privacyONE
in alliance with BIRIȘ·GORAN

LEGAL ALERT

LAW FOR THE APPLICATION OF THE GENERAL DATA PROTECTION REGULATION IN ROMANIA

Date: 27 July 2018

Contact

47 Aviatorilor Blvd., 2nd floor, Sector 1,
Bucharest, Romania

www.privacyone.ro

contact@privacyone.ro

Context

On 25 May 2018, the general legal framework for data protection was substantially amended along with the application of Regulation (EU) no. 2016/679 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 („**GDPR**").

Although the GDPR is directly applicable in all EU member states, the regulation allows each country to adopt derogations or guarantees in certain specific cases – such as journalism, processing of a national identification number or in the context of employment.

In order to institute such derogations, on 27 June 2018 the Romanian Parliament has adopted Law no. 190/2018 providing measures for the application of the GDPR (hereinafter "**GDPR Application Law**", published in the Official Journal no. 651 of 26 July 2018).

The GDPR Application Law enters into force on 31 July 2018 and provides special rules for processing of certain categories of personal data, derogations from GDPR, guidelines for appointing a data protection officer (DPO), for certification authorities, as well as provisions on sanctions.

Additionally, the rules concerning the organization and functioning of the Romanian National Data Protection Authority (ANSPDCP) were amended through a separate law – Law No. 129/2018 in force from 24 June 2018, a form for the notification of personal data breaches to the ANSPDCP was adopted - Decision No. 128/2018 available here, and the procedure for settling complaints has been approved – Decision No. 133/2018 available here.

Relevance

The GDPR Application Law provides special rules or restrictions for certain personal data processing, meaning that the persons who process the personal numeric code (CNP) or apply measures for workplace surveillance must analyze if their processing operations comply with the new rules. For journalistic activities, the law allows for derogations from most categories of GDPR obligations.

If notifiable personal data breaches occur the template notice adopted by ANSPDCP shall be used. In case of on-site investigations, ANSPDCP must observe the guarantees imposed by its organization and functioning law.

Genetic, biometric and health-related data

The automatic decision-making processes or profiling which use genetic, biometric or health-related data may be carried out only based on the consent of the data subjects or if there is an express legal provision. Processing of these categories of data for other purposes is not retricted, thus all grounds provided by Article 9.2 GDPR shall be applicable.

Personal Numeric Code

The conditions for the processing of a national identification number (such as the CNP) in Romania are loosened – it is no longer required to base the processing solely on a legal obligation, consent or the ANSPDCP authorization. Thus, the CNP may be processed based on the legitimate interest (of the controller or a third party), but in this case (and not for the other legal grounds) there are additional requirements:

a) application of technical measures to comply with the data minimization principle and ensure security measures;
b) appointment of a data protection officer (DPO);
c) establishment of data storage periods;
d) periodic training of the personnel who processes data under the authority of the controller or its processor.

Workplace surveillance

Those who are using systems for monitoring employees by [sic] electronic means of communication or video surveillance must comply with the following rules:

a) to thoroughly justify the legitimate interests sought and to ensure that they prevail over the rights and freedoms of the data subjects (*Note: meaning that it is necessary to perform a balance test, and also to document such test in order to demonstrate compliance*);
b) to ensure the full, explicit and prior information of the employees (*Note: the information does not mean collecting consent, which is generally not indicated in employment relationships – however, employers must prove that they provided such information*);
c) to consult in advance with the trade union or the employees' representative;
d) to apply other less intrusive means for fulfilling the purpose for which the monitoring is required and to perform the monitoring only if such less severe

measures were not efficient;

e) the storage period for the personal data resulting from the monitoring may not exceed 30 days, except for the cases expressly regulated by law or in thoroughly justified cases (*Note: thoroughly justified cases may consist in defending claims in court where an incident was recorded on camera, as well as other cases which must be however justified in writing*).

Mention should be made that, although the title of the article is "Processing of personal data in the employment context", the article only concerns these two particular situations, thus leaving unresolved other situations that occur very often, such as processing of sensitive data or data relating to criminal offences without a legal obligation to do so (for example, alcohol testing or requesting criminal records upon hiring). Likewise, the law does not regulate the surveillance (either video or of another type) in other areas.

Performance of a task carried out in the public interest

The GDPR Application Law defines the "performance of a task carried out in the public interest" as including "those activities of the political parties or of citizens' organizations belonging to national minorities and non-governmental organizations that serve the fulfilment of the objectives provided by constitutional law or public international law or the functioning of the democratic system, including the encouragement of citizens' participation in the decision-making process and the preparation of public policies , respectively promoting the principles and values of democracy". This definition is is at least questionable due to the very narrow scope of application and, at the same time, by its vague character, given the provisions of recital 45 GDPR:

"Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. (…) It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association".

It is at least surprising that for the Romanian legislature the public interest is exercised exclusively for a political-democratic purpose, but not also in the medical, social protection or other fields.

Derogations for political parties

Personal data from special categories can be processed by political parties, national minorities' organizations and non-governmental organizations without needing the data subject's consent, if: (a) certain safeguards are applied (information, transparency, respect for the right to rectification and erasure) and (b) the processing is done for reaching the organization's objectives.

Even if the law does not mention it, the GDPR clearly provides in Art. 9.2.d) that special categories of data can be processed by political parties and other non-profit organizations without the data subject consent only if the processing relates to its members or former members or to persons with whom it has regular contact, the processing is done connection with its purposes and the personal data are not disclosed to third parties without the consent of the data subjects. Consequently, the processing without consent is allowed only for those special categories of data which are relevant to that organization's purposes (e.g. party membership, in the case of political parties). GDPR preamble no. 56 provides that "Where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established." Moreover, the derogation allowed for political parties and NGOs is not a general one – these organizations must sill observe all other data protection rules provides in Art. 5 GDPR (information provision, purpose limitation, data minimization, accuracy, security, storage limitation, accountability).

Derogations for journalism and research

Data processing for journalistic purposes, academic, artistic or literal expression, as well as for scientific or historical research, for statistical or archiving purposes of public interest are exempted from the application of most certain GDPR provisions.

In the case of journalism, the GDPR Application Law removed the data processing from the application of most GDPR provisions (save for the sanctions), if the data processing (1) refers to personal data which has manifestly been made public by the data subject, or (2) the data is closely related to i. the quality of the data subject as a public person or ii. the public nature of the facts in which the data subject is involved. In practice, the derogation means that the persons who process data for journalistic activities (if they also meet the other legal conditions) are not held to comply with the data protection obligations, not even confidentiality or data security.

This provision, although based on a derogation allowed under Art. 85 GDPR, is questionable since the reason for which the regulation allows for derogations in

the case of journalistic activities is to ensure a balance between the right to data protection and the right to freedom of expression and information. In other words, derogations should apply only where these two fundamental rights cannot be reconciled – which involves the application of a balance test and the observance of the data protection obligations which remain compatible (e.g., data security measures or data integrity and confidentiality).

Certification bodies

The accreditation of the certification bodies referred to in art. 43 GDPR will be performed by the Romanian Accreditation Association - RENAR, as a national accreditation body. Certification bodies shall be accredited according to applicable legal regulations in accordance with EN-ISO / IEC 17065 and with the additional requirements established by ANSPDCP, as well as with the provisions of Art. 43 GDPR.

Sanctioning of public authorities and bodies

The GDPR Application Law establishes a differentiated sanctions regime between public authorities and bodies and the rest of the entities. More specifically, while the general rule provided by GDPR in Art. 58(2) is that the supervisory authority may order any of a series of measures, including a fine that may reach a maximum of EUR 10 million or 2% of the turnover, or EUR 20 million or 4% of the turnover, depending on the violation, the GDPR Application Law provides for a very different regime for public authorities in Romania.

More specifically, irrespective of the seriousness of the violation in question, the supervisory authority will always issue a warning and will attach a remediation plan drafted in accordance with the annex included in the GDPR Application Law.

The law does not provide for a maximum deadline for remediation, leaving this issue to the discretion of the authority, as well as the "possibility", not the obligation, to resume the control when the deadline expires. It is only if the control is reinstated and it is found that the controlled entity has not fully implemented the measures set out in the remedial plan, that the supervisory authority may apply a fine based on two tiers:

fine from 10,000 lei to 100,000 lei	**fine from 10,000 lei to 200,000 lei**
• Art. 8, art. 11, art. 25-39, art. 42 and 43 GDPR; • Art. 42 and 43 GDPR; • Art. 41 par. (4) GDPR; • Art. 3-9 of the GDPR Application Law.	• art. 5-7 and art. 9 GDPR; • art. 12-22 GDPR; • art. 44-49 GDPR; • Chapter IX GDPR; • art. 58(1) and (2) GDPR.

In other words, although a remedy period was available and yet the violation was not remedied, a public authority may receive a maximum fine of 200,000 lei (approx. 43,000 EUR), while for the same violation a private entity risks a maximum fine of 20 million EURO or 4% of the global turnover in the previous year, with no grace period.

It must be said, however, that this differential treatment originates in the GDPR provisions, namely art. 83 par. (7) which states that *"each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State"*.

Some issues not covered by the GDPR Application Law

First of all, the GDPR Application Law does not contain any provision regarding the age of the children under which controllers offering information society services need the consent of parents / tutors for data processing, as provided for in art. 8 GDPR. This means that in Romania the rule provided by art. 8 (1) GDPR shall be applicable, i.e. **if the information society service is offered to a child and the child is under 16, the data processing requires consent from the holder of parental responsibility**.

Another unregulated issue is the exercise of class actions according to art. 80 (2) GDPR, which means that **class actions will not be possible in Romania**.

As regards the representation of data subjects in accordance with Art. 80 (1) GDPR, the only relevant provision is found in Law 129/2018, which in the context of the modification of art. 14^7 of the organisation law of ANSPDCP provides the conditions for proving the mandate by the organization that ensures representation.

Change of the ANSPDCP organization law

The law amending and supplementing the law on the organization and operation of ANSPDCP (Law 129/2018 amending Law 102/2005 on the establishment, organization and functioning of ANSPDCP, published in Official Gazette no. 503 of 19 June 2018) was adopted on 15 June 2018 as part of the data protection legislative changes in Romania.

Law 129/2018 introduces a new chapter on the ANSPDCP investigations and settlement of complaints. ANSPDCP has the powers to carry out on-site unannounced investigations, and the persons under investigation must provide the

necessary information and documents. If the investigators are prevented from exercising their duties, ANSPDCP may obtain a request for authorization from the Bucharest Court of Appeal. The investigation carried out by ANSPDCP may not begin before 8:00 a.m. and may not continue after 18:00 p.m. (without the written consent of the person investigated) and must be performed in the presence of the investigated person or his/her representative.

Model of reporting security incidents

The GDPR requires the recording data breaches in all cases and to notify such breaches within 72 hours to the supervisory authority if these are likely to result in a risk to the rights and freedoms of natural persons.

ANSPDCP adopted the template *Report of data breaches for personal data controllers* which should be sent to ANSPDCP in case of security incidents, in the situations provided for under the GDPR (ANSPDCP Decision no. 128/2018, published in Official Journal no. 557 of 3 July 2018).

The form is available on the website of ANSPDCP (direct download): http://dataprotection.ro/servlet/ViewDocument?id=1488

This material is only for information purposes and may not be deemed or used as legal advice.

For more details relating to the topics included in this material, the contact persons are:

Andreea Lisievici, Partner (andreea@privacyone.ro)
Dana Ududec, Associate (dana.ududec@privacyone.ro)

47 Aviatorilor Blvd., 2nd floor,
Sector 1, Bucharest

contact@privacyone.ro

www.privacyone.ro