

World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

Volume 9, Number 8

August 2009

Whistle-blowing hotline schemes from the perspective of Hungarian data protection laws

By Dr Zoltán Balázs Kovács, an Associate at Szecskay, Attorneys at Law, based in Hungary.

In this article, we briefly address the requirements under Hungarian data protection law for an employer to transfer personal data of its employees to the United States, and what conditions must be fulfilled when setting up a whistle-blowing hotline scheme at a Hungarian subsidiary.

Data transfer

According to Act no LXIII of 1992 on the Protection of Personal Data and the Disclosure of Information of Public Interest (the 'Act'), transfer of personal data to a country that is not a Member State of the European Economic Area (the 'EEA') is subject to the prior expressed (written) consent from the person whose personal data are to be transferred. The data transferor must obtain consent from the affected person(s) in each individual case. In the context of an employment relationship, the employer is required to obtain the expressed written consent from the relevant employee(s).

In addition, the personal data of a person may also be transferred to a non EEA member country if:

- the said transfer is permitted by a specific Hungarian law and

Dr Zoltán Balázs Kovács can be contacted at:
zoltan.kovacs@szecskay.com

- the laws of the relevant foreign country in question provide for an adequate level of protection for the management and processing of the personal data transferred.

Under the Act, the level of protection is deemed to be adequate if (a) the European Commission so determines (if, for instance, a US company wishing to receive the personal data is on the so-called 'Safe Harbor List' prepared by the US Department of Commerce); (b) there is a treaty in place between Hungary and the relevant foreign country in which the contracting parties guarantee each other an adequate level of data protection or (c) the data manager or processor verifies, by making available the rules it applies to data management and processing, that an adequate level of protection is ensured for (i) the personal data of those affected by data management and processing as well as (ii) their rights and the assertion of their rights (e.g. the data manager applies standard contractual clauses as referred to below or wishes to apply an ad hoc agreement on data transfer). Based on the stance of the Data Commissioner's Office (the 'DCO'), the US, in general, is not regarded as a country that ensures an adequate level of protection for data management and processing.

Based on the DCO's stance, in addition to obtaining the employees' express written consent to data transfer, the employer is required to fulfil the condition under clauses (a) or (c) above. If the standard contractual clauses attached as appendices to Commission Decision of June 15, 2001 on standard contractual clauses

for the transfer of personal data to third countries, under Directive 95/46/EC as amended by Commission Decision 2004/915/EC of December 27, 2004 (applicable in controller to controller relationship) or the standard contractual clauses attached to Commission Decision of December 27, 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (applicable in controller to processor relationship) are signed by the relevant parties (*i.e.* the employer and the other controller or processor), the signed standard contractual clauses do not need to be submitted to the DCO for approval. However, in the DCO's view, if an employer wishes to apply an ad hoc agreement governing the transfer of its employees' personal data to a non-EEA country, the draft agreement must first be submitted to the DCO for approval.

Registration requirement

According to Section 28 of the Act, 'prior to commencing operations, the manager/controller of personal data must notify the data protection commissioner of the following for the purposes of registration:

- a. the purpose of data processing;
- b. the category of data and the grounds for data processing;
- c. persons affected by data management;
- d. the source of data;
- e. the types of data transferred, the recipients and the grounds for transfer;
- f. the deadline for deletion of specific types of data;
- g. name and address (corporate address) of the data manager and the data processor, the place where records are kept and/or where processing is carried out, and the data processor's activities in connection with data management operations and
- h. the name of and contact information for the internal data protection officer.'

Pursuant to Section 30 of the Data Protection Act, 'data management shall not be reported to the data protection registry if data management concerns *e.g.* the data of employees, clients, members and/or students of the entity managing the data'. Nevertheless, pursuant to the prevailing stance of the DCO, an employer wishing to transfer the personal data of its employees to the US must register with the data protection registry (*i.e.* a report must be made).

Whistle-blowing hotline scheme

According to the DCO, the operation of the so-called 'whistle-blowing hotline scheme' is not subject to reporting obligation; however, the operation of such a scheme complies with Hungarian law only if all of the following requirements are met:

1. The scheme is in line with WP 117 of the Working Group 29;
2. Each and every employee must be aware of the existence and operation of the whistle-blowing hotline scheme at the employer and of the possible legal consequences of making a report (the persons affected by the report must be entitled to receive information, have their data corrected and deleted in accordance with the provisions of the Act, particularly, Sections 11–16 thereof);
3. The employees must be informed in detail and in a very precise manner of the existence and operation of the whistle-blowing hotline scheme;
4. If the external service provider qualifies as data processor under the Act, its services may be engaged by the employer. In this case, the external service provider may not make any decisions regarding the data and its role may only be strictly technical in nature (the data manager/controller, *i.e.* the employer remains liable also for data processing); and
5. The employees may not be required to use the whistle-blowing hotline scheme, *i.e.* they may not be ordered by the employer to make reports.

Based on the DCO's stance, if the employer wishes to set up a whistle-blowing scheme, it is advisable to set it up in a way that the system only receives reports made on a non-anonymous basis. This way, information on an employee making a report in bad faith will be provided to the employee affected by the report. As for reports made in good faith, adequate protection must be ensured for the employee making the report. This kind of non-anonymous scheme may prevent employees from making reports in bad faith.

The owner of the employer qualifies as a third-party for the purposes of the Act. Any personal data may only be provided to the owner if the person concerned gives his/her written consent. In the DCO's opinion, if the employer is not involved in the data provision process (*i.e.* the employee making the report provides the data directly to the owner of the employer), the employer is not liable for the data provision. However, the person making the report has to be aware that there are serious consequences (both civil and criminal) to making a report without written consent from the person concerned.

If the employer provides data to its owner without written consent from the person concerned, the employer is liable for the report. If the employer transfers data to its owner without such consent, the employer must take into account that some serious labour, civil and criminal consequences may apply depending on the gravity of the violation and the extent of damages caused.

Finally, it is worth noting that in the DCO's opinion, the whistle-blowing hotline scheme is a "*concept non grata*".

Conclusion

Under Hungarian law, the safest solution for a Hungarian entity wishing to transfer the personal data of its em-

employees to its US parent company is to (i) register with the DCO; (ii) obtain explicit (written) consent from the employee(s) to data management and transfer and (iii) unless the relevant US parent company is listed on the Safe Harbor List, apply any of the standard contractual

clauses referred to above or an ad hoc agreement on data transfer previously approved by the DCO.

The contents of this article are intended to provide only a general overview of the subject matter. Specialist advice should be sought for specific matters.