

After the adoption of the new Personal Data Protection Act last year, Slovakia is encountering another major change in the regulation of personal data processing. This time, however, it is welcomed with pleasure by persons involved in personal data processing. On 15 April 2014, an amendment to the Personal Data Protection Act went into effect, which brings several major changes in personal data processing based on Act No. 122/2013 Coll. on Protection of Personal Data and on Amendments and Supplements to Certain Acts. The amendment was published in the Collection of Laws under No. 84/2014 Coll.

The legal regulation of personal data protection has become an important and closely observed topic for many entrepreneurs. As the obligations introduced by the law, upon its adoption, have literally caused hysteria in business circles, this publication provides an overview of the most significant changes brought by the amendment to the law.

Filing Systems – Notification is Sufficient

One of the most significant changes is the cancellation of the blanket registration of filing systems, 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 possible via electronic submission.

Under the amendment, it will be sufficient to notify the Office of most filing systems. Notification will no longer be necessary, however, for filing systems subject to surveillance by the data protection officer, except for filing systems that process personal data without the data subject's consent based on an exception of processing of personal data necessary for protection of rights and interests of the controller or the third party protected by law – such filing system will always be subject to the obligation of notification. The Office for Personal Data Protection retains the option of deciding that such filing system will be subject to special registration.

Replacing registration with mere notification not only reduces the administrative burden, but entrepreneurs welcome the fact that the notification is not subject to the payment of any fees.

Statutory Body as Data Protection Officer? Yes!

The amendment, welcomed with enthusiasm, mainly in smaller companies, also allows the statutory body to perform the function of the data protection officer, i.e., the person responsible for supervising compliance of the law in the course of processing of personal data. Prior to the amendment's adoption, the law prohibited the statutory body of the controller or a member of such body from performing the function of the data protection officer. By removing this prohibition, the amendment also removes the problem many companies have faced in deciding who to designate to perform the function of the data protection officer.

It is also worth mentioning that, upon the effective date of the amendment, any controller processing personal data through entitled persons, regardless of their number, will be able to designate the data protection officer. Until now, the controller could have designated the data protection officer only if it processed personal data through 20 or more entitled persons.

As mentioned above, where the controller empowers the data protection officer with the exercise of surveillance, it shall not be obliged to provide notification of most filing systems to the Office for Personal Data Protection.

Processing Without Consent – Specification of Conditions

A further change brought by the amendment is the specifications of conditions of processing of personal data without data subject's consent. Prior to the amendment it was permitted to process personal data without data subject's consent, as well as if "such processing is necessary for protection of rights and interests protected by law of the controller or the third party". Such vague guidance has brought interpretation problems in practice. The amendment does not fully solve these problems, though 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." Such processing is allowed only if fundamental rights and freedoms of the data subject, protected by the Slovak Data Protection Act, are not affected by such personal data processing. The proposed wording of the amendment originally included authorization for processing of personal data without data subject's consent also for purposes of monitoring of data subjects, reporting of malpractices at the workplace and for evaluation of work performance and efficiency of data subject. This wording was vetoed by the President – however, this does not mean that in reasoned cases such processing is not allowed.

A Temporary Worker Can Be the Data Protection Officer

Another change brought by the amendment is modification of the term "entitled person". The essence of the proposed 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" will include any person who performs activity based on a work performance agreement or an agreement involving work activity and more.

Pursuant to the law, the controller is obliged to instruct the entitled person about his/her rights and obligations in processing of personal data prior to executing the first operation with personal data by such entitled person. The amendment narrows the substance of such instruction of the entitled persons, namely to the minimum scope required by Directive 95/46/EEC. It will no longer be necessary to prepare the written record of the instruction of the entitled persons but it will be sufficient to prepare any record on the basis of which it will be possible to credibly prove that the instruction has been executed.

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, until such situation is remedied, perform only such operations with personal data as cannot be postponed, and if the controller does not rectify the situation within one month from the day notified by the processor, to inform the Office for Personal Data Protection of such fact. The joint responsibility of the controller and the processor for violation of this obligation, and for damage caused thereby, will also be removed.

Certain Personal Data of Employees Can Be Provided

Pursuant to the law, a controller who is the employer of a data subject may 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, as well as other data if necessary for the fulfilment of job duties of the data subject. The amendment will extend the employer's authorization also to provide the above-mentioned personal data of employees, which in practice means that the employer will be entitled to submit these personal data to a third party for further processing. However, the provision of personal data of an employee (as with disclosure or making it available) 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 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 of the controller or processor to demonstrate the extent and contents of the security measures to the Office for Personal Data Protection remains unchanged.

Last But Not Least – Fines

Anyone involved in personal data processing will undoubtedly welcome the fact that the amended law will return, in most cases, to allowing the Office for Personal Data Protection, when it has the option to impose a fine for violation of the law, to decide whether it will actually impose that fine. According to the wording of the law prior to 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 for fines for violation of the law, from €300,000 to €200,000.

The amendment also involves further, minor changes mostly in order to harmonize the remaining provisions of the law with the above-mentioned significant changes. Should you have any questions regarding legislative changes brought by the amendment or require preparation of an overview of changes tailored to the needs of your company, please do not hesitate to contact a Squire Sanders lawyer at any time.

Contact

Peter Devínsky

Associate/ Advokát

T +421 2 5930 3411

E peter.devinsky@squiresanders.com

The contents of this update are not intended to serve as legal advice related to individual situations or as legal opinions concerning such situations nor should they be considered a substitute for taking legal advice.

© Squire Sanders.