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 12 of 16

Transfer of personal data outside the EU/EEA

Below you will learn:

Important changes

- The requirements for the transfer of personal data will mostly concern international companies and companies which use services that entail the transfer of data to third countries (e.g. cloud services);
- In comparison to the previous legal regulation, new possibilities to ensure the lawfulness of data transfer outside the EU/EEA have been introduced.

Compliance Action Plan

Controllers and processors should:

- review the flow of processed personal data;
- if personal data is transferred outside the EU/EEA, check whether mechanisms for ensuring the lawfulness of the transfer (e.g. model clauses, binding corporate rules, etc.) are implemented;
- check if and where their service providers transfer the personal data received from them;

- if in the past the transfers occurred based on the "Safe Harbour", implement a different legal grounds for the transfer, since the Safe Harbour was abolished and is no longer valid.

Transfer of personal data outside the EU/EEA

Similar to the previous legal regulation, the GDPR also regulates the conditions of data transfer to third counties (outside the EU/EEA) and to international organisations[1]. The rationale for this is the fact that as soon as the personal data leaves the territory where EU law applies, it becomes subject to foreign laws which may not ensure an adequate protection of personal data on a level comparable with Union law. Therefore, this topic will be relevant mostly for international companies and companies which use the services of providers operating outside of the Union (e.g. if they use cloud services and servers located in third countries). On the contrary, this topic will not be relevant to companies who do not transfer data or transfer them only within the EU/EEA.

The starting point for understanding the need to regulate data transfers outside the EU is explained in Recital 101 of the GDPR, according to which flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data is transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by the GDPR should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation.

The transfer of personal data to third countries will be possible if any of the following conditions is met:

Transfer on the basis of an adequacy decision

The European Commission (the "Commission") can decide that a third country, a territory or one or more specified sectors within that third country, or the international organisation ensures an adequate level of protection. Such a transfer does not require any specific authorisation[2]. At least every four years there must be a periodic review of the circumstances on the basis of which the Commission issued its decision.

If the Commission discovers that the circumstances impacting the protection of personal data in a third country (or an international organisation) have been negatively changed, it can decide that such country no longer ensures an adequate level of protection. Such decision does not have a retroactive effect, thus it is effective at the earliest on the day of its adoption. Therefore, the question remains regarding the security of the data that was already transferred.

The Commission will publish in the Official Journal of the European Union and on its website[3] a list of the third countries and international organisations for which it has decided that an adequate level of protection is or is no longer ensured. Currently, countries ensuring an adequate level of protection are: Andorra, Argentina, Canada, Switzerland, Faeroe Islands, Guernsey, Isle of Man and Jersey, Israel, New Zealand and Uruguay.

---

[1] Article 4 (26) of the GDPR: *an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries*.

[2] When accessing the adequacy of the level of protection of personal data, the Commission takes into account elements: the rule of law, respect for human rights and fundamental freedoms, relevant legislation, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organization, effective administrative and judicial redress, the existence and effective functioning of independent supervisory authorities, international commitments, etc.

[3] http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

Transfer to the United States of America has certain specific features. Until 2015 transfer to the USA was possible *inter alia* based on the "Safe Harbour" scheme[4], which allowed for the transfer of personal data to entities located in the USA and registered within the Safe Harbour without additional measures and formalities. However, on 6 October 2015 the Grand Chamber of the CJ EU issued a decision[5], by which it abolished the respective Commission's decision regulating the Safe Harbour, and from this date the transfer of personal data to the USA based on this legislative act is no longer considered lawful[6].

This scheme was substituted by a so called "Privacy Shield"[7], which was passed by the Commission on 12 June 2016. The list of companies which bound themselves to comply with the principles of data protection implemented through the Privacy Shield is published on the US Department of Commerce's website[8].

Transfers requiring adequate safeguards

In the absence of a decision of the Commission as explained above, the transfer of personal data to a third country or an international organisation can be undertaken only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. The appropriate safeguards may be provided for, without requiring any specific authorisation from a supervisory authority, by:

- a legally binding and enforceable instrument between public authorities or bodies;
- binding corporate rules;

  In case of a group of companies, which has subsidiaries in the Union and in third countries, the transfer of personal data within this group of companies can also be carried out on the basis of binding corporate rules. In order for the rules to be binding, they must be approved by the competent supervisory authority, after which they are binding not only within the jurisdiction of the supervisory authority which approved them, but also in all other jurisdictions where the group has subsidiaries. The supervisory authority approves the rules, if:

  - they are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;
  - expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and
  - fulfil further requirements, e.g. the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members, the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question, their

[4] Decision of the Commission 2000/520/EC of 26 July 2000, which contained the principles and requirements related to the protection of personal data, to which entities residing in the USA could voluntarily submit themselves and so to be regarded as reliable when handling of personal data.

[5] http://curia.europa.eu/juris/celex.jsf?celex=62014CJ0362&lang1=sk&lang2=EN&type=TXT&ancre=

[6] The basis for this was a petition of an Austrian citizen Max Schrems, who was a Facebook user from 2008. Facebook transferred personal data of its users to servers located in the USA, where it was further processed. Mr. Schrems filed a complaint with the supervisory authority in Ireland, the purpose of which was that pursuant to information revealed by Edward Snowden in 2013 in relation to the manner in which the American security agencies (especially NSA – National Security Agency) handle personal data in their jurisdiction (i.e. also data of European users), the USA do not ensure protection from surveillance from the side of American authorities. The Irish supervisory authority refused the complaint referring to the safeguards ensured by the American authorities through the Safe Harbour. Upon investigating the matter the CJ EU abolished the Safe Harbour scheme.

[7] http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm

[8] https://www.privacyshield.gov/welcome

legally binding nature, both internally and externally, the rights of data subjects in regard to processing and the means to exercise those rights, the complaint procedures, cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, etc.

- standard data protection clauses adopted by the Commission or adopted by the supervisory authority and approved by the Commission; model clauses that were adopted prior to the GDPR remain valid[9];

  If the controllers or processors use standard contractual clauses for the transfer of data outside of the Union, they can include them in a wider contract, such as a contract between the processor and another processor, or add other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses or prejudice the fundamental rights or freedoms of the data subjects;

- an approved code of conduct (please refer to Lesson 11 for further information regarding this new instrument) together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

- an approved certification mechanism (please refer to Lesson 11 for further information regarding this new instrument) together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

Derogations

In the absence of an adequacy decision or of appropriate safeguards including binding corporate rules, a transfer of personal data to a third country or an international organisation can take place only on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
- the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

The transfer to a third country or an international organization may take place if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards

[9] http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm

with regard to the protection of personal data. In such case the controller must inform the supervisory authority of the transfer.

What now

Controllers and processors should verify if they transfer personal data outside the EU/EEA, or if such transfers are realized by their suppliers of services or goods. Subsequently such transfers must be based on one of the valid legal grounds for the transfer, e.g. on basis of an adequacy decision or on basis of adequate safeguards. If the transfer cannot be grounded by one of the existing legal grounds, it is necessary to ascertain if the transfer can be subject to a derogation from this obligation.

Further information can be found here:

Recitals 6, 23, 101 - 116

Articles 44 – 49

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