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.

Lesson 16 of 16

Practical steps for ensuring compliance and minimizing the risk of sanctions

Summary of the School of Data Privacy

Over the past months we have provided you with detailed information about the new data protection legislation, which substantially alters the conditions regarding the lawfulness of processing. The GDPR *inter alia* extends the territorial reach of the European standard of data protection, whereby the new legislations's ambition is to ensure that the protection of personal data will apply to data subjects located in the Union, as well as if their data is processed outside the Union by subjects established elsewhere.

Further, the GDPR:

- obliges controllers to take a proactive approach to ensure the lawfulness of processing and to be able to demonstrate to supervisory authorities that they have carried out all necessary actions for ensuring compliance;
- regulates the principles which controllers should comply with when processing personal data, at the commencement of processing and at all times during the processing;
- changes the conditions for a data subject to provide valid consent with processing their personal data;
- substantially broadens the data subject's rights (e.g. the right to erase their data from the online environment or the right to personal data portability);
- regulates the controller's extensive information obligation towards data subjects and the obligation to actively communicate with data subjects in justified circumstances;
- increases the standard of security measures for the sake of personal data protection and obliges controllers and/or processors to report personal data breaches to supervisory authorities and/or data subjects;
- introduces new institutes by which controllers can ensure and demonstrate compliance, i.e. codes of conduct and certification mechanisms;

- regulates the obligation to keep records of processing activities, undertake a data protection impact assessment and consult the processing with a supervisory authority in advance;
- regulates the conditions of transfer of personal data to third countries and extends the possibilities to ensure the transfer is compliant;
- introduces a system of a single contact supervisory authorities for cross border processing the controller conducts within the Union;
- establishes substantially higher sanctions for violating the GDPR in comparison with previous legislation.

Timeline of practical steps for ensuring compliance

The GDPR will become effective in slightly less than 12 months, on 25 May 2018. With regard to the importance of the new changes, the extensive character of the matter and the amount of potential fines for noncompliance, we recommend controllers processing personal data (e.g. who employ persons) start carrying out the practical steps necessary to implement the GDPR's requirements without undue delay.

Below we present a list of necessary procedural steps as well as propose a feasible and realistic compliance timeline. We recommend keeping solid documentation of the process of the project of compliance for the sake of being able to demonstrate due and professional care to the supervisory authority in the future.

✓ What: **Assigning a team of employees and securing financial and technical means for the project**

When: July – August 2017

How: First of all it is necessary to assign an employee / employees who will be responsible for (within the scope of their employment) ensuring the compliance of all the controller's processing operations with the GDPR. This also applies if the controller envisages assigning an external provider to develop and conduct the compliance project. In such case the responsible employee(s) will communicate on behalf of the controller with the external provider. Typically such employee can be a member of the legal or HR team, and for technical support the cooperation and awareness of an IT specialist is crucial.

This project team will have to be provided with all required information and trainings so that they are well oriented in the matter and know what needs to be done.

Multinational organizations or businesses must determine whether compliance with the GDPR will be handled on the local (national) level or if the local team will cooperate with headquarters.

✓ What: **Investigation of processing operations**

When: August – October 2017

How: The controller is obliged to determine (i) what personal data they process, (ii) what categories of data subjects are involved and (iii) what processing operations they carry out. This initial input must be determined with emphasis on the level of detail, accuracy, up-to-date state and completeness and the outcomes must be summarised in writing because they will be the starting point for further activities.

✓ What: **Analysis of discrepancies in light of the new legislation**

When: October – December 2017

How: The controller must conduct a thorough analysis of existing internal procedures of all concerned departments (e.g. HR, IT, departments having information about the software solutions at the controller, customer relations, receptionists identifying visitors, internal security, administrators of CCTV systems and other monitoring devices, etc.) – if they deal with personal data. Also, an analysis of documents regulating these internal procedures, if existing, is crucial.

Based on the findings of the analysis a written report should be drafted, identifying shortcomings and risks and proposing suggestions for mitigating risks. The controller's top management should be acquainted with the report.

✓ What: **Data protection officials and processors**

When: October 2017 – December 2017

How: Controllers should verify if, as of the effective date of the GDPR, a data protection official must be appointed or not.

Contracts with processors and possible other persons should be reviewed to secure their wording complies with the GDPR. We recommend analysing the responsibility relationships of these persons regarding data protection, and the corresponding risks of compensation for damages and potential sanctions.

✓ What: **Developing or updating internal data protection policies**

When: January 2018 – March 2018

How: As of the effective date of the GDPR it is necessary for the controller to have implemented new or updated existing internal policies required by the GDPR. This will contain e.g. notifications of data subjects on processing personal data, document retention plans regulating the period of retention of certain documents containing personal data, consents with processing personal data, procedures to be followed in case of requests for data access, principles of protection of personal data, procedures to erase or block data, etc.

✓ What: **Implementing internal procedures**

When: March 2018 – May 2018

How: Controllers are obliged to implement internal procedures binding for employees handling personal data and to duly train them in respect to the tasks that will be required of them as of the GDPR's effective date. These procedures should regulate all general potentialities which can occur during the processing, e.g. in case of breach of the GDPR, data subject's requests for access to data, requests to erase or block data, etc.

Employees handling personal data must be demonstrably and in detail notified of their confidentiality obligation and of all implemented internal procedures regulating the processing, they must know how each relevant document template is used, how to communicate with data subjects, etc.

Of course, all required processing operations should be technically feasible, which should be ensured by an IT specialist.

- ✓ What: **Employee training**

  When: February 2018 – May 2018

  How: In order to raise awareness of the topic of data protection, controllers are obliged to provide trainings for employees handling personal data. The extent of risk and of potential sanctions for violation of the GDPR's provisions, which in certain cases can be as high as EUR 20,000,000 or 4% of the total worldwide annual turnover (whichever is higher), will directly depend on their qualification.

Where to start

The law firm Balcar, Polanský & Spol. s.r.o.'s team of professionals is ready to provide you with further information on any of the requirements mentioned above or any other aspects of the soon-to-be-effective GDPR. Therefore, please do not hesitate to contact our specialists below, or your usual contact person in our law firm.

You can learn more about our expertise, as demonstrated by our international certification in the data protection field, here:

http://www.balcarpolansky.cz/files/251/Focussed%20on%20DP_ENG.pdf

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