Romania's GDPR implementation law: A few national specifics

The new law is now in force. **Andreea Lisievici** and **Dana Ududec** of PrivacyOne explain how Romania has implemented the derogations allowed by the GDPR in national law.

In June, the Romanian Parliament adopted Law no. 190/2018 which provides measures for the implementation of the GDPR (the Romanian GDPR Implementation Law). The law, which entered into force on 31 July 2018 includes, among other measures, special rules for regulating workplace surveillance, implementation of the journalistic exemption, additional guidelines for appointing a data protection officer (DPO), rules for certification authorities, as well as further provisions on sanctions.

However, certain issues where the GDPR offered Member States some leeway for local regulation have not been approached by the Romanian law. For instance, the age of consent for minors in the context of the information society services (Article 8 GDPR) has not been lowered, and there are no provisions for instituting a "class action" in Romania (Article 80(2) GDPR).

This article highlights some aspects of Romania's GDPR Implementation Law, including analysis of requirements which are unclear or appear to go against the spirit of the GDPR[1].

Genetic, biometric and health-related data

The automated decision-making processes or profiling which uses genetic, biometric or health-related data may only be carried out when based on the consent of the data subjects or if there is a specific legal ground for the processing. Processing of these categories of data that does not include automated decision-making or profiling is not restricted. Therefore, in those respects, all grounds provided by Article 9.2 GDPR are applicable.

National identification number

The conditions for the processing of the national identification number (the Personal Numeric Code or CNP in Romania) are loosened compared to the previous legal regime – it is no longer required to base the processing solely on a legal obligation, consent or the authorisation issued by the Romanian Supervisory Authority (ANSPDCP). Thus, the NIN 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:

1. Implementation of technical measures to comply with the data minimization principle and ensure security measures;
2. Appointment of a data protection officer (DPO)[2];
3. Defining data storage timescales; and
4. 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 through electronic means of communication or video surveillance must comply with the following rules:

1. Thoroughly justify the legitimate interests sought and check that they prevail over the rights and freedoms of the data subjects (Note: meaning that it is necessary to perform a balancing test, and also to document such a test in order to demonstrate compliance);
2. Ensure the full, explicit and prior information to the employees (Note: information does not mean collecting consent, which is generally not required in employment relationships – however, employers must prove that they provided such information);
3. Consult in advance with the trade union or the employees' representative;
4. Apply other less intrusive means for fulfilling the purpose for which the monitoring is required and perform the monitoring only if such less severe measures were not efficient;
5. 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).

Although the title of this article in the Romanian law 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 surveillance (either video or of another type) in other areas.

The public interest

The Romanian GDPR Implementation 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 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 of the 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 surprising that the Romanian legislature considers public interest to be exercised exclusively for a political-democratic purpose, and thus excluding the medical, social protection or other fields.

Certification bodies

The accreditation of the certification bodies referred to in Article 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 Article 43 GDPR.

Sanctioning of public bodies

The Romanian GDPR Implementation Law establishes a differentiated sanctions regime between public authorities/bodies and other organisations. More specifically, while the general rule provided by GDPR in Article 58(2) is that the supervisory authority may order any of a series of measures, including a fine that may reach a maximum of €10 million or 2% of the turnover, or €20 million or 4% of the turnover, depending on the violation, the GDPR Implementation Law provides for a very different regime for public authorities and bodies 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 Romanian GDPR Implementation 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 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, depending on the substance of the violation (e.g. from approx. €2,000 to €20,000 for violations of Articles 8, 11, 25-39, 41(4), 42 and 43 of the GDPR and from approx. €20,000 to €43,000 for violations of Articles 5-7, 9, 12-22, 44-49, 58(1) and (2) and Chapter IX of the GDPR).

In other words, if a remedy period is available but the violation is not remedied, a public authority may receive a maximum fine of approx. €43,000, while for the same violation a private entity risks a maximum fine of €20 million 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 Article 83(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".

Issues not covered by the law

The GDPR Implementation Law does not deviate from the GDPR's provision regarding the age of the children under which controllers offering information society services need the consent of parents / guardians for data processing, as provided for in Article 8 GDPR. This means that Article 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.

Romania has not taken advantage of the provision for collective (class) actions according to Article 80(2) GDPR. As regards the representation of data subjects in accordance with Article 80(1) GDPR, the only relevant provision is found in the newly-modified law on the organization and operation of the ANSPDCP (Law No. 102/2005 as amended through Law No. 129/2018), which in art. 14^7 provides the conditions for a case being pursued by a representative organisation.

What is next?

After 25 May, and with the adoption of the Romanian GDPR Implementation Law, we have seen our clients shift from general "GDPR audit" efforts to more granular areas of work. Some of the hottest topics for GDPR compliance are workplace monitoring (where generally there are almost no labour sector-specific legal provisions), controller-processor vs. joint controllership determinations, and performing impact assessments and legitimate interest balancing tests for certain data processing operations. We believe that in the near future companies will continue with a more mature approach to their GDPR requirements.

On the other hand, the reality is that even though ANSPDCP was formally awarded a higher number of employees, we have not seen any actual measures to increase the previous headcount, thus leaving the authority seriously understaffed. It remains to be seen how the Romanian supervisory authority will exercise its powers if this situation does not change in the near future.

AUTHORS

Andreea Lisievici is a Partner and Dana Ududec an Associate at PrivacyOne, a boutique law firm established in Romania that specialises in data protection. Emails: andreea@privacyone.ro dana.ududec@privacyone.ro

REFERENCES

1 An unofficial English translation of law is available at https://www.privacyone.ro/files/Romanian%20GDPR%20implementation%20law%20-%20English%20translation.pdf

2 With regards to appointing a DPO, we have already seen in practice that this requirement is seen as being disproportionate. Some data controllers fear that even remote instances where a national identification number is processed based on legitimate interest (e.g. it is included in a contract document as part of the identification of the signatories) might trigger the obligation to appoint a DPO.

Join the Privacy Laws & Business community

Six issues published annually

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 100+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance.

Included in your subscription:

1. Online search functionality
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

2. Electronic Access
We will email you the PDF edition which you can also access via the *PL&B* website. You may also choose to receive one printed copy.

3. E-Mail Updates
E-mail updates help to keep you regularly informed of the latest developments in data protection and privacy issues worldwide.

4. Back Issues
Access all the *PL&B International Report* back issues since 1987.

5. Special Reports
Access *PL&B* special reports on Data Privacy Laws in 100+ countries and a book on Data Privacy Laws in the Asia-Pacific region.

6. Events Documentation
Access International and/or UK events documentation such as Roundtables with Data Protection Commissioners and *PL&B Annual International Conferences*, in July, in Cambridge, UK.

7. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of privacy legislation worldwide, and sources for specific issues and texts. This service does not offer legal advice or provide consultancy.

To Subscribe: www.privacylaws.com/subscribe

"*PL&B's International Report* is a powerhouse of information that provides relevant insight across a variety of jurisdictions in a timely manner. **Mark Keddie, Global Data Protection Officer, Dentsu Aegis Network**"

Subscription Fees

Single User Access

International Edition **£550 + VAT***

UK Edition **£440 + VAT***

UK & International Combined Edition **£880 + VAT***

* VAT only applies to UK based subscribers

Multi User Access

Discounts for 2-10 users. Enterprise licence for 11+ users.

Subscription Discounts

Introductory 50% discount. Use code HPSUB (first year only) for DPAs, public sector, charities, academic institutions and small and medium companies.

Discounts for 2 and 3 year subscriptions

International Postage (outside UK):

Individual International or UK Edition
Rest of Europe = £22, Outside Europe = £30

Combined International and UK Editions
Rest of Europe = £44, Outside Europe = £60

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

Privacy Laws & Business also publishes the United Kingdom Report.
www.privacylaws.com/UK