12. ROMANIAN DATA PROTECTION LAWS

Updated January 2018

The relevant **Romanian data protection laws** are:

- ✓ Law no. 677 of 2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, as further amended ("**Law no. 677**") which will no longer be applicable starting with May 25, 2018

- ✓ As of May 25, 2018, the European Regulation no. 679 of 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, which repealed Directive 95/46/EC ("**GDPR**"), will take effect and will become directly applicable in Romania

- ✓ Law no. 506 of 2004 regarding the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector

- ✓ Guidelines issued by the National Authority for the Supervision of Personal Data Processing (the "DPA") on September 21, 2017 with regard to the implementation of the GDPR

- ✓ Various Guidelines issued by the Article 29 Data Protection Working Party on data processing at work (of June 8, 2017), on automated individual decision-making and profiling for the purpose of the GDPR (of October 3, 2017), on personal data breach (of October 3, 2017), on consent (November 28, 2017), on transparency, on data protection impact assessment (DPIA) of April 4, 2017

Note

The DPA is currently drafting a law for the implementation of the GDPR in Romania, which should be available by May 25, 2018.

Also, additional guidelines and secondary legislation are likely to be issued both at European level as well at local level with regard to the implementation of the GDPR.

1. Applicability of the Law no. 677

The provisions of the Law no. 677 apply when the data controller (i) is domiciled in Romania, or (ii) uses equipment or means to process personal data located in Romania, (unless the equipment or means are used only for purposes of transit data through Romania). If the data controller uses means and equipment in Romania, but is not domiciled in Romania, the data controller must designate a representative in Romania.

2. Applicability of the GDPR

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

Also, the GDPR, applies to the processing of personal data:

a. of data subjects who are in EU by a controller or processor which is not established in EU, where the processing activities are related to: (a) the offering of goods or services,

irrespective of whether a payment by the data subject is required; or (b) the monitoring of the data subjects' behavior as far as their behavior takes place within EU.

b. by a controller not established in EU, but in a place where Member State law applies by virtue of public international law.

In case the data controller is not registered within EU, the data controller must designate in writing a representative within EU.

3. Data Controllers

Law no. 677

The processing of personal data is defined by Law no. 677 as any operation or set of operations involving personal data, performed by automatic or non-automatic means, such as collection, recording, storage, adaptation or alteration, retrieval, consultation, use, disclosure to a third party by transmission, dissemination or by any other means.

The personal data controller is a natural, or legal person, which decides on the purpose and means of the personal data processing, and operates a recording system of personal data collection and processing which provides specific criteria for accessing the respective data.

GDPR

The processing of personal data has a broader meaning under the GDPR, i.e. any operation or set of operations which is performed with regard to personal data, or 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.

The GDPR defines the controller as the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by EU or Member State law. The controller or the specific criteria for its nomination may be provided for by EU or Member State law.

4. Notification of the Data Processing

Law no. 677

According to Law no. 677, the data controllers must notify the personal data processing to the National Authority for the Supervision of Personal Data Processing (the "**DPA**").

The Notification is sent to the DPA before starting any processing or transfer of personal data. All the documents to be filed with the DPA must be in Romanian. No filing fees must be paid when filing a Notification.

If the data controller processes personal data for two or more unrelated purposes, then it has the obligation of filling in separate Notifications for each of these purposes. The data controller must notify the DPA prior to starting any processing of the personal data.

The failure to notify, in the cases in which the Notification is mandatory, as well as the incomplete Notification or the Notification which contains false information, are violations punishable by fines, provided that they are not committed in such circumstances that will make them subject to criminal law.

Consequently, the data controller must first obtain the DPA's confirmation that the Notification is valid and was assigned a registration number in the Register of Recording of the Personal Data Processing. After receipt of the above-mentioned confirmation, the data controller may start processing and/or transferring the data.

The obligation to submit Notifications with the DPA will remain in effect until May 25, 2018, when the GDPR will become applicable.

GDPR

The GDPR removes the general requirement for the data controller to file a Notification with the DPA regarding the collection and processing of personal data and to seek approval from the DPA in some cases.

5. Sensitive Data

Law no. 677

Sensitive data are the data related to racial or ethnical origin, political, religious, philosophical opinion, criminal offences, minor offences or other convictions, trade union membership, as well as data regarding health or sex life. In addition to these data, under the Law no. 677, personal identification numbers, or other personal data with a general identification function i.e., national ID/passport details are considered sensitive data. The collection and processing of sensitive data require the prior and express consent of the owner of the data.

GDPR

As a general rule, the GDPR provides that the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

The processing of personal data relating to criminal convictions and offences or related security measures based on the consent shall be carried out only under the control of official authority or when the processing is authorized by EU or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.

6. Transfer of the personal data abroad

Law no. 677

In accordance with the Law no. 677, the transfer of personal data to another country is subject to the filing of a prior Notification with the DPA. The transfer of data does not have to be authorized by the DPA if the data are transferred to an EU/EEA country, or to a non-EU/EEA country for which the European Commission has issued an adequacy decision or other mechanisms are in place to ensure an adequate level of protection. Currently the transfer of the personal data to the USA may be done based on the Standard Contractual Clauses approved by the European Commission, US Privacy Shield or based on the consent of the data subject.

GDPR

The transfer of personal data outside the country is no longer object of a Notification to the DPA.

GDPR states that:

- The free movement of personal data within EU is neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

- As a general rule, transfers to third countries, i.e. outside EU, can be carried out (i) on the basis of an adequacy decision, or (ii) based on appropriate safeguards. In the absence of an adequacy decision, or of appropriate safeguards, a transfer of personal data to a third country can take place only in certain conditions, among which:

  (i) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

  (ii) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

  (iii) the transfer is necessary for the conclusion or performance of a contract concluded, in the interest of the data subject, between the controller and another natural or legal person.

7. Registry for Recording the Personal Data Processing

Law no. 677

The Registry for Recording of the Personal Data Processing has the role of assuring the transparence regarding the data controllers' activities and may be consulted by any interested person, such being available online on the DPA's website.

GDPR

The Registry for Recording of the Personal Data Processing will no longer be relevant further to the start of the application of GDPR, given that data controllers are no longer required to file Notifications with the DPA.

8. Novelty of the GDPR

HIGH SANCTIONS. GDPR sets higher fines in case of breach of its provisions than those provided by the current legislation, i.e. fines of up to EUR 20 million or 4% of the annual worldwide turnover can be applied to data controllers for breaching the provision of the said regulation.

HIGHER STANDARDS FOR OBTAINING THE DATA SUBJECT'S CONSENT. The Regulation provides the following rules in relation to the consent of the data subject:

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

- If the data subject's consent is given in the context of a written declaration which also concerns other matters (for example it is included in the employment contract or in an addendum to the employment contract), the request for consent shall be presented in a manner which is clearly distinguishable from the other matters.

- The data subject has the right to withdraw his or her consent at any time and such withdrawal should be as easy as giving the consent. Prior to giving consent, the data subject shall be informed that he/she can withdraw his/her consent at any time.

- When assessing whether consent is freely given, utmost account shall be taken of whether the performance of a contract is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

PROVISION OF NEW RIGHTS FOR THE DATA SUBJECTS. Regulation no. 679 provides new rights for the data subjects in addition to the existing rights. Thus, the data subjects have the following new rights:

- Right to erasure from the database ('right to be forgotten');
- Right to restriction of processing;
- Right to data portability.

NEW OBLIGATIONS OF THE DATA CONTROLLER. One of the key changes in the Regulation no. 679 is that data processors have direct obligations for the first time

- To implement appropriate technical and organizational measures in order to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR.
- To implement appropriate technical and organizational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing.
- To implement appropriate technical and organizational measures for ensuring that only personal data which are necessary for each specific purpose of the processing are processed.
- To maintain records of the processing activities.
- To notify the DPA in case of a personal data security breach.
- **Obligation to designate a data protection office**r.
- To conclude an agreement with the processor which includes all the provisions which are mandatory to be included in such agreement according to the GDPR.
- To carry out an assessment of the impact of the envisaged processing operations on the protection of personal data, prior to the processing, in case a 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.
- To consult the DPA prior to processing in case 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.

JOINT CONTROLLERS. In case two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall determine their respective responsibilities for compliance with the obligations under the GDPR, by means of an agreement between them.