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 11 of 16

Codes of conduct and certification

Below you will learn:

Important changes

- The GDPR introduces new institutes for ensuring and demonstrating that the processing is in compliance with the GDPR, i.e.:
    - codes of conduct, and
    - certification mechanisms, seals and marks;
- Controllers and processors can ensure and maintain compliance with the GDPR through codes of conduct more easily;
- Adherence to codes of conduct will be monitored by accredited entities; if a breach of the code of conduct on the side of the controller or processor is discovered, they can be suspended from participation in the code;
- Certification mechanisms, seals and marks will be introduced for voluntary "self-regulation" by the controller or the processor;
- If the controller or processor adheres to some of these instruments, compliance with the GDPR will be demonstrated for a period of 3 years (the validity of the certification can also be extended).

Compliance Action Plan

Controllers and the processors should:

- monitor whether approved codes of conduct exist in their sector, valid within Slovakia or the EU;
- find out whether certifications, seals or marks exist, which they could obtain and so demonstrate compliance with the GDPR;
- learn about existing certificates, seals or marks, which will be introduced from time to time, and to take these instruments into account when choosing their processors or service providers.

Codes of conduct

The GDPR regulates codes of conduct as documents elaborated by associations or other bodies representing categories of controllers or processors, regulating the processing of personal data specific for these groups of controllers or processors. The codes should contribute to the proper application of the GDPR, taking account the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

The codes will be important for controllers and processors who, by adhering to them, will be able to easily and reliably ensure and demonstrate to the supervising authorities their compliance with the GDPR.

By undertaking to observe an approved code of conduct, the controller or the processor may benefit in several ways, such as:

- best practices will be developed through the codes, regulating how personal data is handled in the respective sector and in the specific context of processing;
- the controller or the processor may rely that the processing of personal data is done lawfully, which can e.g. save financial resources on professional advisors in this area;
- data subjects will consider participation in the approved code as a sign of credibility and assurance that their personal data is processed lawfully;
- together with an enforceable obligation of the data importer residing outside of the EU to adopt appropriate safeguards, approved codes may be used to ensure the lawfulness of the transfer of personal data outside the EU, similar to standard contractual clauses and binding corporate rules;
- compliance with the GDPR may be demonstrated to the supervisory authority more easily.

An association or other bodies representing categories of controllers or processors can prepare a code of conduct relevant for their sector or industry. The code should serve as a "manual" for companies operating in the respective sector, how to correctly carry out processing operations specific for their sector, e.g. entities operating in the banking sector, health and education, pharmaceutical industry, retail, IT sector including cloud services, etc.

The codes may regulate recommended procedures with regard to e.g.: fair and transparent processing, the legitimate interests pursued by controllers in specific contexts, the collection of personal data, the pseudonymisation of personal data, the information provided to the public and to data subjects, the exercise of the rights of data subjects, the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained, the measures and procedures useful for adopting the appropriate technical and organisational measures and measures to implement data protection by design and by default, security measures, the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects, the transfer of personal data to third countries or international organisations, or out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects.

Approving codes

In order for a code of conduct to have the effects as explained above, it must be approved by a competent supervisory authority. The process of approval depends upon whether the code should be valid within a member state, or if it should have general validity within the Union.

If a code is does not relate to processing operations outside a certain member state (e.g. Czech Republic or Slovakia), its draft must be submitted to the respective supervisory authority (in this case the Czech or Slovak Data Protection Authority). The supervisory authority provides an opinion on whether the draft code complies with the GDPR and approves that draft code if it finds that it provides sufficient appropriate safeguards. That supervisory authority also registers and publishes the code.

On the other hand, where a draft code of conduct relates to processing activities in several Member States, the competent supervisory authority, before approving the draft code, submits it in the procedure of cooperation between supervisory authorities of the of the Union and of the Commission to the European Data Protection Board (the "Board"), which provides an opinion on whether the draft code complies with the GDPR or provides appropriate safeguards.

If the Board in its opinion confirms that the draft code complies with the GDPR, or provides appropriate safeguards, the Board submits its opinion to the European Commission. The Commission may, by way of implementing acts, decide that the approved code of conduct, as submitted to it is generally valid within the Union. The Commission ensures appropriate publicity for the approved codes which have general validity. The Board collates all approved codes of conduct in a register and will make them publicly available using appropriate means.

Monitoring compliance with codes of conduct

Besides the competent supervisory authority, compliance with codes of conduct can be monitored by a body which has an appropriate level of expertise and is accredited for this purpose by the competent supervisory authority. Such body must:

- demonstrate its independence and expertise in relation to the subject-matter of the code;
- establish procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;
- establish procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and
- demonstrate that its tasks and duties do not result in a conflict of interest.

The criteria for the accreditation will be determined by the respective supervisory authority after consulting with the European Data Protection Board. If the accredited body discovers non-compliance with the code, it can impose a sanction to the controller or the processor, in the form of appropriate measures, including suspension or exclusion of the controller or processor concerned from the code.

Certification

The GDPR regulates certification mechanisms, seals and marks as further instruments of protection of personal data. These mechanisms should increase the transparency of the processing, and should help data subjects to quickly assess the level of protection of personal data for relevant products and services. Such example is a situation when data protection seals or marks will be

introduced for a certain service, e.g. providing of cloud services, which will mean that the entity who obtains them meets the GDPR's requirements for lawful processing[1].

Certification of processing personal data is an important milestone for creating a reliable and transparent framework for processing. These mechanisms can be implemented by Member States, the supervisory authorities, the Board and the Commission. They should be applied preferably at the Union level, but their validity in a local extent is also admissible. The specific needs of micro, small and medium-sized enterprises should be taken into account.

Certification is voluntary, but does not reduce the responsibility of the controller or the processor to comply with the GDPR. In other words, if e.g. the controller obtains certification, but violates the GDPR by a processing operation, the certification does not limit his liability. The certification can be issued for a maximum period of three years and may be renewed, under the same conditions. Similarly, if the conditions for certification cease to be met, certification can be withdrawn.

Certification may have the following benefits for controllers and processors:

- controllers and processors will be able to demonstrate compliance with the GDPR more easily, especially in connection to adopting appropriate technical and organisational measures;
- data subjects or clients who look for a service provider can take certification into account as a proof of credibility and expertise of the service provider of (e.g. cloud) services; and
- similar to codes, together with an enforceable obligation of the data importer residing outside the EU to adopt appropriate safeguards, certifications may be used to ensure the lawfulness of the transfer of personal data outside the EU, similar to standard contractual clauses and binding corporate rules.

Besides the supervisory authorities, the GDPR also gives the power to grant certifications to certification bodies, which are duly accredited for this activity. Under Slovak conditions the Slovak Data Protection Authority will be entitled to grant accreditation to certification bodies. To obtain accreditation of a certification body, the following criteria set by the GDPR must be met:

- demonstrating independence and expertise in relation to the subject-matter of the certification;
- undertaking to respect the criteria approved by the Board or the competent supervisory authority;
- establishing procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;
- establishing procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and making those procedures and structures transparent to data subjects and the public; and
- demonstrating that the tasks and duties of the accreditation applicant do not result in a conflict of interest.

The accreditation of a certification body will be issued for a period of 5 years maximum with the option of renewal.

What now

Controllers and processors can benefit from participating in approved codes of conduct (valid either within a Member State or within the Union), or from data protection certifications, seals or marks

[1] For better understanding the ISO certificate can be considered, which proves that the subject who obtained it, meets a certain quality in the respective area, as required by this certificate.

which will be introduced after the GDPR becomes effective. Therefore it is recommended that controllers and processors monitor the implementation of these instruments to be able to decide if they will seek to participate in or obtain them.

Further information can be found here:

Recitals 77, 81, 98 – 100, 148, 166, 168

Articles 40 – 43, 57(1) let. p), q), (3) let. e), 64 (1) let. c), 70 (1) let. o), p)

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