

April 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](mailto:office@bapol.sk) or [office@bapol.cz](mailto:office@bapol.cz), or by calling the phone number +421 220 251 311 and +420 251 009 111.*

## *Lesson 9 of 16*

### **Data subject's rights (Part 2)**

#### **Below you will learn:**

#### *Important changes*

- The right to data portability entitles the data subject to have the controller port his/her personal data directly to another controller;
- The content of the data subject's right to object to processing at the controller is changed; the data subject must be duly informed of this right;
- The data subject has a right not to be subject to a decision which:
  - is based solely on automated processing (including profiling); and
  - has legal effects on him/her or which similarly significantly affects him/her.

#### *Compliance Action Plan*

#### Controllers must:

- ensure that the processed personal data are easily portable in a structured, commonly used and machine-readable format;
- check that the data subject was duly informed of their right to object to processing at the time of the first communication;

- check if profiling is carried out and if yes, ensure that a relevant legal ground exists for it.

### *Right to data portability*

The GDPR regulates the right to data portability as the data subject's right to:

- receive the personal data concerning him or her and subsequently have it transferred to another controller<sup>1</sup>; and to
- have the personal data transmitted by a controller directly to another controller.

In the first case, the right to receiving personal data can resemble the previously discussed *right of access to personal data* (refer to Lesson 8). The right to receiving the personal data is regulated more specifically with these differences:

- whereas the right of access to personal data entitles the data subject to access his/her data (i.e. *inter alia* to obtain a copy thereof) in a commonly used electronic form,
- the right to data portability is formulated narrower and in a more detail, in the sense that it entitles the data subject to obtain his/her personal data in a structured, commonly used and machine-readable format. From the technical aspect it is more specific and challenging for the controller, because he/she must provide the personal data in a structured, i.e. systematic and organized format<sup>2</sup>.

The right to data portability may be exercised only if:

- the data was provided to the controller by the data subject;
- the processing is based on consent or explicit consent (in case of a special category of personal data), or it is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, and
- if the processing is carried out by automated means (i.e. not in paper form; for comparison – the right of access to personal data also pertains to data processed in paper form).

If the above conditions are not met, the data subject cannot invoke this right. For example, if the controller obtains the personal data from another controller and not directly from the data subject, the data subject would not have the right to data portability, only the right to access the data.<sup>3</sup>

If the data subject receives his/her personal data within the right to data portability, he/she is entitled to transfer it to another controller. However, this must not adversely affect the rights and freedoms of others. That means that should the right to data portability have a negative effect on the rights and freedoms of others, the transfer (or the provision of personal data to the data subject) should not occur. This situation could arise e.g. in the reality of social networks where among a data subject's personal data are also other people's personal data which is processed (e.g. within their mutual communication). In exercising the right to data portability, the rights of other persons must not be affected.

A significant change introduced by the new concept of the right to data portability lies in that the data subject can also request the controller not to transfer his/her personal data to him/her, but to

---

<sup>1</sup> The exercise of this right is without prejudice to Article 17 of the GDPR regulating the right to erasure. Also, this right does not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

<sup>2</sup> Recital 68 also mentions an "interoperable format", but this is probably more of a recommendation than a binding character of the formulation.

<sup>3</sup> Such formalistic approach of the communitarian or other legislation does not have a material meaning in practical life. The data subject will be entitled / through the provision of the actual Czech Act (Article 12) and the Slovak Act (Article 15) – to the processed personal data, and not just to the information that their name, surname, date or birth, address, etc. is processed. Thus, there is no obstacle for the data subject to provide or to "transfer" the obtained personal data to another controller.

transfer it directly to another controller. In practice this will be usable e.g. if the data subject can change the provider of certain (e.g. telecommunication) services. The data subject would be deprived of the administrative and technical burden connected with the transfer of his/her personal data to another controller, whereas this obligation would pertain to the original data controller "in a structured, commonly used and machine-readable format". The only condition would be the technical feasibility of this request.

### *The right to object*

The GDPR grants the right to object to the processing of personal data to the data subject only in certain specific cases. The data subject is not entitled to object to any processing, but only if:

1. the processing is necessary for:
  - a. the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
  - b. the purposes of the legitimate interests pursued by the controller or by a third party;

including objecting to profiling based on these provisions.

In such cases the data subject is entitled to object to processing at any time, but only on "grounds relating to his or her particular situation". The burden of statement, why the processing should be ceased, is on the part of the data subject, who must state specific circumstances pertaining to his/her person or situation.

If the data subject objected and stated relevant reasons, the controller must not continue the processing of such personal data, unless he/she demonstrates

- compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the data subject; or
- reasons for the establishment, exercise or defence of legal claims.

In such case the controller could continue the processing. That means that if the data subject files an objection based on the reasons above, the burden of proof shifts to the controller to demonstrate the existence of reasons that entitle him/her to continue processing the personal data for the stated purposes.

The data subject must be explicitly notified at the latest at the time of the first communication. This right must be presented clearly and separately from any other information.

2. processing for the purposes of direct marketing;

The data subject is entitled at any time to object to the processing of his/her personal data for the purpose of direct marketing, including profiling in the extent to which it relates to it.

It is an absolute right of the data subject, where he/she is not obliged to state or demonstrate anything else. In other words, if the data subject does not wish that his/her personal data is processed for this purpose, it is sufficient that he/she objects at the controller who is obliged to cease the processing for this purpose immediately. The data subject is not obliged to state reasons pertaining to his/her special situation as in point 1 above. Also, there is no way for the controller could effectively oppose this objection (e.g. by means of claiming that his/her legitimate interest overrides the data subject's rights and interests). As soon as the data subject delivers the objection related to the processing of personal data for direct marketing purposes to the controller, the controller must not continue the processing for this purpose. If, however, the respective data is processed for a different reason based on a different legal ground, such processing is not affected.

Similarly as in point 1, the controller must explicitly notify the data subject of this right, at the latest at the time of the first communication, and the right must be presented clearly and separately from other information.

3. processing for the purpose of scientific or historical research or for statistical purposes;

If the personal data is processed for the above said purposes, the data subject can object to the processing based on grounds relating to his or her particular situation. He/she does not have this right if the processing is necessary for the performance of a task in the public interest.

As in point 1, the data subject must state relevant reasons relating to his/her particular situation in order for the processing to cease.

Contrary to objections pursuant to point 1 and 2, the data subject does not have to be notified of the right to object. The objection can also be raised by automated means using technical specifications.

### *Automated individual decision-making<sup>4</sup> and profiling<sup>5</sup>*

The GDPR provides data subjects protection against the risk of a potentially negative decision that was adopted without any human intervention, i.e. exclusively based on automated decision-making<sup>6</sup>. Recital 71 introduces an example of such decisions an automatic refusal of an online credit application or e-recruiting practices without any human intervention. The DGPR grants the data subject the right not to be affected by a decision which

- is based exclusively on automated processing, including profiling; and
- which has legal effects concerning him or her or similarly significantly affects him or her.

The protection against automated individual decision-making will not apply if the decision

- a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
- b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests<sup>7</sup>; or
- c) is based on the data subject's explicit consent.

In scenarios sub a) and c) the controller is obliged to introduce suitable measures for the protection of the data subject's rights. A minimum standard is to ensure the possibility of human

---

<sup>4</sup> Automated individual decision-making is when a certain matter is decided by automated means, i.e. without any human intervention, e.g. based on certain algorithms defined in advance.

<sup>5</sup> Profiling means 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 (Article 4(4) of the GDPR). Pursuant to Recital 71 of the GDPR the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect.

<sup>6</sup> This is so far regulated in Art. 15 of the Directive, as a prohibition of decisions based solely on automated processing of data intended to evaluate certain personal aspects relating to the data subject, such as his/her performance at work, creditworthiness, reliability, conduct, etc. There is an exception for decisions taken in the course of the entering into or performance of a contract, lodged by the data subject, or if it is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

<sup>7</sup> E.g. for the purpose of tax-evasion monitoring and prevention conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller.

intervention on the part of the controller, i.e. that the decision adopted by automated means will be reviewed by a person to enable the data subject to express his/her point of view to the circumstances of adoption of the decision and to contest the decision.

The automated decision-making must not be based on special categories of personal data (i.e. revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as in Article 9(1) of the GDPR), except in cases where it occurred based on

- explicit consent of the data subject, except where Union or Member State law provide that the prohibition may not be lifted by the data subject;
- substantial public interest, on the basis of Union or Member State law which is proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

and where suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

### *What now*

In order to ensure compliance with the GDPR in the extent of the right to data portability, right to object and rights connected to automated decision making and profiling, controllers should assure themselves to what extent they will be subject to this regulation (e.g. to what extent they will use profiling) and to correspondingly adjust internal processes pertaining to the processing and the communication with data subjects.

Also it will be essential to monitor further Union and local legislation, because the extent of rights and entitlements of data subjects, and the corresponding obligations of controllers, can be modified in favour of *inter alia* the protection of the data subjects or the rights of others, or with the aim to ensure the enforcement of civil claims.

### *Further information can be found here:*

Recitals 68 – 72

Articles 4(4), 20 – 23

### *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