May 2017

Balcar, Polanský & Spol. s.r.o.'s

School of Data Privacy

Regulation (EU) 2016/679 of the EP and of the Council of 27 April 2016, the General Data Protection Regulation (the "GDPR") replaces Directive 95/46/EC (the "Directive"), which currently forms part of Slovak law through Act no. 122/2013 Coll. and part of Czech law through Act no. 101/2000 Coll., the Data Protection Act. The GDPR will come into effect on 25 May 2018, when it will be directly applicable throughout the EU. It will apply to those who process personal data, as well as to natural persons whose personal data is the subject of processing.

To help you navigate the maze of obligations introduced by the GDPR, we have created a regular weekly news series on this topic, which is without a doubt the most important legislative change in European history in the field of data protection.

If you wish to receive the School of Data Privacy series directly to your e-mail box, please subscribe at office@bapol.sk or office@bapol.cz, or by calling the phone number +421 220 251 311 and +420 251 009 111.

Lesson 10 of 16

Security of personal data and personal data breach

Below you will learn:

Important changes

- Controllers will have a dual notification obligation in case of a personal data breach, i.e. towards the supervisory authority and towards the data subject;
- Controllers will be obliged to keep records of personal data breaches.

Compliance Action Plan

- Controllers and processors must implement appropriate security measures to protect the processed personal data;
- For this purpose it will be necessary to thoroughly review the circumstances of the processing in cooperation with IT technicians (e.g. for the purpose of implementing data encryption);
- Implementing internal policies in case a personal data breach is detected is recommended;
- Insurance for the consequences of a potential personal data breach is also recommended;

- Contracts with suppliers which contain the processing of personal data (e.g. payroll, accounting services) should contain provisions on liability for security of personal data[1].

Security of personal data

The GDPR sets out a minimum standard of personal data protection when processing, through several instruments or measures, which the controller is obliged to implement[2]. Considering the aim of the GDPR, it is clear that the main purpose of the new legislation regulating the processing of personal data is to ensure its security and minimize risks – not only from the consequences of human actions (intentional or by negligence, internal at the controller or the processor or external from other entities), but also natural causes or technical malfunction – related to various processing operations.

The GDPR regulates the controller's obligations connected with the security of personal data so that the controller (and processor) is obliged to implement appropriate technical and organisational measures with the aim to ensure an adequate level of security, including confidentiality, appropriate to this risk. These measures can include:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The GDPR sets out the above mentioned security measures as examples, i.e. the controller may also determine other more suitable measures to ensure the security of the data pursuant to their specific conditions. The GDPR lays out the state that the controllers and processors should aim for, but not necessarily the measures. However, they must implement these measures taking into account:

- *the state of the art* – in order to ascertain what options for protecting personal data exist at the moment of determining the security measures, it is suitable that the controller consults the available means of protection with IT specialists. The measures must be of a certain professional level. It is recommended to review these on a regular basis; if during the processing of personal data the level of knowledge of the security measures increases, the controller might be in breach of the GDPR due to the obsoleteness of the security systems;
- *the costs of implementation* – when implementing specific measures the controller considers their costs. However, not implementing appropriate measures due to their financial, personal or time demanding character would not be a relevant argument;
- *the nature, scope, context and purposes of processing* – when determining what security measures the controller implements, he/she must thoroughly consider all circumstances of processing personal data at the time, when the processing is carried out. These circumstances must be reviewed from time to time with regard to the changing conditions of processing;

[1] Agreement on processing is considered a part of the security measures.

[2] These include, in particular, the obligation to keep records of processing activities, the obligation to implement appropriate technical and organizational measures, the obligation to notify the authority and data subjects of a personal data breach, impact assessment on the protection of personal data; previous consultations with the supervisory authority, etc.

- risk of varying likelihood and severity for the rights and freedoms of natural persons – this is an important aspect of processing, whereby the controller is obliged to carry out an evaluation of any potential security risks connected to the processing, which may have a negative effect on the rights and freedoms of natural persons. This evaluation of risks should be carried out especially with regard to risks connected to automated processing (e.g. hacker attacks, IT malfunction, unauthorised or unprofessional interference of third persons into the processing) and with regard to risks connected to the environment in which the data is located (e.g. security of buildings and areas, fire prevention measures, accessibility of servers and other data storage rooms, etc.). When assessing the appropriate level of security, special consideration should be taken regarding the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed[3].

Which specific security measures the controller eventually implements should be a result of a detailed assessment of the circumstances of the processing in the conditions of the specific controller or processor.

A substantial change is introduced with the GDPR's effectiveness, being that controllers will no longer have to elaborate security projects[4] or security documentation[5] as previously required. Instead – where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons – the controller will have to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (*"privacy impact assessment", "PIA"*) prior to the processing, or to consult with the supervisory authority pursuant to Articles 35 and 36 of the GDPR. This obligation will apply in specific cases, e.g. with large scale systematic monitoring of publicly accessible areas, large scale processing of special categories of personal data or of personal data relating to criminal convictions and offences referred, profiling or automated decision making, etc.

For purposes of ensuring and demonstrating the implementation of security measures it is possible that the controller adheres to an approved code of conduct[6] or an approved certification mechanism[7]. Also, the controller must ensure that any natural person acting under the authority of the controller, who has access to personal data (currently a so called "entitled person"), processes it only based on the controller's instructions, unless he or she is required to do so by Union or Member State law.

A substantial obligation of the controller and processor will be the detailed supervision of the performance of the implemented measures and the data protection officer's obligations. The PIA or a consultation with the supervisory authority and the subsequent implementation of technical or organizational security measures will not be sufficient.[8]

Notification of a personal data breach

However responsibly the controller approaches the protection of personal data processed by them, the risk of a personal data breach will probably still not be completely mitigated. Such personal

[3] Article 32(2) of the GDPR.

[4] Article 20 of Act no. 122/2013 Coll., the Data Protection Act as amended (Slovak).

[5] Article 13 (2) of Act no. 101/2000 Coll., the Data Protection Act as amended (Czech).

[6] Article 40 of the GDPR.

[7] Article 42 of the GDPR.

[8] The supervision does not have to be specifically data protection oriented; it can be a part of exercising the rights and duties of managing employees to supervise the work of subordinate employees within an employment relationship. It is also possible to use standard automated means, such as logs (recording of access of a specific person into a system).

data breach may be an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed[9].

In relation to a personal data breach the GDPR regulates two types of the controller's notification obligation:

a) *Notification of the personal data breach to the respective supervisory authority*

In case of a personal data breach the controller is first of all obliged to notify the supervisory authority competent in accordance with Article 55 of the GDPR. This notification must be carried out without undue delay, but where feasible not later than 72 hours after having become aware of it. Where the notification is not made within the stated period, it must be accompanied by reasons for the delay.

Where and in so far as the controller cannot from objective reasons provide the supervisory authority the requested information at the same time, the information may be provided in several phrases without undue further delay.

The notification must at least:

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The controller does not have to notify the supervisory authority if the personal data breach is unlikely to result in risks for the rights and freedoms of natural persons.

b) *Notification of the personal data breach to data subjects*

If a personal data breach occurs which is likely to result in a high risk to the rights and freedoms of natural persons, the controller must communicate the personal data breach to the data subject. This communication must occur without undue delay.

In the communication to the data subject the controller states in clear and plain language the nature of the personal data breach and at least the following information and measures:

- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- the likely consequences of the personal data breach;
- measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Also in this case the GDPR sets out an exception from the notification obligation. The communication to the data subject is not required if any of the following conditions are met:

- the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

[9] Article 32(2) of the GDPR.

- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
- it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so.

Documenting personal data breaches

☐mong the above mentioned notification obligations the controller is obliged to internally document each occurrence of a personal data breach, including circumstances related to the breach, its effects and remedial action taken, and to maintain these records.

Also, the controller must keep a certain communication (i.e. documentation) standard in relation to the notification of the personal data breach to the supervisory authority and to the data subjects (please see above the requirements of such notifications).

What now

Prior to the GDPR's effectiveness, controllers and processors should review their current internal technical and organizational measures with regard to the new requirements, evaluate the risks with regard to the current state of the art, the costs of implementation and the nature of processed personal data, update their current security measures and supervisory and liability mechanisms and ensure due record keeping and procedures for a timely notification of potential security incidents. If they detect a high risk for the rights and freedoms of natural persons, a PIA should be undertaken or the Authority should be consulted. The controllers and processors should be able to demonstrate and justify these steps retroactively, to demonstrate and prove that they are not liable for potential damages under civil law (damage caused to a data subject), administrative law (for an administrative tort) or criminal law (e.g. for the crime of unlawful handling of personal data).

Further information can be found here:

Recitals 83 - 94

Articles 32 – 34

Contact person

For further information, please contact:

Slovakia:

JUDr. Helga Maďarová, CIPP/E
Attorney |Certified Intl. Privacy Professional/Europe

Tel.: +421 220 251 311
Cell: +421 917 092 076

helga.madarova@bapol.sk

Czech Republic:

JUDr. Jaroslav Srb
Attorney

Tel.: +420 220 251 111
Cell: +420 731 609 510

jaroslav.srb@bapol.cz