Prepared by AmCham member

Amendment to Slovakia´s personal data protection act – a step forward

SQUIRE PATTON BOGGS

Slovakia is encountering another major change in the regulation of personal data processing. This time, however, it is welcomed by persons involved in personal data processing.

On April 15, 2014, an amendment to the Personal Data Protection Act came into effect. The obligations introduced by this Act, upon its adoption last year, have caused great consternation in business circles, and so this article provides an overview of the most significant changes brought by the amendment to this regulation.

Filing Systems – Notification is Sufficient

One of the most significant changes is the cancellation of the blanket obligation to register filing systems. It was replaced with an obligation to provide notification of a filing system to the Office for Personal Data Protection of the Slovak Republic. Such notification is not subject to payment of any fees, and is possible via electronic submission.

Under the amendment, it is sufficient to notify the Office of most filing systems. Filing systems subject to surveillance by the data protection officer don't even have to be notified (certain exceptions apply).

Statutory Body as Data Protection Officer? Yes!

The amendment allows the statutory body to perform the function of the data protection officer, i.e., the person responsible for supervising compliance in the course of processing of personal data, which has been welcomed with enthusiasm, mainly in smaller companies. Prior to the amendment's adoption, the law prohibited the statutory body or its member from performing this function.

It is also worth mentioning that, under the amendment, any controller processing personal data through entitled persons, regardless of their number, can designate the data protection officer.

Processing Without Consent – Specification of Conditions

A further change brought by the amendment is the specification of the conditions attached to the processing of personal data, without the data subject's consent. Prior to the amendment, it was permitted to process personal data without the data subject's consent, also if "such processing is necessary for protection of rights and interests protected by law of the controller or the third party". Such vague guidance led to problems of interpretation in practice. The amendment does not fully solve these problems, although it does specify when such processing is allowed – mainly where processing of personal data is "within the scope of protection of property, financial or other interest of controller" or where personal data is "processed for securing safety of the controller by surveillance cameras or similar systems."

A Temporary Worker Can Work with Personal Data

The amendment modifies the term "entitled person". The essence of the change is to extend the definition of entitled persons that come into contact with personal data to all persons in labor relationships, not only those in employment relationships, as it is currently defined. Under the amendment, "entitled person" includes any person who performs activity based on a work performance agreement, or an agreement involving work activity and more.

No Longer Joint Responsibility of the Processor

The amendment also removes the processor's obligation to notify the controller, in writing, if the processor discovers that the controller has apparently infringed the law in the course of processing personal data, and also to inform the Office for Personal Data if the controller does not rectify the situation within one month from the day of such a notification. The joint responsibility of the controller and the processor for violation of this obligation, and for any damage caused thereby, is also removed.

Certain Personal Data of Employees Can Be Provided

The amendment will extend the employer's authorization to disclose or make available, even without the subject's consent, certain personal data of the subject, including title, name, surname, workplace telephone number, email address, etc. as well as the provision of the above-mentioned personal data of employees. In practice, this means that the employer is entitled to submit such personal data to a third party for further processing. However, such provision of personal data may not result in violation of the respect, dignity and safety of the employee.

Security Directive is History

To remove the administrative burden of entrepreneurs in relation to personal data processing, the amendment cancels the obligation of the controllers or processors to prepare a security directive. The law, following the amendment's adoption, requires the documentation of security measures in the form of a security project, but only in a specific category of cases. While in other filing systems, the amendment does not determine the method of documentation of the security measures, the obligation to demonstrate the extent and contents of the security measures to the Office remains unchanged.

Last But Not Least – Fines

Anyone involved in personal data processing will undoubtedly welcome the fact that the amended law returned, in most cases, to allowing the Office to impose a fine for violation of the law when it has the option to do so, and also to decide whether it will actually impose that fine. According to the wording of the law prior to the amendment, the Office was obliged to impose any fine sanctioned by law, in the case of a violation of the law. Another reason to be pleased is a reduced maximum amount of fines for violation of the law, from €300,000 to €200,000.

Peter Devínsky,
Associate,
Squire Patton Boggs