March 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.cz, or by calling the phone number +420 251 009 111.

Lesson 2 of 16

Data Protection Principles

Below you will learn:

Important changes

- As a result of the new accountability principle, companies / institutions processing personal data on their own behalf (controllers) will not only have to comply but also be able to demonstrate that they process personal data in compliance with data protection principles.

Compliance Action Plan

Prior to the GDPR taking effect, controllers should:

- audit the processing of personal data aimed at new obligations;
- create (or update existing) internal rules regulating processing, update the work rules regarding employee monitoring and protection of their personal data, revise employment contracts of employees having access to personal data as well as other documents related to processing;
- ensure and be able to demonstrate employees authorised to access personal data are trained regarding their rights, obligations and the consequences of breaches in relation to themselves and the employer.

Regarding Data Protection Principles

The data protection principles set out by the GDPR are similar to those outlined by the Directive, which are contained in Act no. 122/2013 Coll. and in Act no. 101/2000 Coll., the Data Protection Act. However, the GDPR further specifies and extends them.

Lawfulness, Fairness, Transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

For purposes of the transparency principle, companies / institutions will have to comply with the obligation to provide data subjects, whose personal data they process, with an extensive package of information. They should inform the data subjects in a clear and understandable manner on the conditions of processing and the rights the data subjects enjoy in relation to this[1].

In comparison to the Directive, the list of information that the controllers must demonstrably provide to data subjects prior to processing is significantly broader and among other things includes the right to erasure (i.e. right to be forgotten[2]), the right to object and to file a complaint with the supervisory authority and the right not to be subject to a decision based solely on automated processing, including profiling[3]. Needless to say, among the information on one's rights, data subjects must be notified of the conditions of processing, including the purposes of processing and the legal grounds (e.g. consent, legal requirements, etc.). We will cover the notification obligation in a separate Lesson.

Purpose limitation

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes[4]. In contrast to the actual legislation, further processing for another purpose than that for which the personal data was collected will be permissible under certain conditions. This is a substantial change in Czech and Slovak conditions of processing and means that if the controller collected personal data for a specific purpose, they may process such data for other purposes, if they meet certain conditions.

Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes are not considered to be incompatible with the initial purposes. However, this applies only if the controller ensures appropriate safeguards for data subject's rights and freedoms. For this purpose, the controller or processor should adopt

---

[1] Secret and invisible installed spyware is considered to be illegitimate processing (see the case of a website operator who publishes the e-mail addresses of participants in an internet discussion; WP 29 the Working party on the protection of individuals with regard to the processing of personal data).

[2] So far this has only been judicially laid down by the CJEU, see C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González. The dispute between Google and P. González, who wished to erase an unpleasant episode from the public consciousness; in the press was published information about the forced sale of his property because of an outstanding debt to social insurance, which was subsequently repaid. The Spanish office has ordered Google Inc. to take the necessary measures to remove the personal data relating to p. González from its index and prevent access to that information in the future.

[3] See Article 4, para. 4 of the GDPR, i.e. "*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*".

[4] I.e. it is a general prohibition of further processing for secondary purposes, incompatible with the primary purpose, whereas "*compatibility*" means "*direct relation*" to the primary purpose.

technical and organisational measures such as data minimisation, pseudonymisation[5] or anonymisation.

From our point of view, the processing of personal data collected while dealing with an offense for secondary purposes such as e.g. publishing in a local periodical or via the Internet, or publishing information about the existence of a debt of the owner of an apartment which was primarily processed with respect to administrative issues regarding the house, or disclosure of the collected personal information of individual tour participants to other passengers without their consent, will continue to be considered processing incompatible with the primary purpose.

Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

The adequacy of personal data in relation to the purpose of processing is not always easily defined. To determine whether the processing of certain personal data is adequate will require assessing whether the invasion of data subject's rights, which will occur as a result of processing, is adequate to the legitimate purpose of processing. If the processing of certain personal data for a specific purpose proves excessive, such processing would not be compliant with the GDPR. For example, it would be obviously inadequate to process a data subject's birth number for marketing purposes, since this it is not necessary to process this information for such purpose.

Accuracy

Personal data must be accurate and, where necessary, kept up to date. The controller must ensure that inaccurate personal data is erased or rectified without delay.

Storage limitation

Personal data must be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by this Regulation, in order to safeguard the rights and freedoms of the data subject.

The opinion of the Czech Data Protection Authority, under which operating a camera system at a permanently protected private facility the permissible time limit is e.g. 24 hours (but not exceeding several days), will still be valid. Restrictions will not apply to records acquired by the Czech Police under special legislation or in the event of a security incident when the record will be provided as evidence to the competent authorities for further proceedings.

Integrity and confidentiality

Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Accountability

The controller is responsible for processing personal data in line with the principles explained above, and he/she must be able to demonstrate compliance. To demonstrate compliance, it is

[5] See Article 4, para. 5 of the GDPR, i.e. *"the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."*

possible to execute written documents stating that all aspects of the processing operations within the company or the institution were internally assessed, and the result of the assessment was compliance with the GDPR's provisions.

The GDPR introduces new concepts of *data protection by design* and *data protection by default.*

Data protection by design means that the controller, with regard to various aspects of processing (e.g. the state of the art, the nature, scope, and purposes of processing, risks arising to the data subject's rights) must prior to the start of processing adopt appropriate technical and organisational measures and safeguards for the protection of personal data, and to adapt these from time to time to the actual conditions of processing. In other words, this concept obliges all companies / institutions processing personal data to carry out an internal audit of processing personal data. This requires controllers to proactively deal with the protection of personal data and to set aside human resources and financial and technical resources to assess the lawfulness of the processing and implement measures for its protection.

Data Protection by default means that the controller ensures only the personal data that is necessary for each specific processing purpose is processed. They should ensure that by default, personal data is not made accessible, without the individual's intervention, to an indefinite number of natural persons.

If the controller processes personal data through another person (processor), such person is obligated to process personal data only based on the controller's instructions, unless required to do so by Union or Member State law.

What now

All concerned companies / institutions should carry out an audit of processing personal data to ensure compliance, but also to ensure that they have the ability to demonstrate that personal data is processed with professional care, and to adopt organisational and technical measures and safeguards for this purpose. Suggestions for ensuring this can be found above in the part Compliance Action Plan.

Further information can be found here

Recitals 39, 40, 22

Articles 5, 6, 24, 25, 29, 89(1)

Contact person

For further information, please contact:

Czech Republic:

JUDr. Jaroslav Srb
Attorney

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

jaroslav.srb@bapol.cz

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