BACK TO DATAGUIDANCE

DataGuidance
GLOBAL GUIDANCE IN ONE

GUIDANCE NOTES

About The Author

Julius Zaleskis is an Associate with the largest Lithuanian independent Law Firm LAWIN Lideika, Petrauskas, Valiunas ir partneriai and PhD candidate at the Vilnius University in Lithuania. His practice focuses on privacy and data protection, information technologies, intellectual property, consumer protection, media and sports.

Julius advises leading international and local companies across various industries on all privacy and data protection related issues. He routinely works on such matters as data processing notification, overseas data transfers, direct marketing, online data protection, outsourcing, clinical data protection.

He educates Lithuanian businesses on privacy and data protection and speaks at the events organized by Lithuanian data protection authority on a regular basis. Julius also comments various privacy and data protection issues in local media

Julius Zaleskis holds LLM degree from the Faculty of Law, University of Vilnius (2010). He is fluent in English.

julius.zaleskis@lawin.lt

Lithuania - Employees' Data Transfers

Julius Zaleskis

5 July 2013

1. Legal Environment

Employees' data is protected in Lithuania within a general framework of data protection and the right to private life established by ***Article 22 of the Constitution of the Republic of Lithuania of 1992***. As a Member State of the European Union, Lithuania has implemented all applicable EU data protection laws.

Employees' data transfers in Lithuania are mainly regulated by the ***Law on Legal Protection of Personal Data No I-1374 of 1998*** (the DP Law). The DP Law implements the EU Data Protection Directive 95/46/EC and basically mirrors it with respect to basic definitions, applicability criteria, data quality principles, legitimate data processing criteria, data subjects' rights, data security and data transfers.

The DP Law does not provide for specific regulation on employees' data. In addition, there are no employees' data transfer-related case-law and codes of practice in Lithuania. Thus, data controllers have to follow the general data protection rules for ensuring legality in the area of employees' data transfers.

Data protection enforcement is mainly carried out by the State Data Protection Inspectorate (DPA). The enforcement authority supervises data controllers' activities when transferring employees' data, monitors the lawfulness of employees' data transfers and assists employees in implementing their rights.

2. Requirements for Data Transfers

2.1 Purposes of the transfers

The data controller must ensure that employees' data is transferred for the legitimate purposes specified in advance and is not transferred for purposes incompatible with them.

2.2 Legal grounds for the transfers

In order to transfer employees' data lawfully, the data controller has to rely on at least one of the following grounds for lawful data processing:

- consent
- conclusion or performance of a contract to which the employee is a party
- legal obligation to process the data
- protection of employees' vital interests
- exercise of official authority vested by law and other legal acts in state and municipal institutions, agencies, enterprises or a third party to whom the data is disclosed
- legitimate interests pursued by a data controller or by a third party to whom the data is disclosed, unless such interests are overridden by the interests of the employee.

The DPA examines consent given by an employee with scrutiny as the employee, being the weaker party, may not have given his/her consent of his/her free will. To make the consent given by employees valid, data controllers should ensure that refusal of consent cannot result in any negative consequences for employees.

In practice, in most of the cases the consent given by employees is not considered to freely given and, thus, invalid. Therefore the conclusion/performance of employment agreements and/or the legitimate interests of data controllers are usually used to justify transfers of employee data.

2.3 Sensitive Data

The data controller's abilities are restricted with respect to the processing and transferring of sensitive data of employees which are defined as the data concerning racial or ethnic origin of a natural person, his political opinions or religious, philosophical or other beliefs, membership in trade unions, and his health, sexual life and criminal convictions.

Following Article 5(2) of the DP Law, it is prohibited to process, including transferring, special categories of employees' data (sensitive data). However, there are some exceptions. The DP Law allows the controller to transfer sensitive employees' data provided they have given their consent. As explained above, the DPA considers that the consent of an employee, as the weaker party, may not have been given freely. Thus, the most suitable ground (exception) in practice to process and transfer sensitive employees' data is a specific statutory provision in the field of employment law enabling such processing.

Data controllers are also limited in transferring personal identification numbers which may not in any case be made public or used for direct marketing purposes. The personal identification number may be transferred with the consent of the employee. However, as mentioned above, the DPA usually does not accept the consent of the employee as given freely. Thus, in practice the most suitable exception to process, including to transfer, employees' identification numbers is a specific statutory provision enabling this.

2.4 Proportionality

The principle of proportionality should be ensured. Data controllers must only transfer

employees' data that is necessary to achieve the purposes of the transfer.

2.5 Informing the employees

As required by Paragraphs 1 and 2 of Article 24 of the DP Law, before transferring the data, the data controller must inform the employee thereof, except in the cases where laws or other legal acts determine a procedure for transferring such data and data recipients. The following information must be provided to the employee, except where he / she already has it:

- the identity and permanent place of residence of the data controller and his representative, if any (where the data controller or his representative is a natural person), or indicate the name, code and address of the registered office (where the data controller or its representative is a legal person)
- the purposes of the transfer or the intended transfer of the employee's personal data
- the recipients and the purposes of disclosure of the employee's personal data
- the personal data which the employee must provide and the consequences of his / her failure to provide the data, the right of the employee to have access to his / her personal data and the right to request for rectification of incorrect, incomplete and inaccurate personal data
- the sources and the type of employees' personal data which are or will be collected

2.6 Notification

According to the DP Law, the data may only be processed (including transfers) if notified to the State Data Protection Inspectorate. Usually it is considered that the processing of the employees' data (including transfers) related to daily employment relations falls within the exception of the requirement of notification.

2.7 Documenting Data Transfers

According to Article 6 of the DP Law, the employees' data will be transferred under the employees' data transfer contract between the data controller and the data recipient. The contract must specify the purpose for which the employees' data will be used, the legal basis for transfer and the receipt, the conditions, the procedure of use and the extent of employees' data that are transferred.

2.8 Data Transfers within the European Economic Area (EEA)

Data controllers can transfer employees' data within the EEA without any additional restrictions.

2.9 Data Transfers outside the EEA

Employees' data can be transferred outside the European Economic Area subject to authorisation by the State Data Protection Inspectorate, which is granted if the data controllers demonstrate an adequate level of legal protection for the data in the course of the transfer. The authorisation is not necessary where the transfer is based on the:

- employee's consent
- conclusion or performance of a contract between the data controller and a third party in the interests of the employee
- performance of a contract between the data controller and the employee or relevant pre-contractual measures
- important public interests or legal proceedings
- vital interests of the employee
- prevention or investigation of criminal offences
- public data file regulation

As the DPA considers that the employee, as the weaker party, does not usually give his / her consent freely, the consent of the employee will not usually be sufficient for the transfer of the employee's data without the authorisation.

Data controllers can demonstrate an adequate level of legal protection by using the following means which nevertheless do not eliminate the authorisation requirement:

- data transferred to countries which are whitelisted by the European Commission
- data transferred under the model clauses approved by the European Commission
- data transferred to US companies which have declared adherence to the Safe Harbor privacy principles
- data transferred within an international group of companies under the binding corporate rules, which are approved by the DPA

Data controllers should be aware that the DPA examines applications for authorisation with scrutiny and often requires follow-up clarifications notwithstanding that any of the above means are used.

3. Liability

The main liability for any violation of the data protection rules governing employees' data transfers, or breach of the rights of employees with respect to their personal data, is administrative in nature. The DPA has no power to impose penalties for violations, although it can issue a statement of an administrative offence following which the national courts can impose fines from LTL 500 (approx. € 143) to LTL 2000 (approx. € 571).

Administrative sanctions may only be applied to individuals while the entity as such may not be subject to administrative prosecution. If a company commits a violation, the officer responsible for data protection or the CEO of the company is held responsible for such administrative offence.

There are some criminal sanctions established for certain data and privacy related crimes, however to the best of our knowledge these have never been enforced in relation to employees' data transfers.

In addition, the employee affected by the breach of the DP Law is also entitled to claim pecuniary and moral damages. However, this is not common in practice.

4. Summary

To ensure legal compliance in the area of employees' data transfers, data controllers basically have to follow general data protection principles and rules, in particular:

- The data controller must ensure that employees' data is transferred for specified and legitimate purposes.
- When processing and transferring employees' personal data, the data controller should not rely on employees' consent which is usually not accepted by the DPA.
- The data controller must ensure that the transfer of the employees' data is related to the conclusion and / or performance of the employment agreement or, alternatively, based on the legitimate interests of the data controller.
- The data controller must transfer only such employees' data that is necessary to achieve the purposes of the transfer.
- Employees' sensitive data and personal identification numbers should be transferred only when stipulated by law.
- The data controller has an obligation to inform the employee about his/her data transfer.
- The data controller and the data recipient must conclude the employees' data transfer contract.
- Employees' data can be transferred outside the EEA subject to authorisation by the DPA.