The European Parliament has approved the General Data Protection Regulation

18 May 2016

In brief

Recently, Regulation (EU) 2016/679, dated 27 April, of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data and repealing Directive 95/46/EC was published in the Official Journal of the European Union (the "**Regulation**").

The Regulation establishes a framework of rules related to data protection at the European Union level, enlarges the territory within which the European Union regulations are applicable as regards personal data, imposes new obligations and acknowledges new rights, setting also significant fines for breaching these legal provisions (up to EUR 20 million or 4% of a company's annual worldwide turnover). The Regulation repeals Directive 95/46/EC (General Data Protection Regulation) (the "**Directive**").
The Regulation will enter into force on 25 May 2016, 20 days after its publication date in the Official Journal of the European Union. The Regulation will become directly applicable in the member states in two years following its entry into force, without the necessity of being transposed into national law.

In detail

The Regulation is the result of a process which started in 2009 and included studies, conferences, roundtables and public consultation sessions with interested parties ("stakeholders"), such as the national regulation authorities, consumer protection organisations and others.

The principal amendments with regard to personal data are as follows:

1. **Broadening the definition of personal data and the provision of new definitions.** "*The identification number, location data, online identifier*" are expressly included in the meaning of personal data. Moreover, new definitions are provided for notions such as: "*personal data breach*", "*genetic data*", "*biometric data*", "*data concerning health*", "*group of undertakings*", "*main establishment*", "*child*" and others.
2. **Higher standards for obtaining the data subject's consent**. The Regulation expressly provides that the consent has to be "*explicit*" and that the acceptance has to be "*in a statement or through a positive action that leaves no place for equivoque*". Inactivity or silence cannot represent consent. The declaration of consent

has to be distinct from declarations regarding other aspects (for example, of acceptance of terms and general conditions). The consent can be withdrawn by the data subject. As regards a child's consent, "*where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child*". Member states may lower the threshold age, to a minimum of 13 years.

3. **Significant expansion of the geographical area of application of the European Union's personal data regulations**. The Regulation applies to personal data processing "*in the context of the activities of an establishment of a controller or a processor in the Union*", irrespective of whether the data processing is actually conducted within or outside the European Union. Moreover, the Regulation applies to "*the processing of personal data of data subjects residing in the Union by a controller not established in the Union where the processing activities are related to: (i) the offering of goods or services to such data subjects, or (ii) to the monitoring of their behavior as far as their behavior takes place within the Union*", by a controller that is not established in the European Union.

4. **Provision of new rights for the data subjects**. Data subjects have new rights under the Regulation, including the "right to be forgotten" (the request to erase the personal data) or to rectification, the right to data portability (that is the right of transmitting the data to another controller), the right to object to the processing of personal data, including through profiling. Controllers have new obligations correlated with the the data subjects' rights.

5. **Profiling**. The Regulation stipulated a new restriction for controllers regarding the adoption of decisions based on automated processing, if such processing "*produces legal effects concerning this individual or significantly affects them*". Such processing is allowed, however, based on the data subject's express consent, if necessary for concluding a contract or if expressly authorised by a Union or Member State law.

6. **Obligation to designate a data protection officer**. If (i) the processing is carried out by an enterprise employing 250 or more people; or (ii) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and / or their purposes, require regular and systematic monitoring of data subjects, the controller is obliged to designate a data protection officer (employee or service provider). The data protection officer is responsible to the controller's top management.

7. **Obligation to notify the supervisory authority in the event of a personal data security breach.** Controllers have to notify the supervisory authority within 72 hours of becoming aware of a breach. When the personal data breach is likely to affect adversely the protection of the personal data or privacy of the data subject, the controller also has to communicate the personal data breach to the data subject, without undue delay.

8. **Liabilities, impact assessment, implied protection**. Controllers have to prove they observe the Regulation, including by applying transparent and easily accessible policies concerning the processing of personal data and the exercising of the data subject's

rights. The Regulation provides requires controllers and processors to conduct an impact evaluation of processing operations with personal data, if the processing presents a specific risk to the rights and liberties of the data subject. Moreover, under the Regulation, controllers and processors have to implement technical and organisational measures in such a way that the processing meets the security level in accord with the risks such processing implies and with the personal data that should be protected.

9. **Significant sanctions**. Fines of up to EUR 20 million or 4% of the annual worldwide turnover can be applied to controllers and operators for breaching the Regulation. The sanction will be imposed on a case-by-case basis, considering certain criteria, such as: the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the individual or legal person and of previous breaches by them, the technical and organisational measures and procedures applied, and the degree of cooperation with the supervisory authority in order to remedy the breach.

[Source: *Official Journal of the European Union no. 119L 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, published on 4 May 2016*]

The takeaway

The Regulation represents a significant change to the legislative framework for personal data protection. In preparation for the Regulation's entry into force, controllers should adopt and implement a strategy regarding personal data processing covering at least the following:

(i) Assess what personal data is processed and for what purpose, considering that is possible for such processing to respect the legal framework imposed by the Directive but to breach the Regulation;

(ii) Assess whether the clauses of existing agreements respect the Regulation;

(iii) Review personal data processing policies, procedures and notifications, and update them to comply with the Regulation;

(iv) Assess the requirement to designate a data protection officer.

Let's talk

For a deeper discussion of how this issue might affect your business, please contact:

Sorin David, *Partner*
sorin.david@david-baias.ro

Dan Dascalu, *Partner*
dan.dascalu@david-baias.ro

Anda Rojanschi, *Partner*
anda.rojanschi@david-baias.ro

Manuela Guia, *Partner*
manuela.guia@david-baias.ro

PwC Romania

Lakeview Building
301-311 Barbu Văcărescu Street
Sector 2, Bucharest
Tel.: + 40 21 225 3000
Fax: + 40 21 225 3600

D&B David si Baias SCA

Lakeview Building
301-311 Barbu Văcărescu Street
Sector 2, Bucharest
Tel.: + 40 21 225 3770
Fax: + 40 21 225 3771