Employee Data Privacy – A Regional Overview

HUNGARY

A. Is there a law regulating employee personal data?

Act LXIII of 1992 on the Protection of Personal Data and Publicity of Data of Public Interest.

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

A privacy policy is not a requirement. However, an employee's consent to the transfer of personal data to a third party is required.

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

As a general rule, any personal data may be retained and processed only as long as it is necessary for the purpose of the data processing. For tax declaration and social security purposes, however, it is advisable to keep the tax and social security employee data at least until the relevant tax statute of limitations expires.

D. Can I transfer employee data overseas?

Yes, it is possible to transfer data overseas; however, employee consent is required plus the adequate level of data protection must be ensured.

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

Yes, it is possible with employee consent.

F. What are the consequences of a breach?

The Data Protection Commissioner may start an investigation and prohibit unlawful data processing. The data subject may also file a petition against the controller in the case of a violation of the data protection law.

G. What are the main pitfalls?

The data subject's approval for the transfer of his data to a third party (even within Hungary, the EU or overseas) is always a key requirement. Further, such transfer must be notified to the Data Protection Commissioner.

Contributed by Ban, S. Szabo & Partners

HUNGARY

A. 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 key legislation in Hungary regulating data protection issues is Act LXIII of 1992 on the Protection of Personal Data and Publicity of Data of Public Interest (the "**Data Protection Act**"). The Data Protection Act is a harmonized law with Directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data.

The territorial effect of the Data Protection Act covers all kinds of data controlling and processing that are carried out in the territory of the Republic of Hungary. Therefore, for the collection of personal data from Hungarian individuals, the provisions of the Data Protection Act are applicable.

The Data Protection Act defines the "personal data" as any information relating to the data subject and any reference drawn, whether directly or indirectly, from such information.

"Data controlling" means any operation or set of operations that is performed upon data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction, and blocking them from further use. The "data controller" is defined as a natural or legal person or unincorporated organization that determines the purpose of the data controlling, makes decisions regarding the data and implements such decisions itself or engages a processor to implement them.

"Data processing" means the technical duties in connection with the data, irrespective of the method and instruments used for such operations and the venue where it takes place. The "data processor" means a natural or legal person

or unincorporated organization that is engaged in the processing of personal data on behalf of a controller, including when ordered by virtue of legal regulation. The agreement between the data controller and the data processor must be incorporated into a written form. Any company that is interested in the business activity for which personal data is used may not be contracted for the processing of such data.

In addition, Act XXII of 1992 of the Labor Code contains some data protection aspects regarding the employee-related data, saying that only those data may be requested from the employee and only those data sheets may be required to be filled in which are essential for the purpose of the employment.

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

This is not a requirement in Hungary; however, it is standard in Hungary, especially at foreign-owned, multinational companies, that a global data privacy policy regulates all issues in connection with the data processing.

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

As a general principle, according to the Data Protection Act, any personal data may be retained and processed only as long as it is necessary for the purpose of the data processing. In case of employee-related data processing such period lasts from the commencement until the termination (expiration) of the employment, so at that stage, from a data protection perspective, the processing of the data should be stopped. However, from a tax and social security law perspective, it is necessary for all employers to keep the employee-related data, including the name, address, other personal data, salary data at least until the expiration of the relevant tax statute of

limitations period, that is generally 5-8 years. It may happen, however, that several years following the expiration of the tax statute of limitations period (e.g., prior to application for retirement) the pension fund requests further certificates from all employers of the given employees from the past social security payments. Therefore, as a best practice, the employee-related data, especially the salary, tax, social security payments, are retained by the employer without time limitation.

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

(i) Transfer of personal data to a member state of the European Union

In case of transfer of data to another member state of the European Union, the general rules of the data transfer are to be applied. Please see our answer at question E.

(ii) Transfer of personal data outside of the European Union

Data transfer to a data controller or data processor to a third country (i.e., outside of the European Union) is possible if

(a) the data subject has expressly given his consent to such transfer, or

(b) the law stipulates so, provided that the adequate level of protection is ensured at the third country.

(a) Consent of the data subject

The above regulation, in compliance with the Data Protection Directive, makes possible the transfer of personal data to a third country (i.e., outside the EU) only if the data subject has made express authorization for such data transfer. In our interpretation, this rule

means that the data subject, before making his consent, must be informed about all details of the data transfer (to which country will the data be transferred, what is the purpose of the data transfer, who will be the data controller or processor in that country, what kind of security measures are taken to ensure the protection of data, etc.). If the data subject consents, the adequate level of protection is not a requirement; however, the Data Protection Commissioner, in its practice, requires ensuring adequate level of protection in this case as well.

(b) Stipulation of law

The only other possibility of the data transfer which is not based on the consent of the data subject is the stipulation of the law, provided that the adequate level of protection is ensured. This adequate protection is ensured if

(i) the Commission of the European Union declares that the third country provides adequate protection;

(ii) an international agreement is in effect between the third country and the Republic of Hungary about the data subjects' rights, legal remedies and the independent inspection of the security measures relating to the data controlling and data processing; or

(iii) the data controller or data processor in the third country adduces by disclosing the rules of data controlling and data processing that he ensures the adequate level of protection; in particular, it carries out the data controlling or data processing

in compliance with the decisions of the European Union.

With respect to condition (a) above, the Commission Decisions of the European Union decided that the personal data may be transferred to the members states of the European Union and to the three EEA member countries (Norway, Liechtenstein and Iceland). The Commission has so far recognized Switzerland, Canada, Argentina, Guernsey, Isle of Man, the US Department of Commerce's Safe Harbor Privacy Principles, and the transfer of Air Passenger Name Record to the Unites States' Bureau of Customs and Border Protection as providing adequate protection.

The Commissioner provides that the decision mentioned under precondition (c) above, means (i) Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries (2001/497/EC), and (ii) Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries (2002/16/EC). Consequently, the data controller or processor in the third country must apply the standard clauses described in these two EU decisions.

In addition, the Commissioner confirmed that the adequate protection may be ensured by the application of Binding Corporate Rules for International Data Transfers (**"BCR"**). BCR may be used by multi-national companies for the transfer of personal data from one group company to another. BCR are international codes of conduct which ensure that adequate safeguards are put in place for the rights of the data subjects. The BCR should be approved by each data protection authority of the given country that is involved in the data transfer.

As a last solution, according to the Commissioner, the adequate level of protection may be ensured by ad hoc contractual terms that contain the details of the data transfer and the rights and obligations of the data transferor and data recipient companies.

In case of transferring data to any third party, an agreement must be concluded between the data sender and data recipient parties.

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

As a general rule, the transfer of personal data to any third party (third party means any party who is not the data controller, the data processor and the data subject) requires the consent of the data subject. According to the Data Protection Act, the data subject's consent means any freely given indication of his wishes by which the data subject

signifies his agreement to the controlling of his personal data without limitation or with regard to specific operations. The Data Protection Act does not require any special form of consent, it may be given in a written form, orally (by phone) or via the Internet (in an e-mail, or by clicking to the "Yes" or "Agreed" button).

The Data Protection Act requires written consent only in case of processing sensitive data (special data is, for example, data related to racial or national origin, nationality and ethnic status, political opinion or party affiliation, religious or other convictions of a person, as well as data related to health or criminal record.

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

The Commissioner may inspect the legality of the data controlling or data processing. The Commissioner may initiate such investigation based on either a notification received from a data subject or ex-officio. The Commissioner, during its investigation, controls whether the respective data protection rules are complied with. The Commissioner investigates the circumstances of the data controlling or data processing. The Commissioner may ask information from the data controller about all facts that are in connection with the data controlling, may ask for copies of the respective documents, and may become familiar with the data controlling. The Commissioner may enter into the premises where data controlling is taken place. The data controller has to answer to the recommendation of the Commissioner within 30 days.

In case the data subject finds that the controlling and the processing of his personal data is unlawful or the processed data is incorrect, he may turn to the data controller and ask to correct the data or cease the data controlling or processing.

Any data subject may turn to the Commissioner in case of unlawful data controlling or processing who investigates the case. The Commissioner may oblige the data controller or processor to cease such operation. The data controller must comply with this obligation within 30 days and must report to the Commissioner in writing concerning the measures taken. The Commissioner may also announce to the public the breach of the data protection rules.

If the data controller or processor fails to comply with the data protection provisions, the Commissioner may order that unlawfully controlled or processed data are blocked, deleted or destroyed, may prohibit the unauthorized controlling or processing, thus further suspending the unlawful data transfer. The controller, the processor or the data subject may ask for the court review of the resolution passed by the Commissioner.

The data subject may file a petition against the controller in case of any violation of his rights. The burden of proof of compliance with the laws lies with the data controller. The court, in its judgment, may order the controller to provide the information, to correct or delete the data, to fulfill the data subject's objection, or to disclose the data requested by the data subject. The court may also order the publication of its decision.

G. *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 case of transferring employee data to a centralized database (which is regular in case of international companies), the employee's consent to such transfer is definitely required. In addition, in case the data is transferred to a country outside of the European Union, the adequate level of data protection must be ensured by the recipient company.

As a further requirement, prior to the data transfer, a notification to the Commissioner is required about such transfer.

In case the employee personal data is used for any other purpose other than strictly in connection with the employment, the same procedure should be followed (employee's consent plus notification to the Commissioner.

The Data Protection Act provides that the data controller, and within their sphere of competence, the data processors, must implement adequate safeguards and appropriate technical and organizational measures to protect the personal data, as well as adequate procedural rules to enforce the provisions of the Data Protection Act and other regulations concerning confidentiality and security of data processing. The data must be protected against unauthorized access, alteration, transfer, disclosure or deletion as well as damage and accidental destruction. For the technical protection of personal data, the controller, the processor or the operator of the telecommunication or information technology equipment must implement security measures; in particular, if the processing involves the transmission of data over a network or any other means of information technology.

These rule is obviously require safe physical and/or electronic storing of the data that eliminates any risk of injuring, alteration or deletion of the data, thus further securing that the data should not be available for third parties. In the case of engaging a data processor, the "adequate safeguard" also means that the data processor must make these safety measures and confidentiality must be ensured (i.e., proper confidentiality and safeguarding provisions are necessary in the data processing agreement between the data controller and the data processor.)

Contributed by Ban, S. Szabo & Partners