articles 13 and 14 of the GDPR, certain information must be provided to employees in relation to the collection of their data. Under Spanish laws, no particular form of document is required.

5. How long must I retain employee data? What is best practice?

There are no specific retention periods imposed by data protection regulations other than the need to store the data solely for as long as necessary for the purposes for which the data were collected. Different retention periods are established by other Spanish laws.

6. Can I transfer employee data overseas?

Yes, subject to requirements under the GDPR.

7. Can I transfer employee data to a third party?

Yes, subject to requirements under the GDPR and Spanish law.

8. What are the consequences of breach?

The main consequences of a breach are determined under the GDPR. The consequences therefore include administrative liabilities and fines plus potential criminal liabilities.

9. What are the main pitfalls?

The main pitfall is balancing the employer's control over its employees with the employees' right to privacy. The retention periods for employee data can also be complicated.





Spain

In Detail

1. To what extent does employee data privacy law in your jurisdiction go beyond the GDPR?

With the GDPR coming into force in May 2018, Spain has a draft Data Protection Act pending approval. The purpose of this law is both to “purge the national system” of the national legislation that is contrary to the GDPR and to develop or supplement the GDPR in order to make its application fully effective.

Please note that the draft is at the Parliamentary stage, so the text is not final and is subject to change.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant's personal data in your jurisdiction?

The collection and processing of an applicant's personal data are not regulated in Spain by any specific provision. This processing is subject to the GDPR and the general provisions outlined in question 3 below.

3. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee's personal data in your jurisdiction?

Along with the GDPR, Spanish laws regulate various aspects of personal data protection related to the field of labor law. This sector-specific regulation includes the collection, use, retention, correction and cancellation of personal data. Among these laws, there are the Organic Law 15/1999 of December 13, on the Protection of Personal Data (the “**LOPD**”) and the Royal Decree 1720/2007, of December 21, which approves the Regulation implementing the LOPD (the “**RD 1720/2007**”).

Employers are required to comply with a number of provisions under both the GDPR and Spanish law in relation to the collection, use and/or handling of employee personal data.

4. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee's personal data?

Under Articles 13 and 14 of the GDPR, certain information must be provided to employees in relation to the collection of their data. No particular form of document is required.

Employers also need to comply with several mandatory legal requirements when dealing with the employee's personal file. The main difference in light of the GDPR is that in Spain it is no longer mandatory to register data files with the Spanish Data Protection Authority (“**AEPD**”):





Spain

In Detail

- (a) Employers shall now carry out a record of processing. In general terms, the record of processing shall contain the controller’s identity, the purpose of the processing, the categories of personal data and/or data subjects, the security measures implemented in this regard and, where applicable, an intended disclosure or transfer of data to third countries.
- (b) Regarding security measures, controllers and processors must now implement the security measures they deem appropriate for the adequate protection of the data they are processing, according to Article 32 of the GDPR.

5. For how long must an employer retain an employee’s personal data? What is best practice?

There are no specific retention periods imposed by data protection regulations or guidelines from the AEPD on the retention of employee data. Personal data may be retained for as long as necessary for the purposes for which the data were collected (e.g., as set out under the GDPR) or until the limitation period for various claims has passed.

There are, however, different retention periods established by other Spanish laws, such as the Spanish Code of Commerce, the Spanish General Taxation Law or the Spanish Statute of Workers, depending on the type of data:

- Employment documents – Article 4.1 of the *Royal Legislative Decree 5/2000, of August 4, approving the consolidated text of the Law on Infringements and Sanctions in the Social Order*, establishes that the limitation period for infractions in the social order is three years.
- Social security documents – Article 4.2 of the *Royal Legislative Decree 5/2000, of August 4, approving the consolidated text of the Law on Infringements and Sanctions in the Social Order*, establishes that the limitation period regarding social security infringements is four years.
- Health and safety documents – Article 4.3 of the *Royal Legislative Decree 5/2000, of August 4, approving the consolidated text of the Law on Infringements and Sanctions in the Social Order*, establishes that the limitation period relating to labor risk prevention is five years.
- Accounting and finance records – Article 30 of the *Spanish Code of Commerce* establishes that traders shall keep the books, correspondence, documentation and supporting documents concerning their business, duly ordered, for six years.





Spain

In Detail

- Tax records – Article 66 of the *Spanish General Taxation Law* establishes that the limitation period for the General Administration to demand the payment of unpaid debts is four years.
- Criminal Code – Article 131 of the *Spanish Criminal Code* establishes that the limitation period for crimes against workers is 10 years.

6. What are the legal restrictions on transferring employees’ personal data outside your jurisdiction?

Under Articles 44 to 49 of the GDPR, international data transfers (i.e., those to a country outside the EU/EEA) may be carried out on the following basis:

- International transfers of data based on an adequacy decision: these may take place when the European Commission has decided that the third country in question ensures an adequate level of protection of personal data.
- Transfers subject to appropriate safeguards: the controller or the processor shall provide appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.
- Binding corporate rules (“BCR”): for intra-group international transfers, the AEPD shall approve BCR provided that they: (a) are legally binding and apply to every member concerned of the group of undertakings; (b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and (c) comply with the minimum content set out in the GDPR.
- Derogations: in the absence of an adequacy decision or appropriate safeguards (including BCR), transfers of personal data can still be made if specific conditions apply (for example, the data subject has explicitly consented after being informed of the possible risks).

Additionally, the draft Data Protection Act provides for the AEPD to adopt “standard contractual clauses” for the conduct of international data transfers. Through the use of these clauses, international data transfers may potentially be made without any type of authorization, except for the clauses themselves.





Spain

In Detail

7. What are the legal restrictions on transferring employees' personal data to a third party?

When an employer transfers employee personal data to a third party, the transfer will be subject to the provisions of the GDPR and Spanish law. Under the LOPD and RD 1720/2007, there is a distinction between the disclosure of data to third parties and access to data by third parties:

- *Disclosure of personal data to third parties* – Third parties may have access to employees' personal data for their own purposes. The disclosure of data is regulated in Article 11 of the LOPD, but the GDPR does not contain a specific corresponding article.
- *Access to personal data by third parties* – Third parties have access to personal data when acting on behalf of the controller. The processing of data by a third party is regulated in Article 12 of the LOPD and Article 28 of the GDPR.

8. What are the consequences of breaching privacy laws in your jurisdiction?

Both the GDPR and the draft Data Protection Act consider data breaches relating to a security breach as grave infringements. The following conduct, in particular, will be sanctioned:

- Failure to comply with the duty of the processor to notify the controller of any security breaches of which it is aware.
- Failure to notify the data protection authority of a breach of personal data security, in accordance with Article 33 of the GDPR.

The draft Data Protection Act provides for sanctions in accordance with the GDPR. These infringements shall be sanctioned as follows:

- Administrative liabilities.
- Administrative fines up to EUR 10 million or, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.
- Administrative fines up to EUR 20 million or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.





Spain

In Detail

The level of the penalties shall be measured with due regard to the nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing and the number of data subjects affected and the level of damage suffered, the intentional or negligent character of the infringement, or aggravating or mitigating factors, such as financial benefits/losses avoided.

9. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee’s personal data?

The main pitfall is balancing the employer’s legitimate basis for data processing and its control over its employees with the employees’ right to privacy. With the advance of technology, an employer has more control measures over its employees (e.g., video surveillance cameras, control of devices and communications) and there is a fine line separating the employer’s right to control and the employee’s right to privacy.

In addition, the retention periods for keeping data on former employees, and the applicable conditions, tend to be quite complicated.

Contributed by: **Andrea Sánchez Guarido**, Pérez-Llorca



Sweden



Contributed by: **Advokatfirman Vinge KB**



In Brief



In Detail

Contributed by: **Åsa Gotthardsson**, Advokatfirman Vinge KB



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Sweden

In Brief

1. Does employee data privacy law in your jurisdiction go beyond the GDPR?

There are a few supplementary provisions in the Swedish supplementary laws to the GDPR that may affect the processing of employee data.

2. Is there a law regulating applicant personal data?

Yes, the GDPR and Swedish supplementary laws to the GDPR apply to the processing of applicant personal data.

3. Is there a law regulating employee personal data?

Yes, the GDPR and Swedish supplementary laws to the GDPR apply to the processing of employee personal data.

4. Do I need to have a privacy statement or agreement?

Certain information is required to be provided to employees in connection with the collection of personal data, but no specific form of document is required.

5. How long must I retain employee data? What is best practice?

As a general rule, personal data may be retained and processed only as long as it is necessary having regard to the purpose of the data processing.

6. Can I transfer employee data overseas?

Yes, subject to certain requirements.

7. Can I transfer employee data to a third party?

Yes, subject to certain requirements.

8. What are the consequences of breach?

Employees may claim compensation for damages. The Data Protection Authority may, for example, issue warnings, order corrective compliance measures and/or impose administrative fines.

9. What are the main pitfalls?

- International transfers of personal data within a multinational group of companies.
- Processing of personal data regarding criminal offenses (e.g., within a whistleblowing system).
- Monitoring of employees' use of computers.





Sweden

In Detail

1. To what extent does employee data privacy law in your jurisdiction go beyond the GDPR?

There are a few supplementary provisions in the Swedish supplementary laws to the GDPR that may affect the processing of employee data:

- Special categories of employee data may not be disclosed to a third party unless: (a) there is a legal obligation to disclose such data under employment, social security or social protection laws, or (b) if the employee has given his/her express consent to the disclosure.
- An employer who intends to use camera surveillance in the workplace must consult with trade unions in accordance with the Swedish Employee Co-employment Act.
- Other than authorities, parties may only process criminal offense data if the processing has explicit support in an act, ordinance, regulations or administrative orders issued by a competent authority.
- Personal identity numbers and coordination numbers may only be processed based on consent or when clearly justified with respect to the purpose of the processing, the importance of positive identification or some other significant reason.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant's personal data in your jurisdiction?

Yes, the GDPR and Swedish supplementary laws to the GDPR apply to the processing of applicant personal data. The requirements described in questions 3 to 6 below must be observed in relation to the processing of applicant data.

3. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee's personal data in your jurisdiction?

The Swedish Supplementary Law to the GDPR (SFS 2018:218) implements the GDPR by repealing the Personal Data Act (1998:205) and supplementing the provisions of the GDPR.





Sweden

In Detail

Personal data

Under the GDPR, “personal data” are defined as any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Employee personal data falls under the definition of “personal data.” The GDPR and the Swedish supplementary laws to the GDPR will, thus, apply to the processing of such information.

Controller

With regard to processing of employee data, the employer is typically considered as the controller. The GDPR and the Swedish supplementary laws to the GDPR will apply to employers who are established in Sweden.

A controller must ensure that:

- (a) personal data are processed lawfully, fairly and in a transparent manner in relation to the data subject;
- (b) personal data are collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- (c) personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- (d) personal data are accurate and, where necessary, kept up to date;
- (e) personal data are kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- (f) personal data are processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures; and
- (g) it is able to demonstrate compliance with the general requirements above.





Sweden

In Detail

Lawfulness of processing of personal data

Unless one of the following conditions is satisfied, personal data may be processed only with the consent of the data subject. Such consent must be freely given, specific, non-ambiguous and informed. The data subject may, at any time, revoke his/her consent.

Personal data may be processed without the consent of the data subject if this is necessary:

- (a) for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- (b) for compliance with a legal obligation;
- (c) in order to protect the vital interests of the data subject;
- (d) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
- (e) for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

Special categories of personal data

The GDPR contains a general prohibition against the processing of special categories of personal data. Special categories of personal data are data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Despite the general prohibition, special categories of personal data may be processed with the express consent of the data subject, or if the processing is necessary, e.g.:

- (a) for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;





Sweden

In Detail

- (b) to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; or
- (c) for the establishment, exercise or defense of legal claims.

Data subject rights

The controller must comply with requests from data subjects for exercising their rights of access, rectification, erasure, restriction, objections and data portability.

General obligations

The controller must comply with general obligations, including data protection by design and default, maintenance of records of processing, security requirements, personal data breach requirements, data protection impact assessments, consultations with the data protection authority and designation of a data protection officer.

4. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee’s personal data?

When employee data are collected and processed, the employer must inform the employees of the processing of their personal data. However, no specific form of document is required.

Under the GDPR, the required information to be provided to employees consists of: information on the identity and contact details of the controller; the contact details of the data protection officer (where applicable); the purpose of the processing and the legal basis for the processing, including legitimate interest (where applicable); third country transfers, storage period, rights of data subjects (access, rectification, erasure, restriction, objections and data portability); the right to withdraw consent and lodge complaints to the data protection authority; requirement to provide personal data and the existence of automated decision-making.

5. For how long must an employer retain an employee’s personal data? What is best practice?

There is no requirement to retain employee data for a certain period of time. Personal data shall as a general rule not be kept for a longer period than necessary, having regard to the purpose of the processing.





Sweden

In Detail

There are, however, specific retention periods for certain types of documents, e.g., five to ten years for certain health and safety records and seven years for bookkeeping material. Furthermore, there are general guidelines from the Swedish Data Protection Authority (under the repealed data protection laws) stating, e.g., (a) that candidate data normally shall be deleted when the recruitment process has been completed, unless consent has been obtained for a longer period or the data will be needed for litigation purposes, and (b) that employee data normally should not be kept after termination of employment, but that certain data may be kept for a longer period for administrative purposes, for example, issuance of work certificates, pension payments etc., or for litigation purposes. With respect to litigation, it should also be noted that there are different statutory limitations periods for different claims under Swedish employment laws, that may affect the retention periods for employee data.

6. What are the legal restrictions on transferring employees’ personal data outside your jurisdiction?

Transfers of personal data within the EU or EEA are subject to the general requirements described under question 3 above.

Transfers of personal data to a country outside the EU/EEA may take place if the third country ensures an adequate level of protection for personal data. The transfer of personal data to countries outside the EU/EEA that do not ensure an adequate level of data protection is permitted, e.g., if the transfer is subject to appropriate safeguards (e.g., binding corporate rules or standard data protection clauses adopted by the Commission) or satisfies specific conditions (e.g., consent of the data subject, the transfer is necessary for performance of contract or necessary for the establishment, exercise or defense of legal claims).

7. What are the legal restrictions on transferring employees’ personal data to a third party?

If the controller engages a third party (processor) to handle processing on its behalf, the controller must ensure that a written contract is entered into with the processor (Article 28 of the GDPR).

If the transfer to a third party is a transfer overseas, please see question 6 above.





Sweden

In Detail

8. What are the consequences of breaching privacy laws in your jurisdiction?

Depending on the nature of the breach, there are substantial fines for non-compliance with the GDPR:

- (a) Up to EUR 10 million or, in the case of an undertaking, 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher; and
- (b) Up to EUR 20 million or, in the case of an undertaking, 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

If the Swedish Data Protection Authority concludes that personal data are being processed or may be processed in an unlawful manner, the Authority may, for example, issue warnings, order corrective compliance measures and/or impose administrative fines.

Any person who has suffered material or non-material damage as a result of a breach of privacy laws shall have the right to receive compensation from the controller or processor for the damage suffered.

9. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee's personal data?

International data transfers

For multinational companies with affiliates in several countries around the world, the strict regulations regarding transfer of personal data outside the EU/EEA (please see question 6 above) must be observed in relation to intra-group data transfers.

Monitoring

The Swedish Data Protection Authority has issued non-binding guidelines (under the repealed data protection laws) regarding monitoring employees' use of computers, e.g., email and Internet. According to the Swedish Data Protection Authority, monitoring may be justified only under certain conditions. The Swedish Data Protection Authority has, however, taken the view it will not be permitted to make far-reaching analysis of the employees based on data collected in connection with monitoring activities. Furthermore, an employer would normally not have the right to intentionally access employees' emails marked private, except in cases where there is a serious suspicion of disloyal or criminal





Sweden

In Detail

behavior from the employee. If the employer monitors employees' use of computers, this should be clearly evident from regulations and information provided to the employees. It should also be made clear for the employees how the monitoring is carried out and for what purposes.

Whistleblowing hotline/system

The Swedish Data Protection Authority has taken the view that information regarding criminal offenses is likely to be processed in connection with a whistleblowing system. The Swedish Data Protection Authority has issued a specific ordinance which includes that the following requirements must be met:

- (a) The whistleblowing system shall be complementary to normal internal reporting routines and shall be voluntarily to use. The whistleblowing system shall only be used if there are objective reasons not to use normal internal reporting routines.
- (b) The scope of the whistleblowing system must be limited to serious irregularities in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime and other serious irregularities of vital interest for the company. Serious environmental offenses or lack of security at workplaces could also constitute a serious irregularity.
- (c) Only key or management personnel may be reported by the use of the whistleblowing hotline.
- (d) Requirements under personal data legislation must be met regarding, for example, providing information to employees, processing of sensitive data and data transfers to a third country.

Contributed by: Åsa Gotthardsson, Advokatfirman Vinge KB



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Switzerland



Contributed by: **Pestalozzi Attorneys at Law Ltd**



In Brief



In Detail

Contributed by: **Christian Roos**, Pestalozzi Attorneys at Law Ltd



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Switzerland

In Brief

1. Does employee data privacy law in your jurisdiction go beyond the GDPR?

The GDPR is – aside from its extra-territorial scope – not applicable in Switzerland. Swiss law, however, contains very similar provisions with regard to employee data privacy law and does not go beyond the GDPR (but may be more prescriptive in relation to retention periods). Furthermore, the Swiss Data Protection Act (the “DPA”) is currently under revision and it is assumed that the revised Act will largely adapt to the GDPR.

2. Is there a law regulating applicant personal data?

Applicant data are protected through the DPA and may only be kept for as long as the relation with the applicant is justified.

3. Is there a law regulating employee personal data?

Employee data are regulated under the DPA and Article 328b of the Swiss Code of Obligations.

4. Do I need to have a privacy statement or agreement?

No, there is no legal requirement to have a privacy statement or agreement under Swiss law.

5. How long must I retain employee data? What is best practice?

Employee data should be kept for at least five years from termination of employment as this is when salary-related employment claims become time-barred. However, it is best practice to retain employee data for 10 years from termination, as this is when the general statute of limitations lapses.

6. Can I transfer employee data overseas?

The transfer of employee data requires the employee’s consent and an agreement regarding the processing of the employee’s personal data that restricts the data processor abroad to only processing the data in the manner permitted for the instructing party itself (i.e., the employer) and guaranteeing data security should be in place before any transfer/disclosure takes place.

7. Can I transfer employee data to a third party?

The processing of an employee’s personal data may be assigned to third parties by agreement or by law, subject to certain conditions.

8. What are the consequences of breach?

The consequences of breaching Swiss privacy laws include a fine of up to CHF 10,000 per breach. The revised DPA will, however, provide for considerably higher fines in the future (potentially up to CHF 250,000 based on current discussions). Employees may also claim compensation for damages.

9. What are the main pitfalls?

The systematic or behavioral monitoring of employees is prohibited under Swiss law and is often a pitfall when certain security-related software is introduced in companies.





Switzerland

In Detail

1. To what extent does employee data privacy law in your jurisdiction go beyond the GDPR?

The GDPR is – aside from its extra-territorial scope – not applicable in Switzerland. Swiss law, however, contains very similar provisions with regard to employee data privacy law and does not go beyond the GDPR (but may be more prescriptive in relation to retention periods). Furthermore, the Swiss Data Protection Act (the “DPA”) is currently under revision and it is assumed that the revised Act will largely adapt to the GDPR.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant’s personal data in your jurisdiction?

According to the DPA, data may only be processed for the purpose indicated at the time of collection. Moreover, the data processing must be proportionate in time (please see Article 4 para. 2 and para. 3 of the DPA). A candidate applying for a job consents that his/her personal data are processed until the position is filled. Once the position is filled, the purpose for which the data were collected ceases to exist. It is, therefore, recommended – but there are no specific provisions or guidelines to be followed – that employers delete information relating to unsuccessful applicants within three months after the position is filled. Exceptions apply if (a) the candidate agrees that his/her data can remain stored in a kind of “talent pool” so that he/she can be contacted again in case of another vacancy, or (b) it is reasonably expected that a candidate will bring a discrimination claim. In the latter case, the candidate’s data may be kept for the purpose and as long as necessary to defend such claim.

For the same reasons, data obtained from vetting and background checks must also be deleted immediately after the background check has been made and the requested information has been received and acknowledged. Also for such data, no specific law, code or guidelines exist.

It should be noted that disclosure of an applicant’s personal data to third parties – even if within a group of companies – should be handled with care as this could constitute a violation of the applicant’s privacy. As a general rule, only if a legal obligation exists or if the applicant consents should an applicant’s personal data be disclosed by the employer to a third party. At least, the applicant should be informed before any disclosure/transfer so that he/she has a chance to object to it.

With regard to the disclosure and transfer of an applicant’s personal data outside of Switzerland, the general rules of Article 6 of the DPA apply. Please see question 6.



HOME

GDPR
OVERVIEW

COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Switzerland

In Detail

3. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee's personal data in your jurisdiction?

With regard to employee data privacy, there is one specific provision to note: Article 328b of the Swiss Code of Obligations (the “CO”). This Article provides that the employer may handle data concerning the employee only to the extent that such data concern the employee's suitability for his/her job or are necessary for the performance of the employment contract. Compliance with Article 328b of the CO constitutes part of the employer's obligation to protect the employee's personality rights.

Further, there is a useful document entitled “Guidelines with regard to the processing of personal data in the employment field” issued by the Federal Data Protection and Information Officer (latest version of October 2014; guidelines available in German, French and Italian).

4. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee's personal data?

No, there is no such requirement under Swiss law. It is, however, recommended that employers have a privacy policy in place and also refer to such policy in any employment contract.

5. For how long must an employer retain an employee's personal data? What is best practice?

An employee's personal data should be retained for at least five years from termination as an employee's claims regarding wage entitlement (including bonus payments, etc.) become time-barred after this period. It is, however, often recommended that employers retain employee personal data for 10 years from termination, as the general statute of limitation of 10 years applies to all contractual claims aside from wage entitlement claims. Any personal data that are, however, no longer needed for the purpose indicated at their collection (e.g., for the performance of the employment contract or respective claims based thereon) should be deleted earlier.

6. What are the legal restrictions on transferring employees' personal data outside your jurisdiction?

First, it should be noted that disclosure of an employee's personal data to third parties – even if within a group of companies – should be handled with care as this could constitute a violation of the employee's privacy. As a general rule, only if a legal obligation exists or if the employee consents should an employee's personal data be disclosed by the employer to a third party (including companies within the same group of companies). In any case, an agreement





Switzerland

In Detail

regarding the processing of the employee’s personal data that restricts the data processor abroad to only processing the data in the manner permitted for the instructing party itself (i.e., the employer) and guaranteeing data security should be in place before any transfer/disclosure.

With regard to the disclosure and transfer of an employee’s personal data outside of Switzerland, the general rules of Article 6 of the DPA apply. Data may, thus, not be disclosed abroad if the privacy of the data subject would be seriously endangered, in particular due to the absence of legislation that guarantees adequate protection. Countries considered not guaranteeing such adequate protection are, for instance, the United States, India or China. Before disclosing or transferring personal data to these countries, sufficient safeguards must be put in place, such as the conclusion of contractual clauses, the implementation of binding corporate rules (with regard to inter-company disclosures/transfers) or obtaining the data subject’s consent in the specific case. Another option to lawfully disclose data to the United States is the submission to the Swiss-US Privacy Shield, which is broadly comparable to the EU-US Privacy Shield Framework. EU legislation is considered to provide sufficient protection and disclosures/transfers of personal data from Switzerland to EU countries are generally unproblematic, at least as far as data processing on behalf of the Swiss data controller is concerned.

7. What are the legal restrictions on transferring employees’ personal data to a third party?

The processing of an employee’s personal data may be assigned to third parties by agreement or by law, provided (a) the data are processed only in the manner permitted for the instructing party itself (i.e., the employer as data controller) and (b) disclosure is not prohibited by a statutory or contractual duty of confidentiality. Further, the employer must in particular ensure that the third party guarantees data security.

With regard to transferring/disclosing an employee’s personal data to a third party located abroad, the prerequisites of Article 6 of the DPA as explained under question 6 above must additionally be met.

8. What are the consequences of breaching privacy laws in your jurisdiction?

The consequences of breaching Swiss privacy laws include a fine of up to CHF 10,000 per breach (please see Articles 34-35 of the DPA). The revised DPA will, however, provide for considerably higher fines in the future (potentially up to CHF 250,000, based on current discussions).

In addition, an employee may claim contract violation and/or a violation of his/her personality rights, which might lead to damages and moral tort compensation.





Switzerland

In Detail

9. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee’s personal data?

The monitoring of employees (which is prohibited under Swiss law if it is done systematically or constitutes a monitoring of an employee’s behavior) is a constant hot topic that needs to be approached with great care. Also, the processing of sensitive data in the employment context, such as health data, should be handled with care as the processing of sensitive data is specifically and rather strictly regulated under Swiss law.

Contributed by: **Christian Roos**, Pestalozzi Attorneys at Law Ltd

 [Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Turkey



Contributed by: **DAB Law Firm**



In Brief



In Detail

Contributed by: **Irmak Dirik Erunsal, Melis Buhan & Sezin Akoglu Duzenli**, DAB Law Firm



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Turkey

In Brief

1. Is there a law regulating applicant personal data?

Yes, the law numbered 6698 on Protection of Personal Data ("**Data Protection Law**"), enacted in 2016, protects the personal data of applicants as long as they are processed.

2. Is there a law regulating employee personal data?

Yes, the Data Protection Law, the Labor Code and the Code of Obligations.

3. Do I need to have a privacy statement or agreement?

The Data Protection Law states that the written explicit consent of the employee is required before their personal data can be processed, transferred or stored. However, the Law is silent on any particular form of document that an employer shall provide to its employees to obtain their written consent. However, in practice, the most common way is to cover the consent of the employees under an employment agreement or a data protection policy.

4. How long must I retain employee data? What is best practice?

As per the general principles of the Data Protection Law, personal data shall be kept for the time period stated under the relevant law or the time period necessary to process the personal data.

5. Can I transfer employee data overseas?

As per Article 9 of the Data Protection Law, as a general rule, the explicit written consent of the data subject/employee is required for overseas transfers. However, there are some exceptions to this rule.

6. Can I transfer employee data to a third party?

The Data Protection Law defines transfer of data to third parties within Turkey and abroad separately. Accordingly, the transfer of personal data to third parties is explained under the Data Protection Law and again, in principle, the explicit written consent of the data subject/employee is required. However, two exceptional cases do not require consent.

7. What are the consequences of breach?

Imprisonment and administrative fines.

8. What are the main pitfalls?

The explicit written consent of employees is required before employers can process, transfer, record and collect their personal data. Employment agreements, employment-related documents and policies should be reviewed and revised to reflect the processing of employee data.





Turkey

In Detail

1. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant’s personal data in your jurisdiction?

The Law numbered 6698 on Protection of Personal Data (“**Data Protection Law**”) regulates the provisions concerning protection of data privacy in the recording, processing and transmission of personal data, obligations of the entities processing personal data and the procedures and principles to be followed in this respect. The Data Protection Law defines “personal data” as any type of information of any real person whose identity is determined or may be determined. Accordingly, even though there is no specific reference to applicants under the Data Protection Law, the personal data of the applicants are also protected as long as they are processed. In this respect, the data requested from the candidates must be reasonable and such data must be stored as per the Data Protection Law. The applicant must be informed regarding the process of usage and storage of his/her personal data. In relation to a background and reference check, the explicit consent of the candidate must be obtained.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee’s personal data in your jurisdiction?

Yes, under Article 3 of the Data Protection Law, “personal data” is defined as any type of information of any real person whose identity is determined or may be determined. In this regard, real persons may be employees, business partners, clients, etc. The Data Protection Law also defines sensitive data. Accordingly, data relating to race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and dressing, membership of association, foundation or trade union, health, sexual life, criminal conviction and security measures, and biometrics and genetics are defined as sensitive data.

The Labor Code and the Code of Obligations also cover employee personal data. As per Article 75 of the Labor Code (Law No. 4857) (*published in the Official Gazette dated June 10, 2003 and numbered 25134*) “employers should keep a personnel file for each of their employees, in which they shall include, in addition to the identification details of the employee, all the documents and records that the employers are obliged to keep by law and present them to the authorized officials and offices as and when requested.” It also provides that “employers are obliged to use the information they gain access to regarding employees with integrity in line with the law and not to disclose any information, the confidentiality of which would be to the rightful benefit of the employee.”





Turkey

In Detail

Moreover, pursuant to Article 419 of the Code of Obligations (Law No: 6098) (*published in the Official Gazette dated February 4, 2011 and numbered 27836*), the employer may only use the personal data of the employee in the event that such data are related to the predisposition of the employee to the work or are required for the performance of the employment contract.

3. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee's personal data?

The Data Protection Law requires the written explicit consent of the employee before their personal data are processed, transferred or stored. However, it is silent on any particular form of document that an employer shall provide to its employees to obtain their written consent. However, in practice, the most common way is to cover the consent of the employees under an employment agreement or a data protection policy that the employees have consented to.

Moreover, as per the Labor Code, employers are under an obligation to keep the personal data of their employees in their personnel file and to use such personal data to the extent permissible by the employment contracts and employment relationship. Furthermore, as explained above, as per Article 419 of the Code of Obligations, the employer may use any personal data pertaining to the employee only to the extent related to his/her aptitude to work or necessary for performance of the employment contract.

4. For how long must an employer retain an employee's personal data? What is best practice?

As per the general principles of the Data Protection Law, personal data shall be kept for the time period stated under the relevant law or the time period necessary to process the personal data. Accordingly, employers shall comply with the time period stated under the applicable law or shall keep the personal data until the need to keep the data ceases to exist. Since the Data Protection Law and the Labor Code do not provide a specific timeframe for retention, the general provisions of the Code of Obligations shall apply which set out a time limit of 10 years. Moreover, as per the Data Protection Law, in the event that the need to keep the personal data no longer exists, then the personal data shall be deleted or destroyed by the individual/entity that keeps the data or as per the request of the data subject or be anonymized.

5. What are the legal restrictions on transferring employees' personal data outside your jurisdiction?

The Data Protection Law defines the transfer of data to third parties within Turkey and an overseas transfer separately. Principally, the explicit written consent of the data subject/applicant/employee is required for overseas transfers and





Turkey

In Detail

for the transfers made to third parties. However, the Data Protection Law introduces two exceptions to this general rule by taking into account the exceptions stated for the processing of personal data and sensitive data. The exceptions for the transfer of personal data without obtaining explicit consent of the data subject are regulated under (a) the second paragraph of Article 5 of the Data Protection Law, and (b) the third paragraph of Article 6 of the Data Protection Law, provided that adequate measures are taken.

Accordingly, as per second paragraph of Article 5 of the Data Protection Law, personal data may be transferred without explicit consent if:

- (a) it is explicitly stipulated under the laws;
- (b) it is necessary for the protection of the life or physical integrity of a person who is incapable of giving his/her consent or whose consent is legally invalid due to practical impossibility;
- (c) it is necessary to process the personal data of the parties of a contract, if it is directly related to the execution or performance of the contract;
- (d) it is imperative for the data controller to fulfill its legal obligations;
- (e) the data has been made public by the relevant person;
- (f) the data processing is imperative for the establishment, usage or protection of a right; or
- (g) it is imperative to process data for the legitimate interests of the data controller provided that the fundamental rights and freedoms of the relevant person are protected.

Sensitive data are also defined under the Data Protection Law (please see above). As an exception to the general rule, it is stated under the third paragraph of Article 6 that sensitive data, except for data concerning health and sexual life, can be processed without obtaining the explicit consent of the data subject if processing is permitted by any law. On the other hand, data relating to health and sexual life may only be processed without obtaining the explicit consent of the data subject for purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment, and care services, planning and management of health services and financing by persons under the obligation of secrecy or authorized institutions and organizations.





Turkey

In Detail

In light of the above, and the existence of the above-mentioned exceptions, the personal data of an applicant/employee may be transferred overseas or to third parties without obtaining their explicit consent.

In overseas transfers, even with the existence of the exceptions, the Data Protection Law requires that the foreign country to whom personal data are being transferred has an adequate level of protection. In the absence of an adequate level of protection, the data controllers in Turkey and abroad shall commit, in writing, to provide an adequate level of protection and the approval of the Data Protection Board must be obtained.

Furthermore, the Data Protection Law sets forth that, save for the provisions of international agreements, “in cases where the interests of Turkey or the data subject will be seriously harmed,” personal data may only be transferred abroad upon approval of the Data Protection Board. As the Data Protection Law is silent on the details of the enforcement of this Article, we anticipate that this matter will be clarified under secondary legislation.

6. What are the legal restrictions on transferring employees’ personal data to a third party?

As per the transfer of personal data to third parties, the exceptions outlined in question 5 above also apply.

The third parties that the personal data are being transferred to shall be the persons that are authorized to obtain or record personal data. Accordingly, the data processor or the data controller can be a real or a legal entity. As per the explanations of the Data Protection Board, the transfer of personal data within the same data controller shall not be deemed to be a transfer of data to third parties. Therefore, a transfer of personal data of the employees to the other departments of the same legal entity shall not be considered a transfer of data to third parties. However, the transfer of personal data to other entities existing under the same group of companies is considered a transfer of data to third parties and, accordingly, the rules stated under Article 8 of the Data Protection Law shall be applied.

7. What are the consequences of breaching privacy laws in your jurisdiction?

The relevant provisions of the Criminal Code numbered 5237 are applied to crimes committed against the protection of personal data. Accordingly, unlawful storage of personal data is subject to a penalty of imprisonment from one year to three years. Any person who illegally records personal data on another person’s political, philosophical or religious opinions, racial origins, illegal moral tendencies, sex lives, health or relations to trade unions shall be sentenced to a penalty of imprisonment from two years to six years.





Turkey

In Detail

In the case of unlawful transmission or reception of personal data, the penalty is increased to imprisonment from two years to four years. In the event that the above-mentioned crimes are committed by government officials or to facilitate the performance of a profession, the punishment shall be increased by half.

Furthermore, those who do not delete or destroy personal data despite the expiry of the time period stipulated in the relevant laws for the maintenance of such data shall be punished by imprisonment from one year to two years.

Please note that the investigation and prosecution of the offenses contained in this section are subject to a complaint from an individual, except in relation to the recording of personal data, unlawful collection of the data or failure to destroy the data.

The Data Protection Law also imposes administrative fines for certain misdemeanors:

Misdemeanors	Administrative Fines	
	Minimum	Maximum
Breach of the Obligation to Inform	TL 5,000	TL 100,000
Breach of Data Security Obligation	TL 15,000	TL 1,000,000
Failure to fulfill the Decisions of the Board	TL 25,000	TL 1,000,000
Breach of the Obligation to register with the Data Controllers Registry	TL 20,000	TL 1,000,000

8. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee’s personal data?

- The employees must be informed of the purpose, scope and methods to be used in the processing of their personal data and their explicit consent must be obtained.
- The employment agreements and other relevant employee-related documents should be reviewed and revised in terms of processing and storing of the personal data.
- The data protection and confidentiality policies and consent mechanism, especially for multinational companies whose servers are located abroad, must be reviewed and revised.

Contributed by: Irmak Dirik Erunsal, Melis Buhan & Sezin Akoglu Duzenli, DAB Law Firm

 [Link to biography >](#)



United Arab Emirates

Contributed by: **Mayer Brown LLP**



In Brief



In Detail

Contributed by: **Tom Thraya, Jad Taha & Omar El-Khattabi, Mayer Brown LLP**



[Link to biography >](#)



[Link to biography >](#)



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



United Arab Emirates

In Brief

1. Is there a law regulating applicant personal data?

There are currently no specific federal laws or regulations in the UAE that directly address data privacy, and there is no national authority in charge of regulating the collection of personal data.

The Dubai International Financial Centre (“**DIFC**”), a free zone in the Emirate of Dubai, issued a data protection law in 2007 (“**DIFC Data Privacy Law**”) that regulates applicant personal data and subjects it to the same restrictions as employee personal data.

2. Is there a law regulating employee personal data?

Please see response to question 1.

3. Do I need to have a privacy statement or agreement?

Privacy statements or agreements are generally not required in the UAE.

The DIFC, however, requires employers to issue either a privacy policy or agreement and obtain a written statement from employees consenting to the employer’s use and management of personal data.

4. How long must I retain employee data? What is best practice?

There are generally no legal requirements with respect to the retention of employee data. However, due to the statute of limitations on employment claims, it is advisable to retain such employment data for a period of five years for hard copies of data and 15 years with respect to data in electronic/digital format.

5. Can I transfer employee data overseas?

There are generally no federal restrictions on transfers of employee data overseas, although the DIFC Authority

requires (a) any jurisdiction receiving such employee data to be listed by the DIFC authorities as an acceptable jurisdiction and (b) the consent of the individual appointed by the employer to process such data (“**Data Controller**”), who must assess whether additional employee consent is required.

The Data Controller must notify the Commissioner of Data Protection of the DIFC (the “**Data Commissioner**”) when it is processing sensitive personal data and/or transferring personal data outside the DIFC to a jurisdiction that does not have adequate levels of data protection. If processing of personal data continues, the Data Commissioner must be notified annually.

6. Can I transfer employee data to a third party?

Please see response to question 5 – the same principles apply to the transfer of employees’ personal data to third parties.

7. What are the consequences of breach?

In the DIFC, breach of data privacy obligations may lead to penalties, damages and compensation owed to the non-breaching party.

8. What are the main pitfalls?

Employers should be aware that protected employee data may sometimes be accessible to third parties, exposing them to potential liability.

Those seeking clarity on the limitations and restrictions on data collection must also be attuned to a rapidly changing legislative landscape in the UAE, which might lead to reforms that impose additional data collection/management requirements on employers.





United Arab Emirates

In Detail

1. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant's personal data in your jurisdiction?

There are currently no specific federal laws or regulations in the UAE that directly address data privacy, and there is no national authority in charge of regulating the collection of personal data. The UAE Constitution, however, provides UAE citizens with a right to privacy in the context of personal correspondence. Article (31) of the Constitution provides for a general right of “freedom of corresponding through the post, telegraph or other means of communication and the secrecy thereof shall be guaranteed in accordance with the law.” Most commentators agree that this gives rise to an individual's general right to privacy. However, that right is limited to citizens of the UAE. Additionally, Article (378) of the UAE Penal Code (Federal Law 3 of 1987) criminalizes the publication of personal data that relates to any individual's private or family affairs.

The Dubai International Finance Centre (“**DIFC**”), a free zone in the Emirate of Dubai, issued a data protection law in 2007 (“**DIFC Data Privacy Law**”). The DIFC Data Privacy Law regulates the treatment of personal data but only with respect to the DIFC. The DIFC Data Privacy Law specifically extends to an applicant's personal data and, in practice, subjects this type of recruitment data to the same restrictions applicable to other forms of data collected from hired employees. These restrictions include the following: (a) processing data only with the consent of the applicant and when such data are either required by law to be processed or if it is necessary for the performance of a contract to which the applicant is a party and (b) transferring data out of the DIFC only when an adequate level of legal protection is afforded to the data in the jurisdiction receiving such data (and is listed by the DIFC authorities as an acceptable jurisdiction).

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee's personal data in your jurisdiction?

As noted above, there are currently no specific federal laws or regulations in the UAE that directly address data privacy, and there is no national regulator in charge of regulating the collection of personal data. The UAE Constitution, however, provides UAE citizens with a right to privacy in the context of personal correspondence. Additionally, the UAE Penal Code criminalizes the publication of personal data that relates to any individual's private or family affairs.

The DIFC Data Privacy Law regulates the treatment of employee personal data but only with respect to the DIFC. As with respect to applicant data, such restrictions include the following: (a) processing data only with the consent of the employee and when such data are either required by law to be processed or if it is necessary for the performance of





United Arab Emirates

In Detail

a contract to which the employee is a party and (b) transferring data out of the DIFC only when an adequate level of legal protection is afforded to the data in the jurisdiction receiving such data (and is listed by the DIFC authorities as an acceptable jurisdiction).

3. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee’s personal data?

There is generally no requirement in the UAE to have such a document. The DIFC, however, requires employers to issue either a privacy policy or agreement that sets forth the parameters of data collection and management and obtain a written statement from employees consenting to the employer’s use and management of personal data.

4. For how long must an employer retain an employee’s personal data? What is best practice?

A minimum of one year of employee data retention is recommended, as terminated employees can file claims relating to their employment for up to one year following their termination. However, it should be noted that other legal claims (e.g., criminal and civil) have longer limitation periods and therefore a longer retention period may be advisable (i.e., five years for hard copies of data and 15 years with respect to data in electronic/digital format).

5. What are the legal restrictions on transferring employees’ personal data outside your jurisdiction?

Employers in the UAE are generally permitted to transfer employees’ personal data outside of the UAE.

In the DIFC, however, the individual appointed by the employer to process such data (the “**Data Controller**”) is required to (a) notify the DIFC Authority (“**DIFCA**”) prior to sending any data outside the DIFC and (b) in the event that the ultimate destination of the personal data is not considered by the DIFCA to be an acceptable recipient of personal data, obtain the written approval of the Commissioner of Data Protection of the DIFC (the “**Data Commissioner**”). If the DIFCA concludes that the ultimate destination of the transferred data does not adequately protect such data, then employers must seek the consent of the relevant employee. If processing of personal data continues, the Data Commissioner must be notified annually.

Please note that such transfer of information should be deemed as a necessity (this includes, but is not limited to, disclosures of employee personal data relating to (a) the protection of the concerned employee, (b) the furtherance of claims in the context of a legal proceeding or (c) compliance with legal or regulatory requirements).





United Arab Emirates

In Detail

6. What are the legal restrictions on transferring employees' personal data to a third party?

The answer provided to question 5 above applies equally to the transfer of employees' personal data to third parties.

7. What are the consequences of breaching privacy laws in your jurisdiction?

In the event of a breach of the DIFC Data Privacy Law or any relevant privacy statement/agreement governed by DIFC law, an affected employee would be entitled to lodge a formal complaint with the Data Commissioner. The Data Commissioner would directly mediate any such conflict, reserving the right to issue an injunctive order or force a breaching party to pay damages, penalties or other compensation. The Data Controller may appeal any decision made by the Data Commissioner within 30 days of receiving such decision.

8. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee's personal data?

Employers collecting, using or managing employees' personal data should be aware that such data collection activities could be subject to the DIFC's data privacy requirements should they enter into an agreement that is governed by the laws of the DIFC, even in the absence of any other corporate or commercial activities in the DIFC. Additionally, please note the applicability of the DIFC Data Privacy Law in the event that third parties are granted access to personal data on employees other than through the disclosure of such information by employers.

Overall, the UAE is currently undergoing considerable legislative changes that could lead to either the promulgation of a formal data privacy legal regime or the imposition of additional data privacy requirements. Employers should also be aware that such legislative changes could occur specifically with respect to one of the UAE's free zones, requiring an in-depth study of the federal and free-zone legislative landscape prior to engaging in the collection, use or management of employee personal data.

Contributed by: **Tom Thraya, Jad Taha & Omar El-Khattabi**, Mayer Brown LLP



[Link to biography >](#)



[Link to biography >](#)



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



United Kingdom

(England & Wales)



Contributed by: **Mayer Brown International LLP**



In Brief



In Detail

Contributed by: **Nicholas Robertson & Katherine Fox, with input from Oliver Yaros**, Mayer Brown International LLP



[Link to biography >](#)



[Link to biography >](#)



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



United Kingdom

In Brief

1. Does employee data privacy law in your jurisdiction go beyond the GDPR?

The Data Protection Act 2018 (the “DPA”) (which, among other things, incorporates the provisions of the GDPR into UK law) goes beyond the scope of the GDPR in certain areas (e.g., in relation to special categories of personal data).

2. Is there a law regulating applicant personal data?

Although the legislation does not specifically refer to job applicants, the GDPR and the DPA extend to job applicants as they fall within the definition of “data subjects.” The DPA also covers the processing of personal data relating to criminal convictions in certain circumstances which often comes up in relation to job applications.

3. Is there a law regulating employee personal data?

Yes, both the GDPR and the DPA regulate the processing of employee personal data.

4. Do I need to have a privacy statement or agreement?

The GDPR and the DPA require employers to be transparent and therefore notify their employees about how their data are handled and processed. Privacy notices or privacy statements are generally used by employers to inform employees about how their data are collected, used, stored, transferred and protected.

5. How long must I retain employee data? What is best practice?

The general rule is that personal data should be kept no longer than necessary. The length of time for retaining data depends on the type of personal data and the purpose for which they are processed.

6. Can I transfer employee data overseas?

Transfers within the EEA are permissible in accordance with the conditions set out in the GDPR. Transfers outside the EEA are prohibited unless sufficient additional protections are in place.

7. Can I transfer employee data to a third party?

Yes, if done in accordance with the conditions set out in the GDPR and the employer is satisfied that the third party has appropriate safeguards in place to comply with the GDPR and the DPA.

8. What are the consequences of breach?

Under the DPA, the Information Commissioner’s Office can impose information, assessment and enforcement notices, and/or extensive fines. There are also potential criminal sanctions.

9. What are the main pitfalls?

- Compliance with particular requirements when handling special categories of personal data.
- Relying on consent as a lawful basis for processing employee personal data will be more difficult for employers. Consent has frequently been provided through the employment contract which is now unreliable.
- Procedures for handling data subject access requests.
- Transfers outside the EEA.





United Kingdom

In Detail

1. To what extent does employee data privacy law in your jurisdiction go beyond the GDPR?

The Data Protection Act 2018 (“**DPA**”) covers the processing of data for certain domestic purposes which are not covered by the GDPR (e.g., immigration, criminal law enforcement, and national security). In addition, the DPA also defines the role of the UK’s independent data privacy body, the Information Commissioner’s Office (“**ICO**”). In drafting the DPA, the UK exercised its discretion to deviate in certain areas as permitted under the GDPR, which means that the DPA may differ in these areas from other European Member States.

In relation to employee personal data, the DPA is largely reflective of the GDPR. It does, however, build on the provisions of the GDPR with regard to the processing of special categories of personal data (e.g., racial or ethnic origin, health data, biometric data). In particular, the DPA clarifies that the processing of special categories of personal data in connection with employment law will be permitted for the purposes of the GDPR if certain conditions are met. These are where:

- the processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the employer or employee in connection with employment;
- the employer has an appropriate policy in place when the processing is carried out; and
- the additional safeguards set out in Part 4 of Schedule 1 to the DPA are observed.

The DPA also requires employers to maintain an appropriate policy document in relation to processing data relating to criminal convictions for the purposes of employment.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant’s personal data in your jurisdiction?

The GDPR refers to “data subjects” which would include job candidates in the same way that it does employees. Employers require a lawful basis for processing a job candidate’s personal data. One of the bases that employers commonly rely on for processing employees’ and candidates’ personal data is a “legitimate interest,” according to which processing by the employer will be lawful if it is necessary for the purposes of the legitimate interests pursued by the employer; provided that such interests do not override the interests or fundamental rights and freedoms of the data subject. Employers are therefore permitted to collect, use and/or handle information related to the job application if they can show that processing is necessary to consider the candidate for the vacancy (i.e., the legitimate purpose).





United Kingdom

In Detail

The ICO guidance recommends that a legitimate interests assessment is carried out by an organization if legitimate interests are relied upon. This is an exercise that employers will need to be aware of and document.

There are separate provisions which apply to the collection of special category data, e.g., information relating to an applicant’s disability or racial or ethnic origin.

In addition, job applications frequently request details of any unspent criminal convictions. Under the GDPR, the processing of personal data relating to criminal convictions and offenses (which is treated under the GDPR and the DPA as a separate category of personal data to special category data) is completely prohibited. The only basis for processing this type of data is under the DPA. Under the DPA, an employer can process personal data relating to criminal convictions and offenses if it is necessary to do so in connection with employment, or it meets one of the conditions set out in the DPA, which include (but are not limited to):

- the individual consents to the processing;
- the processing relates to personal data which has been made public by the individual; or
- the processing is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), is necessary for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

Employers must be transparent with job applicants about the processing of their data, where it is stored, for what legitimate purpose and for how long, among other things. It is advisable that employers have a clear privacy policy/ notice addressing these points and others that are required under the GDPR (e.g., details of candidates’ rights to be forgotten, or to rectify or access their data) and that recruiters are obliged to provide this information to applicants. The DPA requires an “appropriate policy document” in place when processing special categories of personal data and criminal convictions.

There are also restrictions on the transfer of applicants’ personal data overseas and to third parties. Please refer to responses to questions 6 and 7 for further details which similarly apply to job applicants and employees alike. It may, however, be more difficult for an employer to show a legitimate basis for transferring a job applicant’s data than it would for an employee’s data.





United Kingdom

In Detail

3. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee’s personal data in your jurisdiction?

Yes, the DPA regulates the collection, use and/or handling of employees’ (who fall within the definition of “data subject”) personal data and special category data. Perhaps one of the most significant implications of the GDPR relates to an employer’s ability to rely on employee consent, which prior to the GDPR was often given through signature of the employment contract, as a basis for processing. Consent is no longer considered a reliable basis for processing personal data (except in certain limited cases). In particular, it is often not deemed to be genuine consent due to the imbalance of power in the employee-employer relationship. Instead, employers should have another lawful basis for processing personal data. In most cases, employers will rely on legitimate interest as the lawful basis (for processing employee data) or the fact that it is necessary in order to perform the contract, for example, processing of financial details in order to pay the employee, or compliance with a legal obligation.

If special category data (e.g., as noted above, racial or ethnic origin, health data, biometric data) are processed, there are additional considerations to take into account as this information requires a higher level of protection. Under the GDPR, the processing of special category data is prohibited unless there is a lawful basis for doing so. Examples of this include where (a) processing is necessary for the performance of the employment contract, (b) the employee has given explicit consent to the processing of his/her personal data for specified purposes, (c) the processing is necessary for reasons of the public interest (such as equal opportunities monitoring), and/or (d) the processing is necessary to assess an employee’s working capacity on health grounds, subject to appropriate confidentiality safeguards.

4. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee’s personal data?

A specific data protection agreement with the employee (or his/her consent) is not required to the extent that the handling of personal data is “necessary” to give effect to the employment relationship or for the purposes of hiring a job applicant. However, under the GDPR, employees and job applicants must be provided with specific information about how their personal data are processed. A privacy policy or statement is therefore frequently adopted by employers for this purpose.





United Kingdom

In Detail

If special category data and/or criminal convictions and offenses data are processed, under Schedule 1, Part 4 of the DPA, an appropriate policy must be in place which:

- (a) explains the employer's procedures for complying with the data protection principles in connection with the processing of the data; and
- (b) explains the employer's policies with regard to the retention and erasure of personal data processed, giving an indication of how long such personal data are likely to be retained.

Employers are also required to maintain a detailed record of how they process data and, where processing is likely to result in a high risk to the rights and freedoms of the employee, carry out a data protection impact assessment. This is a means for assessing and identifying any data protection risks within the employer's organization arising from data processing. In some circumstances, it is a requirement to carry out a data protection impact assessment before processing data – for example, in the case of adopting a new technology to be used for HR purposes.

5. For how long must an employer retain an employee's personal data? What is best practice?

The general principle is that personal data must be kept for no longer than is necessary for the purpose for which the data are processed. Employers should periodically review the data they hold and erase or anonymize it when they no longer need it.

There are exceptions to this principle which permit personal data to be stored for longer periods where it is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (and then only if there are appropriate technical and organizational measures to safeguard the rights and freedoms of data subjects). These may be unlikely to apply in an employment context.

In essence, what the data protection principles require of employers is a structured and methodical approach to obtaining data from employees from recruitment to termination. Only the data required for the employment relationship should be acquired, and they should then be stored securely and regularly reviewed to ensure they remain required, accurate and up to date. When data ceases to be required, they should be securely erased.

The GDPR does not specify retention periods for employee personal data and therefore it will be for employers to determine how long certain employee data should be retained, always bearing in mind the overriding principle that data should be retained for no longer than is necessary for the purpose for which it was gathered. For example, it is unlikely





United Kingdom

In Detail

that it would be necessary to retain an unsuccessful job candidate’s personal information for longer than 12 months. It is advisable that employers give thought to their practices around retention periods as the GDPR effectively requires employers to demonstrate, for each category of personal data, why it is being kept and the reasons behind the length of retention.

6. What are the legal restrictions on transferring employees’ personal data outside your jurisdiction?

The GDPR prohibits the transfer of employees’ personal data unless certain conditions are met. There must be an adequate level of data protection in the country to which data are transferred which is equivalent to the level required in the EU. If the country where the recipient of the data is located does not guarantee an adequate level of data protection, an employer must implement certain additional safeguards for the employees’ personal data before they may be transferred.

This will not present problems in the EU and the EEA given the application of the GDPR, however, outside of the EU, most countries are not considered to provide an adequate level of data protection. Generally, one of the legal safeguards or derogations must apply to ensure the legality of transferring data outside the EU. For example, the EU Commission has deemed a country to have an adequate privacy regime, standard contract clauses, EU model clauses, binding corporate rules, explicit consent in limited circumstances and, in respect of the United States, under the Privacy Shield. This has always been the position and the GDPR does not change this.

Once the UK leaves the EU, the GDPR will only apply in the UK as a result of the DPA. In terms of the effect this will have on data transfer, the DPA similarly prohibits the transfer of personal data outside of the UK unless certain conditions are met. In practice, however, the conditions under the DPA largely mirror the conditions under the GDPR. For instance, an employer will still be able to transfer personal data outside of the UK provided there is an adequate level of data protection in the country to which the data are transferred. Under the DPA, this condition will be satisfied if the EU Commission has determined that that country ensures an adequate level of protection of personal data. Employers will therefore not have to drastically change their approach to data transfer post-Brexit.

7. What are the legal restrictions on transferring employees’ personal data to a third party?

Generally, the position with regard to the transfer of employee data to third parties has not changed under the GDPR and the DPA. Transfers are permissible subject to appropriate steps being taken to protect personal data in accordance with the GDPR.





United Kingdom

In Detail

Where data are processed on behalf of the employer (i.e., the controller), employers must only use third-party processors (e.g., payroll companies) that provide sufficient guarantees that they have implemented appropriate measures to protect personal data. Employers need to ensure that processors agree to certain contractual requirements set out in the GDPR concerning the confidentiality of personal data, international transfers of personal data, audits, return of personal data and other requirements. This is most effectively done through the employer entering into an agreement with the third party which requires compliance with the GDPR.

8. What are the consequences of breaching privacy laws in your jurisdiction?

The ICO has extensive powers of enforcement under the DPA and the ability to sanction controllers and other persons for breach of privacy laws. These include both criminal and civil sanctions. The ICO also has powers of entry and inspection which it can rely on in order to search the premises of a controller or processor who is suspected of being in breach of the legislation under the DPA. The below list identifies the key criminal and civil sanctions which employers should be aware of (however this is not an exhaustive list of offenses under the DPA):

Criminal sanctions

New criminal offenses have been introduced under the DPA, including unlawfully obtaining personal data without the consent of the controller or deliberately altering or concealing information which should be provided in response to a data subject access request. It also continues to be an offense to knowingly or recklessly obtain or disclose personal data without the consent of the controller. Furthermore, directors, managers, secretaries, officers or other persons purporting to act in that capacity will also be found personally criminally liable where an offense has been committed by the body corporate and it is proved that the offense was committed with their consent, connivance or can be attributed to their neglect.

Financial sanctions

There are a range of administrative fines across two bands:

- Up to the greater of EUR 20 million or 4% of the total worldwide turnover of the preceding financial year in limited circumstances.
- In other cases, up to the greater of EUR 10 million or 2% of the total worldwide turnover of the preceding financial year.



HOME

GDPR
OVERVIEW

COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



United Kingdom

In Detail

The sanction to be applied should be effective, proportionate and dissuasive and take into account the nature, gravity and duration of the infringement, whether it was intentional or negligent, any repetition of infringements, and any adherence to a code of conduct or approved certification mechanism.

Notification requirements

There is a requirement for controllers to notify the ICO of a breach without undue delay and, where feasible, not later than 72 hours after becoming aware of a data breach. If the controller is not able to provide full details of the breach within that 72-hour window, the ICO advises that controllers should still notify the ICO within 72 hours of the reason for the delay and provide them with an indication of when they expect to provide more information about the breach. There are specific requirements as to what information should be provided with the notification to the ICO and therefore controllers are advised to have a plan prepared in advance to deal with any data breach.

Where a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, there is also a requirement for controllers to communicate the personal data breach to the data subject without undue delay.

9. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee’s personal data?

- The particular requirements when handling special category data. Please see answers to questions 3 and 4 above for further details.
- Employers will find it difficult to rely on consent as a lawful basis for processing employee personal data. Under the GDPR, employers have to meet a much higher threshold to show that the employee consented to the processing of their data. Employers will therefore need to rely on alternative legal justifications for processing employee data.
- Failure to have proper procedures in place to handle data subject access requests and data breaches. With a greater awareness of their rights, we have seen an increase in the number of requests made by applicants, employees and ex-employees to review the data which the employer has processed about them. The timeframe for responding to a data subject access request is now limited to 30 days unless the request is especially complex.
- Transfers outside the EEA. Please see the answer to question 6 above for more details.

Contributed by: **Nicholas Robertson & Katherine Fox**, with input from **Oliver Yaros**, Mayer Brown International LLP



[Link to biography >](#)



[Link to biography >](#)



[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 

Directory

 Belgium

Nicolas Simon

Van Olmen & Wynant,
Avenue Louise 221, 1050 Brussels, Belgium



+32 2 644 05 11



nicolas.simon@vow.be



<http://www.vow.be/team.html>

 Czech Republic

Petra Sochorová

Havel & Partners,
Na Florenci 2116/15, Recepcie A, 110 00 Prague 1 – Nové Město, Czech Republic



+420 255 000 111



petra.sochorova@havelpartners.cz



www.havelpartners.cz/en/team/counsel/73-counsel/32-petra-sochorova

 Czech Republic

Richard Otevřel

Havel & Partners,
Na Florenci 2116/15, Recepcie A, 110 00 Prague 1 – Nové Město, Czech Republic



+420 255 000 111



richard.otevrel@havelpartners.cz



www.havelpartners.cz/en/team/counsel/73-counsel/41-richard-otevrel



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 

Directory

 Denmark



Tina Brøgger Sørensen
Kromann Reumert,
Sundkrogsgade 5, 2100 Copenhagen OE, Denmark

 [+45 70 12 12 11](tel:+4570121211)  tib@kromannreumert.com

 en.kromannreumert.com/people/tina%20broegger%20soerensen

 Egypt



Sharif Shihata
Shalakany Law Office,
12 El Maraashly Street, Zamalek, Cairo, Egypt

 [+20 2 272 88 888](tel:+20227288888)  sshihata@shalakany.com

 www.shalakany.com

 France



Julien Haure
Mayer Brown,
10 Avenue Hoche, 75008 Paris, France

 [+33 1 53 53 36 48](tel:+33153533648)  jhaure@mayerbrown.com

 www.mayerbrown.com/people/Julien-Haure/



Directory

 France



Régine Goury
Mayer Brown,
10 Avenue Hoche, 75008 Paris, France

 [+33 1 53 53 43 40](tel:+33153534340)  rgoury@mayerbrown.com

 www.mayerbrown.com/people/regine-goury/

 Germany



Dr. Guido Zeppenfeld
Mayer Brown LLP,
Friedrich-Ebert-Anlage 35-37, 60327 Frankfurt am Main, Germany

 [+49 69 79 41 2241](tel:+496979412241)  gzeppenfeld@mayerbrown.com

 www.mayerbrown.com/people/dr-guido-zeppenfeld-llm/

 Germany



Björn Vollmuth
Mayer Brown LLP,
Friedrich-Ebert-Anlage 35-37, 60327 Frankfurt am Main, Germany

 [+49 69 79 41 1587](tel:+496979411587)  bvollmuth@mayerbrown.com

 www.mayerbrown.com/people/Bjorn-Vollmuth/



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 

Directory

Germany



Vanessa Klesy

Mayer Brown LLP,
Friedrich-Ebert-Anlage 35-37, 60327 Frankfurt am Main, Germany



+49 69 79 41 1283



vklesy@mayerbrown.com



www.mayerbrown.com/people/Vanessa-Klesy

Greece



Tania Patsalia

Bernitsas Law,
5 Lykavittou Street, GR-106 72, Athens, Greece



+30 210 361 5395



tpatsalia@bernitsaslaw.com



www.bernitsaslaw.com/lawyers/tania-patsalia/intellectual-property-data-protection-and-privacy=practices/

Hungary



Péter Szemán

Bán, S. Szabó & Partners,
H-1051 Budapest, József Nádor Tér 5-6, Hungary



+36 1 266 3522



pszeman@bansszabo.hu



www.bansszabo.hu/en/team/dr-peter-szeman



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 

Directory

 Iceland



Áslaug Björgvinsdóttir

LOGOS Legal Services,
Efstaleiti 5, 103 Reykjavík, Iceland



+354 5 400 300



aslaug@logos.is



<https://en.logos.is/the-team/partners>

 Ireland



Ailbhe Dennehy

A&L Goodbody,
International Financial Services Centre, North Wall Quay, Dublin 1, D01H104, Ireland



+353 1 649 2000



ALGDublin@algoodbody.com



www.algoodbody.com/our-people/ailbhe-dennehy

 Israel



Revital Shprung-Levy

Goldfarb Seligman,
Ampa Tower, 98 Yigal Alon Street, Tel Aviv 67891, Israel



+972 3 608 9853



Revital.Shprung-Levy@goldfarb.com



www.goldfarb.com/our-attorneys/revital-shprung-levy



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 

Directory

 Israel**Gal Sion**

Goldfarb Seligman,
Ampa Tower, 98 Yigal Alon Street, Tel Aviv 67891, Israel

 [+972 3 608 9853](tel:+97236089853)  Gal.Sion@goldfarb.com

 www.goldfarb.com/our-attorneys/gal-dayan-sion

 Italy**Francesco D'Amora**

Quorum Studio Legale e Tributario Associato,
Via Cino del Duca 5, 20122 Milan, Italy

 [+39 02 87 21 32 37](tel:+390287213237)  fdamora@quorumlegal.com

 www.quorumlegal.com

 Netherlands**Hermine Voûte**

Loyens & Loeff,
Fred. Roeskestraat 100, 1076 ED Amsterdam, Netherlands

 [+31 20 578 59 75](tel:+31205785975)  hermine.voute@loyensloeff.com

 <https://www.loyensloeff.com/en-us/our-people/hermine-voûte>



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 

Directory

 Norway



Christopher Sparre-Enger Clausen

Advokatfirmaet Thommessen AS,
Haakon VII's gate 10, 0116 Oslo, Norway



+47 23 11 11 11



csc@thommessen.no



www.thommessen.no/en/people/partners/christopher-sparre-enger-clausen/

 Poland



Agata Szeliga

Sołtysiński Kawecki & Szlęzak,
Jasna 26, 00-054 Warsaw, Poland



+48 22 608 70 06



agata.szeliga@skslegal.pl



www.skslegal.pl/en/zespol/agata-szeliga/

 Poland



Katarzyna Paziewska

Sołtysiński Kawecki & Szlęzak,
Jasna 26, 00-054 Warsaw, Poland



+48 22 608 71 92



katarzyna.paziewska@skslegal.pl



www.skslegal.pl/en/zespol/katarzyna-paziewska/



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 

Directory

 Russia



Markus Schaer

Secretan Troyanov Schaer SA,
Ulitsa Usacheva 33, Bldg. 1, 119048 Moscow, Russia



+74 95 232 03 01



markus.schaer@sts-law.ru



www.sts-law.ru/en/team_markus_schaer

 Saudi Arabia



Tom Thraya

Mayer Brown LLP,
Index Tower, Dubai International Finance Centre, Floor 11, Unit 1104, Dubai, United Arab Emirates



+971 4 375 7161



tthraya@mayerbrown.com



www.mayerbrown.com/people/Tahan-Tom-A-Thraya

 Saudi Arabia



Jad Taha

Mayer Brown LLP,
Index Tower, Dubai International Finance Centre, Floor 11, Unit 1104, Dubai, United Arab Emirates



+971 4 375 7166



jtaha@mayerbrown.com



www.mayerbrown.com/people/Jad-A-Taha



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 

Directory

South Africa



Ross Alcock

ENSAfrica,
150 West Street, Sandton, Johannesburg, 2196, South Africa



+27 11 269 7600



ralcock@ensafrica.com



www.ensafrica.com/lawyer/ross-alcock?Id=320&searchterm=ross%20alcock

Spain



Andrea Sánchez Guarido

Pérez-Llorca,
Paseo de la Castellana, 50, 28046, Madrid, Spain



+34 91 426 03 67



asanchez@perezllorca.com



www.perezllorca.com/en/lawyer/andrea-sanchez-2/

Sweden



Åsa Gotthardsson

Advokatfirman Vinge KB,
Box 1703, SE-111 87, Stockholm



+46 10 614 30 00



asa.gotthardsson@vinge.se



www.vinge.se/en/our-people/asa-gotthardsson/



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 

Directory

Switzerland



Christian Roos

Pestalozzi Attorneys at Law Ltd,
Loewenstrasse 1, 8001 Zurich, Switzerland



[+41 44 217 91 11](tel:+41442179111)



christian.roos@pestalozzilaw.com



<https://pestalozzilaw.com/en/lawyers/christian-roos/>

Turkey



Irmak Dirik Erunsal

DAB Law Firm,
Poyracık Sokak, Feza Apt. No.18/7, Nisantasi Sisli, Istanbul, Turkey



[+90 212 234 44 25](tel:+902122344425)



idirik@dablawfirm.com



www.dablawfirm.com/who-we-are

United Arab Emirates



Tom Thraya

Mayer Brown LLP,
Index Tower, Dubai International Finance Centre, Floor 11, Unit 1104, Dubai, United Arab Emirates



[+971 4 375 7161](tel:+97143757161)



tthraya@mayerbrown.com



www.mayerbrown.com/people/Tahan-Tom-A-Thraya



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 

Directory

 United Arab Emirates



Jad Taha
Mayer Brown LLP,
Index Tower, Dubai International Finance Centre, Floor 11, Unit 1104, Dubai, United Arab Emirates

 [+971 4 375 7166](tel:+97143757166)  jtaha@mayerbrown.com

 www.mayerbrown.com/people/Jad-A-Taha

 United Kingdom



Nicholas Robertson
Mayer Brown International LLP,
201 Bishopsgate, London, EC2M 3AF, United Kingdom

 [+44 20 3130 3919](tel:+442031303919)  nrobertson@mayerbrown.com

 www.mayerbrown.com/people/nicholas-robertson/

 United Kingdom



Katherine Fox
Mayer Brown International LLP,
201 Bishopsgate, London, EC2M 3AF, United Kingdom

 [+44 20 3130 3169](tel:+442031303169)  kfox@mayerbrown.com

 www.mayerbrown.com/people/Katherine-Fox/



Legal Statement

This publication provides information and comments on legal issues and developments of interest to our clients and friends. The foregoing is not a comprehensive treatment of the subject matter covered and is not intended to provide legal advice. Readers should seek legal advice before taking any action with respect to the matters discussed herein.

© 2018 Mayer Brown. All rights reserved.

Attorney advertising. Prior results do not guarantee a similar outcome.