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 or office@bapol.cz, or by calling the phone number +421 220 251 311 and +420 251 009 111.

Lesson 8 of 16

Data subject's rights (Part 1)

Below you will learn:

Important changes

Controllers will be obligated to:

- acquaint themselves with the content of data subject's new rights granted to them by the GDPR;
- implement effective internal procedures for handling data subject's requests concerning the processing (e.g. the duty to provide them with a copy of the data subject's personal data that they process and to demonstrate the lawfulness of processing);
- prepare policies and materials informing data subjects of how they can exercise their rights regarding the controller.

Data subjects can *inter alia* request:

- erasing their personal data if the processing is not lawful or if they withdraw their consent with processing;
    - if the controller made the processed personal data public (e.g. in connection with social media), if there is a grounded request for erasure, he/she is obligated to forward the request to all who process the published data. This obligation is formulated very broadly and its practical application will probably be a matter of further testing;

- restriction of processing his/her data, e.g. during the processing of their complaint related to the processing of their personal data or if the data subject objects against erasure for another reason.

Compliance Action Plan

Controllers should:

- create internal procedures for the timely handling of data subject's requests concerning the lawfulness of processing of their personal data (especially clients and employees);
- train a team of employees who handle the requests as to their rights and obligations;
- prepare template responses to requests, create procedures ensuring compliance with statutory periods, ensure that the data subjects are provided with all information to which they are entitled;
- ensure that the way of handling the requests meets the technical requirements of the GDPR;
- verify whether, in connection with the information obligation, another person's right to privacy will not be violated and create procedures for mitigating such risks;
- ensure that it is possible from the technical and organizational perspective to satisfy a request for erasure or restriction of processing in the controller's systems.

Regarding the data subject's rights

The GDPR extends and specifies the data subject's rights. For completeness we will include the list of all the data subject's rights as introduced by Chapter III of the GDPR. With regard to the extent of the matter we will discuss the data subject's rights in the next two lessons.

Right of access to personal data

In contrast to the controller's information obligation, as discussed in Lesson 7, the right of access to personal data is formulated differently: whereas the information obligation applies to the controller and obliges him/her to automatically, i.e. without a specific request of the data subject, provide the data subject with certain information, the right of access is independent from whether the controller met his/her information obligation, and entitles the data subject to access his/her personal data and to receive additional information about it on the basis of a his/her request.

The content of the right of access is the data subject's right to obtain from the controller confirmation as to whether or not personal data concerning him or her is being processed. If so, he/she is entitled to access (i.e. have a copy) to the personal data and receive further information[1] relating to the processing.

The controller must provide a copy of the personal data undergoing processing free of charge. For any further copies requested by the data subject, the controller may charge a reasonable fee

[1] I.e. a. the purposes of the processing; b. the categories of personal data concerned; c. the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; d. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; e. the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; f. the right to lodge a complaint with a supervisory authority; g. where the personal data are not collected from the data subject, any available information as to their source; h. the existence of automated decision-making, including profiling, and at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; i. where personal data is transferred to a third country or to an international organisation, the data subject has the right to be informed of the appropriate safeguards relating to the transfer.

reflecting administrative costs connected therewith. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information must be provided in a commonly used electronic form. This requirement is capable to induce further costs for entities processing personal data in paper form or in special formats, which will need to be converted into generally readable electronic form. Further costs can arise in connection to software and hardware equipment, administrative staff, etc.

Pursuant to Recital 63, the controller may provide remote access to a secure system, which would provide the data subject with direct access to his or her personal data. That means that if, e.g., the controller anticipates a greater frequency of data subject's requests for access to data, he/she may comply with this obligation by introducing a secure database of personal data into which the data subject will have access to the extent of his/her own personal data. However, this suggestion has a recommendatory rather than authoritative character.

The data subject's right of access to his/her personal data corresponds with the controller's obligation to implement internal procedures and organisational and technical measures in order to be able to satisfy the data subject's requests within a statutory period, which is "without undue delay" and in any event within one month of receipt of the request. This period may be extended by two further months where necessary.

Controllers should also introduce work procedures as to how to proceed in such occasions, train staff to process the requests, notify the staff of the obligations pertaining to data protection, e.g. about the obligation to maintain confidentiality, and to ensure that they have the appropriate technical and organisational equipment to be able to handle the data requests in a generally readable electronic format.

Exemptions from the right of access

The GDPR further regulates certain exemptions from the right of access to personal data:

- first of all, the right to obtain a copy of one's personal data must not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. Should the rights of another person be infringed by complying with the right of access to data, technical and organizational measures should be taken with the aim to avoid such infringement. However, the result of those considerations should not be a refusal to provide all information to the data subject. Since in this case there might be a collision of at least two equal rights or freedoms[2], in case of a dispute the respective court would be entitled to decide with final validity.
- where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates. However, this does not mean that if the processing of the data subject's request would be demanding as to the time and extent, that the controller would not be obliged to satisfy such request;
- the data subject's request should be motivated by verification of the lawfulness of the processing of his/her personal data; a request filed for a different purpose may not be satisfied by the controller.

The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

[2] The data subject's right of access to personal data and another person's right e.g. to protection of personality, to privacy, privacy of correspondence, trade secret, IP rights, etc.

Right to rectification

The data subject has the right to have the controller, without undue delay, rectify inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject has a right to have incomplete personal data completed, including by means of providing a supplementary statement.

Right to erasure ("right to be forgotten")

The right to "be forgotten" raised many emotions during the legislative process of preparation the GDPR, especially in connection with providing information society services by companies such as Google, Facebook, etc. Services provided by these and other companies are specific in that they process an enormous amount of data subjects' personal data, store them on servers and further process them; with regard to the extensive amount of data and processing operations they anticipated many obstacles in regard to the right to be forgotten. This right, still governed only by case law[3] has, however, become a part of the GDPR's final wording, in the following content:

The data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay, if conditions regulated by the GDPR are met. This right corresponds with the controller's obligation to erase personal data without undue delay where one of the following grounds applies:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

  According to this assumption if personal data was collected or processed e.g. for the purpose of direct marketing, and the controller changed their business activities and no longer aims for marketing activities towards the data subject, his/her personal data should be erased.

- the data subject withdraws the consent on which the processing is based[4], and where there is no other legal grounds for the processing;

  Withdrawal of the consent does not render the processing undertaken prior to the withdrawal unlawful. (Please refer to Lesson 4 for more information on consent).

- the data subject objects to the processing pursuant to Article 21(1) of the GDPR[5] and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2) of the GDPR [6];

  The right to object to processing will be discussed in the next lesson.

- the personal data have been unlawfully processed;

  This reason is very general and formulated so broadly that a large number of data subject's requests for erasure of data will be able to be included under it. The risk connected to it is that it will be the controller's obligation to demonstrate that data is processed lawfully (regarding the lawfulness of processing see Lesson 3). Thus, the fact that the data subject will claim that his/her personal data is processed unlawfully will be enough to shift the

---

[3] At the EU level, see especially the judgment ECJ (Grand Chamber) of 13. 5. 2014, Case C 131/12 Google Spain SL, Google Inc. against the Agencia Española de Protección de Datos (AEPD), Mario González Costeja.

[4] Pursuant to Article 6 (1) let. a) or Article 9(2) let. a) of the GDPR.

[5] The data subject has a right to object, on grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or if it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject that require protection of personal data, in particular where the data subject is a child, including profiling based on those provisions.

[6] Where personal data is processed for direct marketing purposes, the data subject has the right to object at any time to the processing of his/her personal data, which includes profiling to the extent that it is related to such direct marketing.

burden of demonstrating the opposite to the controller. The controller should therefore ensure that he/she is not in distress as to the evidence for proving the lawfulness of the processing, and to keep sufficient records about the processing and the legal grounds relating to it.

It will be interesting to monitor how Member States will approach the implementation of exemptions[7] in their own legislation. Naturally, the controllers who process personal data on a cross border basis should acquaint themselves with these local specifics to ensure compliance of the processing in each Union State.

- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

  This applies e.g. to a situation where personal data processed so far should be erased after some time (and where an exemption allowing further processing, e.g. for archiving purposes in the public interest does not apply – see below).

- the personal data have been collected in relation to the offer of information society services referred to in Article 8(1) of the GDPR.

  That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child.

Specifics pertaining to published personal data

Where the controller has made the personal data public and is obliged to erase the personal data pursuant to the rules mentioned above, the controller will take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data. These measures will be taken taking into account the technology available and the cost of implementation.

This provision reflects perhaps one of the most revolutionary changes in the processing of personal data introduced by the GDPR. This provision basically obliges the controller who processed a data subject's personal data, and within this processing the data was made public, if the data subject submits a justified request for erasure of his/her personal data:

- to proactively adopt adequate measures including technical measures,
- to effectively inform controllers who process the said data that the data subject requests erasure of his/her personal data, its copies and replications,
- all of the above with regard to available technology and the cost of implementation.

Pursuant to Recital 66, the said measure was adopted specifically to strengthen the right to be forgottten in the online environment. However, it is not quite clear as to how the processor determines the group of controllers who process personal data that have been made public[8], and thus how to identify the concrete controllers whom the controller should notify of the request for erasing personal data. In practice, the application of this provision will be subject to further testing regarding how the compliance with this provision will be enforceable and to what extent the data subject's right reflecting this obligation will be eventually realisable.

[7] Article 23 of the GDPR.

[8] For the sake of completeness, please note that in Slovak conditions after the GDPR becomes effective it will no longer be lawful to process personal data that has been made public pursuant to Article 10(3) let. e) of Act no. 122/2013 Coll. Pursuant to the GDPR, if no other legal grounds exist for processing of such data, the processing of data which was made public will be in contradiction to the principles of lawfulness, fairness and transparency, the principle of purpose limitation and compatibility of purposes.

Exemptions from the right to erasure

The above obligations of controllers will not apply if the processing is needed:

- for exercising the right to freedom of expression and information;
- for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- for reasons of public interest in the area of public health[9];
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- for the establishment, exercise or defence of legal claims.

Right to restriction of processing

Restriction of processing[10] means the controller is entitled only to store the personal data without any processing operations. If processing is done by automated means, it is necessary to adopt appropriate technical measures for this purpose (e.g. to withdraw it from the online environment). The data subject has a right to request that the controller restricts the processing if any of the following applies:

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
- the data subject has objected to processing pursuant to Article 21(1) of the GDPR pending the verification whether the legitimate grounds of the controller override those of the data subject.

Where processing has been restricted pursuant to the above rules, such personal data will, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

A data subject who has obtained restriction of processing will be informed by the controller before the restriction of processing is lifted.

Also

In connection to the right of rectification, erasure and restriction, the controller is obligated to communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed. This obligation does not apply if this proves impossible or involves disproportionate effort. The controller must inform the data subject about those recipients if the data subject requests it.

[9] Pursuant to Article 9(2) let. h) and i) of the GDPR, and Article 9(3) of the GDPR.
[10] Article 4(3) of the GDPR.

What now

In connection with the rights discussed above, the controller has extensive obligations to which we refer in the Compliance Action Plan section. To ensure compliance with the GDPR, controllers are advised to consult their legal advisors and IT professionals about their internal procedures for processing personal data.

Further information can be found here:

Recitals 63 - 69

Articles 15 - 19

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