June 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 15 of 16

Sanctions and derogations

Below you will learn:

Important changes

- The GDPR substantially increases the maximum fines for the breach of obligations connected to personal data protection:
    - in cases of a more grave breach of the GDPR, the maximum amount of the fine is EUR 20,000,000 or, in the case of an undertaking, 4% of the of the total worldwide annual turnover of the preceding financial year (whichever is higher); the fine is up to CZK 10 million (Czech Rep.) and EUR 200,000 (Slovakia) so far;
    - in other instances, the maximum amount of the fine is EUR 10,000,000 or, in the case of an undertaking, 2% of the of the total worldwide annual turnover of the preceding financial year (whichever is higher); the fine is up to CZK 5 million (Czech Rep.) and EUR 50,000 (Slovakia) so far;
- The supervisory authority is not obliged to impose a fine for breach of the GDPR. However, if it is appropriate and purposeful with regard to the circumstances of the case, it may impose a difference measure (in addition to the fine or instead of it).

Compliance Action Plan

- Auditing the processing of personal data and accessing which processing operations are not compliant with the GDPR;
- Identifying areas with the highest risk and carrying out actions for mitigating the risk of fines;
- Considering the option to conclude insurance contracts for insuring the risks connected to personal data processing.

Sanctions

Administrative fines

When deciding whether to impose an administrative fine and its amount the supervisory bodies must give due regard to circumstances such as e.g. the nature, gravity and duration of the infringement (taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them), the intentional or negligent character of the infringement, any action taken by the controller or processor to mitigate the damage, the degree of cooperation with the supervisory authority, the categories of personal data affected by the infringement, etc.

If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of the GDPR, the total amount of the administrative fine must not exceed the amount specified for the gravest infringement.

In each individual case the imposition of administrative fines must be effective, proportionate and dissuasive.

The GDPR categorises various types of infringement into two main groups according to the graveness of the infringement, to which correspond different maximum amounts of the administrative fine:

Administrative fine of up to EUR 10,000,000 EUR or 2% of turnover

The first category includes infringements for which the GDPR allows the maximum administrative fine of EUR 10,000,000 or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. The respective obligations include:

- processing personal data relating to children in connection to information society services (Article 8);
- processing which does not require identification (Article 11);
- implementation of technical and organizational measures to ensure data protection by design and by default (Article 25);
- the obligation of joint controllers to agree their responsibilities for compliance with the obligations pursuant to the GDPR (Article 26);
- the obligation to designate a representative for controllers or processors not established in the EU (Article 27);
- obligations relating to the establishment of processors and obligations of processors (Article 28 a 29);
- the obligation to maintain written records (Article 30);
- the obligation to cooperate with supervisory authorities (Article 31);
- the obligation to ensure the safety of data and to report breaches (Articles 32 - 36);
- obligations connected to the appointment of a data protection officer (Articles 37 - 39);

- obligations of a certification body (Articles 42 and 43); and
- obligations of monitoring bodies (Article 41(4)).

Administrative fine of up to EUR 20,000,000 EUR or 4% of turnover

The second category includes infringements for which the GDPR allows imposing a fine of up to EUR 20,000,000 or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. These are infringements of the following obligations:

- obligations related to the principles for processing including consent (Articles 5 – 7 and 9);
- infringement of the data subject's rights (Articles 12 - 22);
- infringement of obligations related to the transfers of personal data to third countries or to an international organisation (Articles 44 - 49);
- any obligations pursuant to Member State law adopted under Chapter IX; and
- non-compliance with an order related to the flow of personal data by the supervisory authority and other related infringements (Article 58).

The Directive which is still effective delegates the Member States to adopt appropriate measures for ensuring its applicability, especially to introduce sanctions for breach of Member State laws adopted on its basis.[1]

The Czech legislative body has done so mainly in chapter VII "Administrative breaches", in articles 44 – 46 of the Czech Data Protection Act. A natural person in the position of a controller or a processor could be imposed a fine of up to CZK 1,000,000 for certain breaches, and up to CZK 5,000,000 if there are aggravating circumstances. Any natural person can be imposed a fine of CZK 1,000,000 for publishing personal data in contradiction to a restriction to do so regulated by a special Act[2]; for such breach conducted by means of print or radio media or via television or other similarly effective means corresponds to a fine of CZK 5,000,000. Legal persons may be imposed fines for such breaches in the amount of CZK 5,000,000 or 10,000,000.

The Slovak legislative body has done so mainly in chapter IV "Sanctions and publication of breach", in articles 47 – 71 of the Slovak Data Protection Act. Controllers and processors can currently be punished by a fine in the amount of EUR 300 – 200,000. A natural person who is not a controller or a processor, can be imposed a fine of EUR 150 – 2,000.

Other measures

Besides the power to impose an administrative fine pursuant to the above-mentioned principles, the supervisory authority also has the power to use other measures, i.e.:

- to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of the GDPR;
- to issue reprimands to a controller or a processor where processing operations have infringed provisions of the GDPR;
- to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to the GDPR;

[1] Article 24 of the Directive.

[2] Refer to Act no. 141/1961 Coll., on Criminal Procedure, as amended, and e.g. its provision about prohibition of publishing data about persons participating in a criminal procedure which do not directly relate to the criminal conduct; prohibition of publishing information on ordering or performance of telephone interception and records of telecommunication operations; restriction of announcement of information that violates the principle of presumption of innocence; prohibition of publishing information allowing identification of the identity of an aggrieved person of less than 18 years of age. Also see Act no. 218/2003 Coll., on the Administration of Justice in matters of minor persons, as amended, and a similar restriction on providing information on minors.

- to order the controller or processor to bring processing operations into compliance with the provisions of the GDPR, where appropriate, in a specified manner and within a specified period;
- to order the controller to communicate a personal data breach to the data subject;
- to impose a temporary or definitive limitation including a ban on processing;
- to order the rectification or erasure of personal data or restriction of processing and the notification of such actions to recipients to whom the personal data have been disclosed;
- to withdraw a certification or to order the certification body to withdraw a certification issued, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;
- to order the suspension of data flows to a recipient in a third country or to an international organisation.

Penal sanctions

In Article 84 and in Recital 149 the GDPR obliges Member States to determine rules for other, also criminal, sanctions for violating the GDPR,[3] including sanctions of seizure of profits acquired in connection with the breach. However, the principle restricting the imposition of two or more sanctions for the same act violating the GDPR should always be observed.

The Czech Criminal Code[4] already today regulates the crime of unlawful handling of personal data, which can be punished by imprisonment, monetary fine or punishment of restriction of activities.[5] Pursuant to the Act on the criminal liability of legal persons and related proceedings[6], both natural and legal persons may face Criminal liability for the unlawful handling of personal data.

The Slovak Criminal Code[7] also regulates the crime of unlawful handling of personal data, which can be punished *inter alia* by imprisonment up to two years.[8]

Derogations and specific processing situations

The GDPR grants Member States the right to derogate from the wording of the GDPR, or (where the GDPR does not contain the respective provisions) to adopt their own legal regulation in the following affairs:

- national security, prevention and detection of crime;
- processing and freedom of expression and information;
- processing and public access to official documents;
- processing of the national identification number (birth number);
- processing in the context of employment;
- processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; and

---

[3] Article 84 of the GDPR.

[4] Act no. 40/2009 Coll., the Criminal Code (Czech).

[5] See Article 180 of the Criminal Code: "(1) Who, even by negligence, unlawfully publishes, announces, makes accessible, otherwise processes or appropriates personal data, which was collected about another person in connection to the performance of public authority, and causes serious damage to the rights and legitimate interests of a person, to whom the personal data pertain, will be punished by imprisonment of up to three years or by prohibition of activities. (2)...".

[6] Act no. 418/2011 Coll., as amended.

[7] Act no. 300/2005 Coll., the Criminal Code (Slovak).

[8] Article 374 of the Criminal Code: "(1) Who unlawfully provides, makes accessible or publishes personal data about another person collected in connection to the performance of public authority or exercising of his/her constitutional rights, or personal data about another person collected in connection to exercise of work or employment or position, by which he/she breaches an obligation regulated by a generally binding legal regulation, will be punished by imprisonment up to one year. (2)..."

- obligations of secrecy connected to professional confidentiality.

What now

We recommend controllers and processors carry out an audit to identify the most risky areas of processing operations and subsequently to prioritize steps for mitigating the risks of administrative fines or other sanctions. For this purpose it is suitable to access the extent of potential liability in connection with contracts with business partners, customers or suppliers, to which the controllers and processors are contractual parties, and to adjust the responsibilities between the parties accordingly.

To transfer the risk we recommend considering insuring the respective liability for loss caused by processing operations.

Further information can be found here:

Recitals 148 - 165

Articles 83 – 84 and Articles of Chapter IX

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