CVETKOVIĆ, SKOKO & JOVIČIĆ
LAW OFFICE

Knez Mihailova Street 7/IV • 11000 Belgrade • Serbia • Phone/fax (+381) 11 3281-949 • 3281-890 • 3283-764 • www.cplaw.rs • e-mail: office@cplaw.rs

March 2018

In focus: General Data Protection Regulation of the European Union

On April 27th 2016, the European Parliament and the Council of the European Union adopted the Regulation 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 (hereinafter: the "**Regulation**"), which shall apply starting from May 25th 2018.

One of the main reasons for adoption of Regulation is the need for increased protection of the individual due to rapid technological developments and globalization which lead to a significant increase in the scale of collecting and sharing personal data. Thus, the aim of the Regulation is a strong and more coherent data protection framework that will allow the digital economy to develop across the European Union (hereinafter: the „**Union**"), in a way that the right to data protection shall be regulated and balanced with other fundamental rights stipulated in the Charter of Fundamental Rights of the Union, in accordance with the principle of proportionality.

Although the Republic of Serbia is not a state member of the Union, the Regulation shall be applicable directly to certain business entities in the Republic of Serbia. In addition, the Republic of Serbia has opened chapter 23 in the process of integration negotiations with the Union (which, inter alia, relates to personal data protection), which implies that the regulations of the Republic of Serbia will be harmonized with the provisions of the Regulation. The stated is confirmed by the working draft of a new Data Protection Law which was published in December 2017 by the Ministry of Justice of the Republic of Serbia, where its provisions introduced most of the institutes that are regulated by the Regulation.

The text bellow shall introduce the overview of the territorial scope of the Regulation as well as the most relevant solutions and institutes subject to the Regulation.

I. Territorial scope

The Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

Additionally, the Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data

subjects in the Union; or (b) the monitoring of their behavior as far as their behavior takes place within the Union.

II. Personal data and identification of a natural person

The Regulation defines personal data as any information relating to an identified or identifiable natural person. In the context of ubiquitous digitalization process, the Regulation, among other identifiers, regulates the online identifier for identification of the data subject, protected by this Regulation, which can be connected with natural persons via their devices or applications.

III. The grounds for processing of personal data

The Regulation has introduced the exact grounds for processing of personal data: (1) the consent of the data subject, (2) performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (3) compliance with a legal obligation to which the controller is subject; (4) protection of the vital interests of the data subject or of another natural person, (5) performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, (6) existence 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 which require protection of personal data.

IV. Processing based on consent

The Regulation stipulates that consent for processing personal data should be a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data, such as by a written statement, including by electronic means, or an oral statement. In addition, the Regulation exempli causa regulates what shall be considered as electronic statement (e.g. ticking a box when visiting an internet website), and what shall not be considered as consent (silence, pre-ticked boxes).

V. Processing based on a child's consent

By the Regulation, a child under than 13 years of age shall never be entitled to give consent for the processing of personal data in relation to online services. For children 13 to 15 years of age, there is a general rule by which the consent of the parent is mandatory, unless member states of the Union provide by law that the parent's consent is not mandatory for that age, but in any case, member states shall not be entitled to reduce this limitation below 13 years.

Children that are at least 16 years old may independently give their consent for the processing of personal data in relation to online services. The Regulation does not stipulate a child's consent for processing of data that are not in relation to online services, which means that regulations of member states shall be applicable in these situations.

VI. Legitimate interests as the ground for processing of personal data

The Recitals of the Regulation stipulates what can be treated as legitimate interests of the controller or third party for processing of personal data, for example when the data subject is a client or in the service of the controller, as well as in the case of processing of data for the purpose of preventing fraud or for the purpose of direct marketing.

The legitimate interests of the controller or third party for processing of personal data shall not be sufficient when such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

VII. Notification on processing

The Regulation extensively regulates the information that controller is obliged to deliver to data subject. The controller is obliged to provide the data subject with notification at the time when personal data are obtained, if personal data are collected from the data subject, and in other cases:

- within reasonable time after obtaining the personal data, but at the latest within one month;
- if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject;
- if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

The controller shall not be obliged to provide the notification in certain cases, for example when the provision of such information proves impossible or would involve a disproportionate effort.

VIII. Rights of the data subject

The Regulation on systematic manner regulates the rights of the data subject (as well as the terms and conditions for exercising those rights): 1) right to access and information on processing; 2) right to rectification; 3) right to erasure ('right to be forgotten'), 4) right to restriction of processing; 5) right to data portability; 6) right to object; 7) right to withdraw the consent for processing of personal data; 8) right not to be subject to a decision based solely on automated processing; 9) right to be notified on personal data breach; 10) right to lodge a complaint with and effective judicial remedy against a supervisory authority, 11) right to an effective judicial remedy against a controller or processor, 12) right to compensation of material and non-material damage.

IX. Records of processing activities

The Regulation stipulates the obligation for a controller and processor to maintain a record of processing activities. The obligation of maintaining a record of processing activities shall not apply to an enterprise or an organization employing

fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data or personal data relating to criminal convictions and offences.

X. Security of processing and personal data breach

According to the Regulation, the controller and processor are obliged to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. The Regulation prescribes some of the technical and organizational measures which might be taken, such as: (a) the pseudonymization and encryption of personal data, (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

In addition, the Regulation stipulates the procedure, i.e. the system of notification in case of the personal data breach: 1) obligation of the processor to notify the controller on personal data breach; 2) obligation of the controller to notify the supervisory authority on personal data breach; 3) the obligation of the controller to notify data subject on personal data breach. The notification obligation of the controller and processor entails their previous obligations in terms of measures taken or proposed to be taken to mitigate its possible adverse effects.

XI. Data protection impact assessment and prior consultation

The Regulation prescribes the obligation of the controller to, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data if some type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons.

The controller shall consult the supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. Where the supervisory authority is of the opinion that the intended processing would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority, within the terms stipulated by the Regulation, shall provide written advice to the controller and, where applicable to the processor.

XII. Data protection officer

The Regulation introduces the data protection officer. The controllers and processors are obliged to appoint him: (1) where the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (2) where 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 on a large scale; or (3) where the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.

The controllers and processors shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data as well as that data protection officer performs his tasks in independent manner without any instructions, retribution or dismissal due to lawful exercise of those tasks. The data protection officer shall directly report to the highest management level of the controller or the processor. The Regulation regulates in detail the tasks and obligations of data protection officer.

XIII. Codes of conduct and certification

The Regulation encourages the drawing up of codes of conduct intended to contribute to the proper application of this Regulation. The supervisory authority is competent to provide an opinion on whether the draft code or amendment complies with this Regulation and to approve that draft code or amendment.

The Regulation also encourages the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The certification shall be issued by certification bodies accredited by supervisory authority or the national accreditation body, under the terms closely stipulated in the Regulation.

XIV. Transfers of personal data to third countries or international organizations

The transfer of personal data to third countries or international organizations may take place by the Decision on adequacy rendered by the Commission of the Union, based on the terms closely stipulated in the Regulation. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organization ensures an adequate level of protection. The Regulation stipulates certain exceptions by which transfer of data may be executed to the third parties or international organizations without previous decision on adequacy.

XV. Administrative fines

The Regulation stipulates the general terms for imposing administrative fines and criteria which supervisory authorities need to take into consideration when deciding whether to impose an administrative fine. Depending on the provisions of the Regulation that are infringed, the following administrative fines are stipulated:

- up to 10.000.000,00 EUR, or, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher;
- up to 20.000.000,00 EUR, or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Member states of the Union shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.