

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 6 of 16

Special category of personal data

Below you will learn:

Important changes

- The GDPR explicitly regulates that the term special category of personal data (after this "sensitive data") also contains genetic data and biometric data, if they are processed for unique identification of a person;
- The legal grounds for processing of sensitive data are slightly different from the current legal regulation;
- Member States are entitled to adopt their own modifications of processing sensitive data.

Compliance Action Plan

- If the controller process sensitive data, it is essential to correctly define the legal grounds of the processing;
- If the legal ground is the data subject's consent, it is necessary that it meets specific qualitative requirements.

Processing the special category of personal data

The GDPR defines sensitive data first as personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership of a person. Also, the GDPR considers sensitive data genetic data¹, biometric data² for the purpose of uniquely identifying a natural person, data concerning health³ or data concerning a natural person's sex life or sexual orientation.

The GDPR recognizes that sensitive data merit specific protection as the context of their processing could create significant risks to the data subject's fundamental rights and freedoms. Therefore, in Article 9 (1) the GDPR enshrines a general prohibition of its processing, which can only be overridden by the circumstances outlined in Article 9 (2). The possibility to override the general prohibition of processing sensitive data is regulated by an exhaustive list of exceptions; therefore, the circumstances under which it is possible to circumvent the general ban of processing sensitive data may not be extended.

Exceptions from the general prohibition of processing sensitive data

The general prohibition against processing sensitive data will not apply if one of the following conditions exist:

- a) *the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition may not be lifted by the data subject;*

Regarding the requirements for the granting of consent to be valid please refer to Lesson 4. However, please note the particularity regarding the consent for processing sensitive data, the consent must be explicit (a condition that does not apply if sensitive data is not processed).

Sensitive data cannot be processed where the applicable law states that even the data subject's explicit consent cannot override the general prohibition of processing sensitive data.

- b) *processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;*

This legal ground extends the current regulation by explicitly stating that the processing of sensitive data is lawful where it is necessary to perform obligations arising from a collective agreement.

Processing personal data for purposes of employment law, social insurance and social security is possible based on the current legal regulation.⁴

- c) *processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;*

A comparable legal ground is contained in the current legislation.⁵

¹ Personal data relating to the inherited or acquired genetic characteristics of a natural person that give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

² Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

³ Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

⁴ Article 9 let. d) and f) of the Czech Data Protection Act no. 101/2000 Coll. and Article 14 let. g) of the Slovak Data Protection Act no. 122/2013 Coll.

- d) *processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;*

A comparable legal ground is contained in the current legislation.⁶

- e) *processing relates to personal data which are manifestly made public by the data subject;*
and
f) *processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;*

A comparable legal ground is contained in the current legislation.⁷

- g) *processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be 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;*

This is an extension and further specification of the legal ground regulated in Article 14 let. b) of the Slovak Data Protection Act. Such legal ground is not yet regulated in the Czech legislation.

- h) *processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional;*
and

- i) *processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;*

These two provisions extend and further specify the current legal ground regulated in the current legislation.⁸

Sensitive data may be processed for the purposes referred to in point (h) when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by competent national bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by competent national bodies.

- j) *processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law, which shall be proportionate to the aim pursued, respect the essence*

⁵ Article 9 let. b) of the Czech Data Protection Act no. 101/2000 Coll. and Article 14 let. c) of the Slovak Data Protection Act no. 122/2013 Coll.

⁶ Article 9 let. e) of the Czech Data Protection Act no. 101/2000 Coll. and Article 14 let. d) of the Slovak Data Protection Act no. 122/2013 Coll.

⁷ Article 9 let. g) and h) of the Czech Data Protection Act and Article 14 let. e) of the Slovak Data Protection Act no. 122/2013 Coll.

⁸ Article 9 let. c) of the Czech Data Protection Act and Article 14 let. f) of the Slovak Data Protection Act no. 122/2013 Coll.

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.

It is a new provision under which the processing of sensitive data for the specified purposes is lawful if it is not inadequate in regard to the data subject's rights and appropriate safeguards for their protection are ensured (e.g. data minimisation, pseudonymization, etc.; please refer to Lesson 3).

Member States are entitled to maintain or introduce further conditions, including limitations, in regard to the processing of genetic data, biometric data or data concerning health. In regard to this provision, there may be further divergences in the conditions for processing this data in the legislation of various Member States, therefore entities processing such data on a cross border basis should pay due attention to existing nuances.

Changes in processing sensitive data

In connection to processing sensitive data the controller's obligations will change as follows:

- under Slovak conditions it is a novelty that the processing of a data subject's photograph or a graphic image of his/her signature will not be regarded as processing sensitive data, if they are not processed as biometric data, i.e. for a person's unique identification or authentication (e.g. for purposes of biometric passports);
- on the other hand, under Czech conditions, in the opinion of the Czech Office for Personal Data Protection⁹, it is clear that portraits reflect the racial or ethnic origin of the depicted person, clothing or headgear may reflect the religion etc. A photograph or other image of the person is a document of a personal nature, which also includes biometric and other characteristics of the data subject, revealing the facts defined in Article 4 let. b) of the Czech Data Protection Act as sensitive data, and can therefore be a source of information for the processing of sensitive data. However, if the information from the photography of the data subject is used for a mere distinction of its appearance compared to other persons and such information is not processed further, such use can't be considered as processing sensitive personal data. A similar view is also held by the Working Party WP 29, which in its opinion on online social networks notes that "*the working party in general does not consider images on the Internet as sensitive data, unless the images are clearly used to reveal sensitive data about individuals.*"
- the controller will not have to notify the Data Protection Authority or be subject to the obligation to register pursuant to Article 33 of the Act¹⁰, instead he/she will be required to keep records pursuant to Article 30 of the GDPR;
- if sensitive data is processed on a large scale¹¹, the controller will be obligated to carry out a data protection impact assessment and to appoint a data protection officer;
- the transfer of sensitive data to a third party with a seat in a third country which does not ensure an adequate level of protection of personal data will be lawful only based on the data subject's prior explicit consent, unless special legislation provides otherwise.

⁹ Opinion no. 12/2012, on the use of photography, video and audio recording of individuals.

¹⁰ The Czech Data Protection Act no. 101/2000 Coll. and the Slovak Data Protection Act no. 122/2013 Coll., both as amended.

¹¹ The term "on large scale" is not defined in the GDPR and with regard to direct applicability of the GDPR, the Slovak Data Protection Authority is not entitled to propose a definition of this term into local legislation. Until the Working Party 29 introduces guidelines in relation to the interpretation of this term, controllers may refer to recitals 91 and 97 of the GDPR.

Criminal records / data on offences

The GDPR does not classify this information as sensitive data. It will continue to apply that the controller, for purposes of processing personal data relating to:

- criminal convictions and offences or related security measures; or
- processing personal data in criminal registers pursuant to a special legislation;

may be a relevant public authority empowered by law.

Any comprehensive register of criminal convictions will be kept only under the control of an official authority.

Processing of a national identification number

Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application (e.g. a birth number). In that case, the national identification number or any other identifier of general application may be used only with appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.

What now

If the controller processes sensitive data, it is necessary to ensure that they do so based on a relevant legal ground pursuant to the GDPR. Should the legal ground be the data subject's consent, the wording and the way the consent is granted should be revised and updated in line with the new conditions.

Further information can be found here:

Recitals 51 – 56, 91, 97

Articles 4 (13) – (15), 9, 10, 87

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

