12. ROMANIAN DATA PROTECTION LEGAL REGIME

Updated October 2018

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

- ✓ 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of natural persons with regard to the processing of personal data and on the free movement of such data, which repealed Directive 95/46/EC ("**GDPR**"), will take effect and will become directly applicable in Romania

- ✓ 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 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

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: (i) the offering of goods or services, irrespective of whether a payment by the data subject is required; or (ii) 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.

Thus, the GDPR has an extended jurisdiction since it applies to all companies processing the personal data of data subjects residing in EU, regardless of the company's location.

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

Novelties brought by the GDPR

Consent of the data subject

GDPR 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 the 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.

Rights of the data subject

GDPR provides new rights for the data subjects in addition to the existing rights. Thus, the data subjects have the following new rights:

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

Data Controllers & Processors

The GDPR defines the data 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.

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.

One of the key changes brought by the GDPR is that data processors have direct obligations such as:

- 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 pseudonymization, 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.

Notification of the Data Processing

Another key change brought by the GDPR is the removal of the general requirement for the data controller of filling a Notification with the relevant data protection authority regarding specific processing of the personal data. Thus, as per the press release posted on the DPA's website on May 17, the DPA officially advised that the data controllers will no longer be required to file Notifications as of May 25.

Under GDPR, the key responsibility of a data controller is to be accountable, i.e. to take actions in line with GDPR, and to be able to explain the compliance with GDPR to the data subjects and the DPA, as and when required.

The compliance with the GDPR provisions

The following steps that must be taken by a compliant company:

1. To identify all the data processing operations carried out by the company and keep records of the processing activities

The companies with more than 250 employees have the obligation to keep records of the data processing. Small businesses employing fewer than 250 employees are exempt from these records keeping requirements unless their processing activities are risky, frequent or include sensitive personal data.

The records must provide among others:

(i) The categories of data which are processed.

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, and 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 appropriate safeguards for the rights and freedoms of data subjects.

(ii) The legal basis for the processing purposes.

(iii) The location of the data storage system and of the data recipients.

(iv) The states where the personal data are transferred and the time limits for the keeping of the personal data;

As a general rule, transfers to third countries, i.e. outside EU, can be carried out on the basis of an adequacy decision, or 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:

- 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;

- 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;

- 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.

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

(v) The security measures taken by the company.

The companies must implement Security Policies mentioning the security measures taken in accordance with the GDPR provisions.

2. To carry out a Data Privacy Impact Assessment ("DPIA")

The companies must carry out a DPIA where new personal data processing involves the "systematic and extensive evaluation" of individuals resulting in legal effects, or significantly affects those individuals.

Under the GDPR, the data controller/processor must not only comply with the general principles provided by GDPR, but also be able to prove such compliance. If the data controller is carrying out "high risk" processing, it must carry out a DPIA and, in some cases, consult the DPA.

A DPIA is mandatory if the processing operation is "likely to result in a high risk to the rights and freedoms of natural persons". When determining whether data processing is likely to result in a high risk, the Guidelines issued by Art. 29 - Working Party on April 2017 provide the criteria that must be taken into consideration.

The Guidelines provide that processing operations meeting at least two of these criteria will require a DPIA. However, a processing operation meeting only one criterion may require a DPIA depending on the circumstance. Art. 29 - Guidelines also recommend using a DPIA when a processing operation is using new data processing technology.

In case a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, the data controller must consult the DPA.

3. To appoint a Data Protection Officer (DPO)

GDPR provides that the private entities, irrespective of their size and their capacity (data controller or data processor), must appoint a DPO if such:

- are involved in regular and systematic monitoring of data subjects on a large scale; or

- conduct large-scale processing of special categories of personal data, like that which details race or ethnicity or religious beliefs.

According to the Guidelines posted on the website of the Romanian DPA *http://www.dataprotection.ro/index.jsp?page=Lansare_Ghid_aplicare_RGPD&lang=ro* on

September 21, 2017, the DPA's recommendation for private entities is to appoint a DPO even if such appointment is not mandatory under GDPR.

DPO's responsibilities:

- informing the company's management and its employees on the GDPR's compliance requirements;
- training staff involved in data processing;
- conducting audits to ensure compliance and address potential issues proactively;
- serving as the point of contact between the company and the DPA;
- maintaining comprehensive records of all data processing activities conducted by the company;
- interfacing with data subjects to inform them about how their data are being used, their rights to have their personal data deleted, and what measures the company has put in place to protect their personal information.

4. To update the Notices of Information and the Privacy Policies

The Notices of Information and the Privacy Policies must be updated in order to provide the legal basis based on which the data are processed and all the data subjects' rights provided by the GDPR.

5. To inform the DPA and the data subjects regarding any breach of the security of the personal data in accordance with the provisions of Art. 33 and Art. 34 of GDPR

In case that the security breach causes serious risks for the individuals' rights and freedoms, the data controller has the obligation to file a Breach Notification with the DPA. The breach must be notified to the DPA within 72 hours after the data controller becomes aware of it. A template of the Breach Notification is posted on DPA's website. The DPA's Decision no. 128 of 2018 requires the data controller to sign the Breach Notifications with electronic signature, and file it electronically.

According to Article 34 of the GDPR, when the personal data breach is likely to result in a high risk regarding the rights and freedoms of natural persons, such breach must be also immediately notified to the affected data subjects.

The sanctions for the breach of GDPR

GDPR sets higher fines in case of breach of its provisions than those provided by the previous data protection 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.

Implementation of GDPR in Romania

The Law no. 190 of 2018 on the Measures for the Application of the GDPR ("**Law no. 190**") provides the rules for the implementation at national level of the GDPR.

Given that the GDPR provides Member States with the possibility to adopt further exemptions, derogations, conditions, or rules in relation to specific processing activities, the Law no. 190 includes provisions regarding the following matters:

(i) The processing of the personal data in the employment context in case electronic or video surveillance systems are used by the employer at the working place.

This type of processing can be done subject to the additional conditions provided by Law no. 190, including the consultation with the Trade Union/Employees' Representatives.

(ii) The processing of the personal identification numbers of the natural persons in relation to the legitimate interest of the data controller. The processing can be done by ensuring additional safeguards, including the appointment of a DPO.

(iii) The processing of health data for an automated decision-making purpose or profiling is permitted only with the explicit consent of the data subject.