NEWSLETTER

Information about the new data protection regulation of the EU and the related tasks

The new general data protection regulation no. 2016/679 of the European Parliament and of the Council (the "**Regulation**"), which **brings significant changes regarding the processing of personal data in its train,** will be applicable in the territory of the European Union **as of May 25, 2018.**

Please read our summary about the major rules of the Regulation, the changes and the actions to be taken.

(1) According to the definition of concepts in the Regulation, "personal data" means any information relating to an identified or identifiable natural person ("data subject"). Compliance with the Regulation is obligatory for every data controller or processor which is established in the Union, or which processes data in connection with the offering of goods or services to persons staying in the Union or while monitoring their behavior regardless of whether the processing actually takes place in the Union or not.

The Regulation is mandatory also in the absence of a relevant provision of the national law, and prevails over any divergent provision of the national law.

(2) By May 25, 2018, all data processing in progress must be coordinated with the rules of the Regulation. We would like to draw your attention to the following rules in particular:

- In the case of illegal data processing, i.e. an infringement of the Regulation, **the upper limit of the fine to be imposed will be 20 million EUR or 4 % of the total worldwide annual turnover,** whichever is higher. This represents a significant rise compared to the currently effective rules. Furthermore, the controller and the processor have joint and several liability for the entire material or non-material damage incurred as a result of an infringement of this Regulation; and the member states are also entitled to introduce other sanctions.
- According to the **principle of accountability**, the controller must fully document and prove the lawfulness of processing (i.e. the legal grounds, purpose and the required extent) and appropriate guarantees must be built in the data processing procedures in the future.
- **The range of legal grounds for data processing has increased** from two to six; the legitimate interest of the processor is a new one, and the necessity of a contract concluded/to be concluded with the data subject for processing is a legal basis which eliminates the difficulties caused by the obligation to obtain the data subject's consent.
- **It is a novelty** that a **prior impact assessment** must be carried out before data processing for the case **where the data processing involves high risk** for the rights of natural persons (e.g. when introducing new technologies); in this respect, it must be examined how the planned operation affects the protection of data, and it may also be mandatory to request the opinion of the data protection authority.
- The Regulation allows processing for a purpose **differing from the intended purpose of data collection**, but compatible with the original purpose, if the relevant aspects are given.
- A larger emphasis and a more detailed regulation is devoted to the **information obligation of the processor.** Special attention must be paid to this, since providing inappropriate information may cause that data processing becomes unlawful.
- The requirements of **internal data protection policies** for controllers and processors have been determined regarding the data processed and the disclosure by transmission to third parties, as well as compliance with the Regulation. We would like to note that the internal data protection policies are not identical with the ones determined by the effective Act on Information, which affects only special data controllers.
- It becomes obligatory for the controllers to notify any **personal data breach** to the data protection authority within a tight timeframe, and in some cases even to notify the data subjects; however, the scope of events determined as personal data breach is narrower. All these increase the risk of an authority procedure, imposing a fine and the claim assertion by the data subject.
- The new provisions concern the obligations of processors and the related contracts.
- **Joint data control** has been regulated (i.e. where two or more controllers jointly determine the purposes and means of processing), which extends to the legal relationship of controllers, thus also to their respective liability.

- The scope of employment, duties and independence of **the data protection officer** (currently: person in charge of data protection) increases and his/her legal status is strengthened from a labor law perspective.
- The conditions of the applicability of **binding corporate rules** are also regulated, which primarily affects data disclosure by transmission to a member of the company group outside the EU.
- **The rights of data subjects** are supplemented by the right to data portability (release of data to the data subject and direct transmission to another controller), and the rights are also expanded in respect of data control with automated processing, including profiling (e.g. the data subject's right to object and the manner of exercising his/her right of information).
- The possibility of **pseudonymisation** is introduced, which means that as a result of technical and organizational measures, the personal data can no longer be attributed to a natural person without the use of additional information, provided that such additional information is kept separately. This institution does not only provide safety but it is also useful, since processing for different purposes (e.g. statistical purposes) becomes possible. The introduction of pseudonymisation does not exclude the possibility to choose any other data protection measure.
- The Regulation regulates the possibility of **disclosure by transmission** and the data subject's **right to erasure** in a broader range than the effective legal regulations.
- **The rules of the Regulation are also applicable in respect of processing in the context of employment with the proviso** that **Member States may, by law or by collective agreements, provide for more specific rules in this respect** until May 25, 2018.

With regard to the fact that the effective Hungarian legal environment is superseded by the Regulation, it must be examined by all means whether data controlling and processing is performed in line with the Regulation or not.

Please note that no additional EU or national detailed regulations have been elaborated so far, but it should be closely observed whether such detailed rules appear before the entering into effect of the Regulation.

(3) The following duties may arise in connection with the Regulation:

1. **Developing data controlling in compliance with the Regulation, elaborating appropriate internal policy**; **documenting** the source of the existing information and their transmission, as well as compliance with the Regulation.
2. **Reviewing** and modifying **the contracts** affecting data controlling (including joint control) and processing, **developing a new contractual practice.**
3. **Reviewing the legal grounds applied** in connection with the processing of personal data in light of the new legal grounds, appropriate documentation (preparing an impact study, if necessary).
4. **Providing appropriate information** to the data subject, **documenting this** and **reviewing the** present **data protection declarations** and the related internal policies.
5. Transforming and/or developing internal procedures to eliminate, notify and examine personal **data breaches**, with special regard to outsourced activities (e.g. data processing).
6. Elaborating **internal data protection policies** whose contents comply with the Regulation.
7. Reviewing the method of requesting and documenting **consents to processing**, with special regard to **children** (introducing the checking of the age of data subjects, and, if need be, obtaining the parents' consent to the processing).
8. Handling the data subjects' **requests in connection with access, transmission or profiling**; updating the relevant procedures, settling information safety issues, and reviewing the related practice.
9. Uncovering the obligatory application areas of **pseudonymisation**, and exploiting the possibilities involved, internal regulation.
10. **As regards the right to erasure and the right to be forgotten,** the contents of the Regulation must be enforced and the current data erasures performed, internal regulations updated.
11. Preparing for and executing **data protection impact assessments** (by taking the new system of aspects prepared by the data protection authority into consideration).
12. Appointing a **data protection officer** for carrying out the above duties, and identifying the data protection supervisory authority competent in the Member State.
13. Preparing and implementing **IT developments**.

Should you need further information about the above, or should you need our assistance in performing the assessments and carrying out the duties as regards compliance with the Regulation, please do not hesitate to contact us.

Budapest, April 4, 2017

***

This Newsletter has been prepared for information purposes and cannot be deemed as a comprehensive analysis of the modifications. Therefore it cannot be interpreted as a legal opinion or a legal advice in a concrete matter.

Szabó, Kelemen & Partners Attorneys
address Lövőház utca 39, 1024 Budapest, Hungary
web www.sz-k-t.hu
phone +36 1 288 8200
fax +36 1 288 8299