NEWSLETTER 5/2017

General Data Protection Regulation

New legal regulation of personal data protection

I. General Data Protection Regulation

- **As of 25th May 2018** the **General Data Protection Regulation ("GDPR")**, i.e. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, **will become effective** in all EU member states.

- The GDPR represents the **most important change in the area of the protection of privacy and personal data** since the existing Directive (95/46/EC) has been adopted; the new regulation **integrates the area at the level of EU** and will impact all subjects processing personal data.

- **The main aim** of the GDPR is to reinforce the protection of natural persons in connection with the internet expansion and the development of new surveillance instruments and at the same time to ease free movement of personal data within the united digital market.

- The new legislation has been adopted in the form of **Regulation**, which means that it will be directly **effective in the whole EU** and no national legal regulations will be established. In the Czech Republic it **will replace** the existing **Act No. 101/2000 Coll., on protection of personal data**.

II. Definitions under the Regulation

- **Personal data** means any information relating to an identified or identifiable natural person ("data subject"). The definition newly emphasizes that a natural person can be also identified by reference to an identifier such as location data or online identifier (e.g. web address or cookies) of that natural person.

- **Processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- **Controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes means and terms of the processing of personal data.

- **Processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

III. Consent of the data subject

- **Consent** of the data subject according to the GDPR means "*any **freely given**, **specific**, **informed and unambiguous** indication*" of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

- The consent must be presented **separately** from other conditions presented to the data subject for his or her approval and **cannot be a condition for providing the service**, unless the processing is necessary for providing such service.

- Where processing is based on consent, the controller shall be able to **demonstrate** that the data subject has consented to processing of his or her personal data.

- Within the consent the data subject should be informed about his or her rights according the GDPR; the data subject shall have **the right to withdraw** his or her consent at any time.

- The consent given **before** the date of effectiveness of the GDPR, which will not correspond with the requirements according the GDPR, cannot be seen as an updated and applicable one.

IV. Rights of the data subject

- One of the most significant changes brought by the GDPR will be **the remarkable reinforcement of rights of data subjects**. These rights will be especially following:

  (i) **right of access** by the data subject means the right to know and be informed specifically about the purposes of the processing, the period for which the personal data will be stored, recipients of personal data, the logic of automated processing and about possible results of such processing;

  (ii) **right to rectification** according to which the data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her;

  (iii) **right to erasure** is a right newly embodied in the GDPR and means the right of the data subject to obtain from the controller the erasure of personal data concerning him or her without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent, if the processing is based on the consent, and where there is no other legal ground for the processing; (c) the data subject objects to the processing; (d) the personal data have been unlawfully processed;

(iv) **right to be forgotten** is an extended right to erasure. The controller shall take reasonable steps, including technical measures, in order to erasure of any links to, or copy or replication of those personal data. However, the GDPR sets a lot of exceptions relating this right (e.g.: for reasons of public interest in the area of public health or for statistical purposes);

(v) **right to restriction of processing** means the right to obtain from the controller restriction of processing where one of the following applies: (a) the accuracy of the personal data is contested by the data subject, (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the defence of legal claims; (d) the data subject has objected to processing. The fact that the processing was restricted must be clearly marked in the system;

(vi) **right to data portability** may be applied by the data subject, if the processing (a) is based on consent or on the contract and (b) is carried out by automated means. In this case the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to keep those data for his or her personal use or transmit them to another controller. If it is technically possible, the data subject shall have the right to the transmission of his or her personal data from one controller directly to another one;

(vii) **right to object** means that the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her;

(viii) **the right not to be subject to a decision based solely on automated processing**, which produces legal effects concerning him or her.

V. Cancelation of the registry obligation and implementation of the principle of responsibility

- The GDPR abandons the principle of the mandatory registration of the controller with the Data Protection Office and newly establishes **the principle of responsibility**, which means that the controller and the processor are obliged, regardless of their size and number of their employees, to implement appropriate technical, organisational or procedural measures in order to be able to prove that they act in accordance with the data processing principles of the GDPR.

- In order to demonstrate the conformity with the GDPR, the controller and the processor shall adopt internal policies, realize procedural changes and install measures, which respect principles of the **data protection by design and by default**. These measures shall be based on **minimisation** of processing, **pseudonymisation**, **transparency** with respect to purposes of processing and on facilitated **access** by data subjects to their data. The controller and the processor may also follow the rules according the so-called **Codes of conduct** worked out by specialists.

VI. Data Protection Officer

- Absolutely new is the position of the **Data Protection Officer** (DPO). The controller and the processor **are obliged** to designate a data protection officer if:
  (i) the processing is carried out by a public authority or body (except for courts acting in their judicial capacity);
  (ii) their core activities consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
  (iii) their core activities consist of processing on a large scale of special categories of data (e.g. data relating to state of wealth).

- The Data Protection Officer might be appointed **voluntarily** too.

- The Data Protection Officer shall be designated on the basis of **professional qualities** and, in particular, expert knowledge of data protection law and practices.

- The Data Protection Officer may be **an employee** of the controller or processor, or fulfil the tasks on the basis of **a service contract**. The controller shall ensure that the DPO is involved all issues which relate to the protection of personal data. The DPO shall be independent and directly report to the highest management level of the controller or the processor.

VII. Security of processing

- The GDPR lays big stress on the field of security of processing. In the case of any personal data breach, **the controller must** without undue delay, but not later than 72 hours, **to notify the personal data breach to the Data Protection Office**; in serious cases the controller has to inform the data subjects too.

VIII. Supervision over controllers and processors with activities in more than one Member State

- New is also the legal regulation of the supervision over controllers and processors that have activities in more than one Member State. In this case the supervision will be exercised in all countries, where the controller or the processor has his seat, only by the supervisory authority from the country, where is the **main establishment** of the controller or the processor (i.e. the place of his central administration); unless the decisions on the purposes and means of the processing are taken in another establishment, in which case such establishment is to be considered to be the main establishment.

IX. Penalties

- The GDPR implements **high penalties** for breaches; depending on the seriousness of the breach it may impose an administrative fine up to **10 000 000 EUR** (or up to **20 000 000 EUR**), or up to **2%** (or up to **4%**) of the total worldwide annual turnover of the preceding financial year, whichever is higher.

We hope the above summary will ease your orientation in the new legislation. We are available for any of your additional requests or information or legal assistance in the area.

Editor: JUDr. Magda Stárková, advocate, e-mail: starkova@akvk.cz

---