A Regional Guide to Employee Data Privacy

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.

GDPR Overview

The new European General Data Protection Regulation[1] ("**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.

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

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.
  - **Erasure (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.

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.

Hungary

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

In Brief

In Detail

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

Link to biography >

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 >

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

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.