Bulletin of the *Transilvania* University of Braşov – Special Issue
Series VII: Social Sciences • Law • Vol. 11 (60) No. 2 - 2018

SOME ASPECTS OF THE ROMANIAN LAW ON IMPLEMENTING MEASURES FOR THE GENERAL DATA PROTECTION REGULATION

Elena-Nicoleta MIHĂILĂ[1]

Abstract: *This short article intends to examine some aspects of the Romanian law on implementing measures for the General Data Protection Regulation (GDPR), such as the processing of the national identification number, the personal data processing in the context of labour relations, the personal data processing for journalistic purposes or the purpose of academic artistic or literary expression, and, last but not least, the corrective measures and penalties for the infringement of the General Data Protection Regulation. Only time will tell if, in accordance with the specific nature of our national legal regime, the Romanian policy-maker was inspired as to the legislative solutions adopted for the application of the GDPR.*

Key words: *GDPR, national implementing measures, national identification number, labour relations, right to be digitally forgotten, corrective measures and penalties.*

1. Preliminary considerations

The General Data Protection Regulation (GDPR) lays down the obligation of Member States or allows them to adopt certain national rules for the application of this European regulation in accordance with the specific nature of the national legal regime. Thus, for the purposes of applying the rules of the Regulation, within the limits and in accordance with the provisions stating, on a punctual basis, the regulatory freedom of each Member State to adapt its rules on personal data processing to national realities and peculiarities, the Romanian legislator adopted the Law no. 190/2018 on implementing measures for the Regulation (EU) 2016/679.

Law no. 190/2018 sets out concrete measures designed to ensure the implementation in the national legal space of article 9 paragraph (4) on the processing of genetic data, biometric data or data concerning health, article 37-39 on the data protection officer, articles 42-43 on certification, art. 83 paragraph (7) on whether and to what extent administrative fines may be imposed on public authorities and bodies established in Member States, article 85 on processing and the freedom of expression and information, article 87 on processing of the national identification number, article 88 on

[1] Bucharest Bar – Romania, www.lawyersclass.ro, mihaila.nicoleta@gmail.com.

data processing in the context of employment and article 89 on safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

From the above we chose to present in this short article the aspects of national law concerning the processing of the national identification number, the personal data processing in the context of labour relations, the personal data processing for journalistic purposes or the purpose of academic artistic or literary expression, and, last but not least, the corrective measures and penalties for the infringement of the General Data Protection Regulation.

2. Processing a national identification number (art. 87 GDPR)

According to article 8 paragraph (7) of Directive 95/46/EC on the processing of special categories of data, the Member States could determine the conditions under which the national identification number or any other identifier of general application could be processed.

In this respect, the law transposing the Directive (Law no. 677 from 21st of November 2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data) stipulated in article 8 paragraph (1) that the processing of the personal identification number or of other personal data with a general identification function may be carried out only if the data subject has given an express and unequivocal consent, or the processing was expressly stated by a legal provision. As an exception, according to article 8 paragraph (2) of the transposition law, the national supervisory authority could establish other situations in which such data could be processed, but only after adequate safeguards have been provided in order to observe the data subject's rights.

Since in practice the collection and processing of the personal numeric code and other personal data having an identification function of general applicability was done without a thorough justification, the National Authority for the Supervision of Personal Data Processing issued a decision in order to clarify how to process this type of data, as well as the copies of the documents that contain them (Decision no. 132 from 20th of December 2011 of the National Authority for the Supervision of Personal Data Processing on the conditions for the processing of the personal numeric code and other personal data having an identification function of general applicability). This decision defined in article 1 paragraph (2) the notion of *personal data with a general identification function* as those numbers identifying a natural person in certain record systems and that are of general applicability, such as: the personal numeric code [article 1 paragraph (1) of the Decision no. 132/2011: "The Personal Numeric Code represents a significant number that uniquely individualizes a natural person, constituting an instrument for verifying the civil status and for identification by authorized persons in certain computer systems", series and identity card number, passport number, driving license, social or health insurance number. Also, the consent for the processing of this type of personal data should have been expressly provided in a form which allowed the controller to prove it (Şchiopu, 2017c, p. 85-91).

Under the General Data Protection Regulation, according to article 87, Member States are allowed to further determine the specific conditions for the processing of a national identification number or any other identifier of general application, establishing appropriate safeguards for the rights and freedoms of the data subjects pursuant to GDPR.

Given the possibility to detail the processing conditions, article 2 paragraph (1) letter b) of Law no. 190/2018 has taken over the definition of the national identification number from article 1 paragraph (2) of the Decision no. 132/2011 mentioned above, with the difference that instead of "social or health insurance number" now the definition refers to the "number of social health insurance".

Article 4 paragraph (1) of Law no. 190/2018 further states that the processing of a national identification number, including the collection or disclosure of documents containing it, may be carried out under the conditions laid down in article 6 paragraph (1) of the General Data Protection Regulation on the lawfulness of processing (for details, see Şandru, 2017, p. 129-135 and 2018, p. 39-48), the legal basis being one of the pillars of personal data processing (Şchiopu, 2017b, p. 97). When the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, article 4 paragraph (2) of Law no. 190/2018 provides that the processing can be carried out only with the establishment by the operator of a series of safeguards.

These safeguards shall include firstly the implementation of appropriate technical and organizational measures to respect in particular the principle of data minimisation and to ensure the security and confidentiality of personal data processing as referred to in article 32 GDPR. Secondly, it is necessary to appoint a Data Protection Officer, in accordance with article 10 of the Law no. 190/2018. Thirdly, the operator must set storage times according to the nature of the data and the purpose of the processing, as well as specific deadlines in which personal data must be erased or revised for erasure. The envisaged time limits for erasure of a national identification number or any other identifier of general application must be entered in the records of processing activities provided by article 30 paragraph (1) GDPR, the compliance with the obligation to keep track of personal data processing activities being a prerequisite for compliance and, at the same time, a proof of the controller's accountability (Şchiopu, 2018b, p. 94). The last safeguard concerns the periodic training, as to their obligations, of the persons processing personal data under the direct authority of the controller or the processor.

3. Personal data processing in the context of labour relations (art. 88 GDPR)

Another aspect in relation to which the national legislator may provide for more specific rules regards the protection of the rights and freedoms in respect to the processing of employees' personal data in the employment context. According to article 88 paragraph (2) GDPR, "those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place".

The Romanian legislator chose to provide specific rules on the monitoring of electronic communications and/or video surveillance systems at the workplace when the processing has as legal basis the legitimate interests pursued by the employer. Since the monitoring of electronic communications in the workplace (phone, internet browsing, email, instant messaging, VOIP, etc.) is considered the main threat to employees' privacy (Article 29 Data Protection Working Party, 2017, p. 12) and the processing operations using video monitoring systems can be disproportionate to the rights and freedoms of employees, and therefore, generally unlawful (Idem, p. 19), such processing can be carried out under legitimate interest only when five conditions are met cumulatively.

First of all, the legitimate interests pursued by the employer must be duly justified and prevail over the interests or rights and freedoms of the data subject. Secondly, the employer must have completed the mandatory, complete and explicit prior notification to employees. Thirdly, the employer must have consulted the trade union or, where appropriate, the employees' representatives before introducing the monitoring systems (but their approval is not required). The fourth condition requires that other less intrusive forms and ways to achieve the purpose pursued by the employer have not previously proved their effectiveness. The latter condition concerns the length of storage of personal data that must be proportionate to the purpose of the processing, but not more than 30 days, with the exception of situations expressly governed by law or duly justified cases.

However, the employers will have to take into account not only the provisions of the General Data Protection Regulation, but also article 8 of the European Convention on Human Rights (right to respect for private and family life, home and correspondence) and the relevant ECHR case-law (for monitoring of telephone and internet use: *Halford v. the United Kingdom* no. 20605/92, judgement of 25 June 1997; *Copland v. the United Kingdom* no. 62617/00, judgement of 3 April 2007; *Bărbulescu v. Romania* no. 61496/08, Grand Chamber judgement of 5 September 2017; for opening personal files stored on a professional computer: *Libert v. France* no. 588/13, judgement of 22 February 2018; for video surveillance: *Köpke v. Germany* no. 420/07, decision on the admissibility of 5 October 2010; *Antović and Mirković* v. Montenegro no. 70838/13, judgement of 28 November 2017) when deciding the introduction of a surveillance system at the workplace.

4. Personal data processing for journalistic purposes or the purpose of academic artistic or literary expression (art. 85 GDPR)

Recital (153) states that "Member States law should reconcile the rules governing freedom of expression and information, including journalistic, academic, artistic and or literary expression with the right to the protection of personal data pursuant to this Regulation. *The processing of personal data solely for journalistic purposes, or for the purposes of academic, artistic or literary expression should be subject to derogations or exemptions from certain provisions of this Regulation if necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information* [emphasis added], as enshrined in Article 11 of the Charter". Equally, Recital

(4) GDPR provides that „The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality".

To that effect, article 85 paragraph (2) GDPR provides that for processing carried out for journalistic purposes or for the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from chapter II-VII and IX "if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information".

Our legislator considered that, in order to ensure a balance between the right to protection of personal data, on the one hand, and the freedom of expression and the right to information, on the other hand, the processing can be performed by way of derogation from the chapters mentioned above only if the processing concerns personal data that have been made public by the data subject in a manifest manner or data which are closely linked to the data subject's status of public person or to the public character of the facts in which the data subject is involved.

Therefore, in the three hypotheses mentioned above (data made public by the data subject, data which is closely linked to the data subject's status of public person and data which is closely related to the public character of the facts in which the data subject is involved), when the data is processed for journalistic purposes, the data subject will not be able to rely in relation to journalists on the right to be forgotten provided by article 17 GDPR due to the derogation introduced by article 7 of the Law no. 190/2018.

However, since the respective legal grounds of original publishers (journalists) and search engines are different (the search engine has its own legal ground, which derives from its own economic interest and that of the users to have access to the information via the search engines and using a name as terms of search – Article 29 Data Protection Working Party, 2014, p. 6), the data subject, even in the three hypotheses, will still be able to rely on the right to be *digitally* forgotten (right to de-referencing) given that "the universal diffusion and accessibility of that information by a search engine, together with other data related to the same individual, can be unlawful due to the disproportionate impact on privacy" (Ibidem).

The effectiveness of the right to be forgotten in the online environment was somewhat strengthened as a result of the actions taken by the French data protection authority (Şchiopu, 2017a, p. 202), but none of the possible approaches to the implementation of the right to de-referencing seems to be appropriate for all cases in which the data subjects wish to rely on the right to digital oblivion (Şchiopu, 2018a, p. 72).

5. Corrective measures and penalties (art. 83 GDPR)

Recital (148) states that "In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement [emphasis added] of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation". To that effect, the initial version of the Law on implementing measures for

the General Data Protection Regulation provided in article 12 paragraph (1) that, in the case of the application of sanctions to public authorities and bodies, depending on the circumstances of each case, the supervisory authority may impose a reprimand or a fine. This legislative solution was described in the Explanatory Memorandum to the Bill on implementing measures for Regulation (EU) 2016/679.

Article 2 paragraph (1) letter a) of the Law no. 190/2018 defines the public authorities and bodies as the Chamber of Deputies and the Senate, the Presidential Administration, the Government, the ministries, the other specialized bodies of the central public administration, the autonomous public authorities and institutions, the county and local public administration authorities, other public authorities, as well as the subordinated or coordinated institutions. Also, for the purposes of this law, cult units, associations and public utility foundations are assimilated to public authorities and bodies.

The legislative initiators considered that, in relation to the nature of the data processed, it is undeniable that the breach of data protection rules in the case of special data processing, such as health data, by a public entity, presents a high degree of social danger and may lead to serious violations of the data subject's rights and considerable damage, both material and moral. Therefore, the absence of a penalty with a fine in the public sphere would encourage the violation of the rights or interests of the data subjects who are in a position of inequality with respect to the respective public institution or authority. Thus, the activities of the latter are subject to higher requirements than those concerning the behaviour of a natural person, for whom they must show and exercise greater diligence in relation to the data subjects, especially in respecting the fundamental right guaranteed by article 26 of the Constitution (right to intimate, family and private life), as well as the articles 7 (respect for private and family life) and article 8 (protection of personal data) from the Charter of fundamental rights of the European Union [The Explanatory Memorandum to the Bill on implementing measures for Regulation (EU) 2016/679, p. 6].

Despite the Explanatory Memorandum, since article 83 paragraph (7) GDPR allows any Member State to lay down rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State, the bill was later modified so as public authorities and bodies cannot be directly fined at the moment of the finding of the contravention, irrespective of the nature, gravity and duration of the infringement and of its consequences. To that effect article 13 paragraph (1) of the Law no. 190/2018 provides that, in the event of finding an infringement of the General Data Protection Regulation or of the Law no. 190/2018 by the authorities or public bodies, the national supervisory authority concludes a report on the finding and sanctioning of the contravention by which it applies the sanction of the reprimand and to which it attaches a remedial plan.

The remedial period will be determined in relation to the risks associated with the processing and the steps to be taken to ensure the conformity of the processing. The remedial period is defined by article 2 paragraph (1) letter e) of the Law no. 190/2018 as a period of time of no more than 90 days from the date of communication of the report of finding and sanctioning the contravention, during which the public authority or body has the possibility to remedy the found irregularities and to fulfil its legal obligations.

After 10 days from the deadline the National Supervisory Authority can resume the control. If the control reveals that the public authority or body has not fully implemented the measures set out in the remedial plan, the National Supervisory Authority, depending on the circumstances of each case, may impose a contraventional fine. Therefore, although the data subjects are usually in a position of inequality with respect to the public institutions or authorities, and irrespective of the nature, gravity and duration of the infringement and of its consequences, the public authorities and bodies cannot be directly fined. Consequently, this lack of direct sanction most probably will not enhance the legal and practical certainty for natural persons as to the processing of their personal data by the public authorities and bodies as recital (7) would have wanted.

6. Instead of a conclusion

Only time will tell if, in accordance with the specific nature of our national legal regime, the Romanian policy-maker was inspired as to the legislative solutions adopted for the application of the General Data Protection Regulation, especially as regards the corrective measures and penalties that can be applied to public authorities and bodies. In the meantime we hope that the courts will apply the data protection legislation taking into account not only the letter of the Romanian law on implementing measures for Regulation (EU) 2016/679 but also its European spirit.

References

Șandru, D.-M. (2017). Elemente privind reglementarea consimțământului în prelucrarea datelor cu caracter personal, potrivit art. 6 din Regulamentul nr. 2016/679 [Elements concerning the regulation of the consent in the processing of personal data, in accordance with Article 6 of Regulation (EEC) No 2016/679]. *Revista română de drept al afacerilor*, No.*5*.

Șandru, D.-M. (2018). Situații în care este permisă prelucrarea datelor cu caracter personal fără consimțământul persoanei vizate [Situations in which the processing of personal data is allowed without the consent of the data subject]. In A. Săvescu (coord.), *RGPD – Regulamentul general privind protecția datelor cu caracter personal: comentarii și explicații*. Bucharest: Hamangiu.

Şchiopu, S.-D. (2017a). Efectivitatea dreptului de a fi uitat [The effectiveness of the right to be forgotten]. In I. Alexe, N.-D. Ploeșteanu, D.-M. Șandru (eds.), *Protecţia datelor cu caracter personal. Impactul protecţiei datelor personale asupra mediului de afaceri. Evaluări ale experienţelor româneşti şi noile provocări ale Regulamentului (UE) 2016/679*. Bucharest: Universitară.

Şchiopu, S.-D. (2017b). Pilonii prelucrării datelor cu caracter personal [The pillars of personal data processing]. *Revista Universul Juridic*, No.*6*.

Şchiopu, S.-D. (2017c). Prelucrarea unor categorii speciale de date cu caracter personal: codul numeric personal sau orice alt identificator cu aplicabilitate generală [The processing of special categories of personal data: national identification number or any other identifier of general application]. *Revista Universul Juridic*, No. *8*.

Şchiopu, S.-D. (2018a). Aplicarea teritorială a dreptului la uitare digitală (dreptul la înlăturare) în lumina cererii de decizie preliminară introdusă de Conseil d'État (Franța) la 21 august 2017 - Google Inc./CNIL (Cauza C-507/17) [The territorial scope of the right to be forgotten (right to de-referencing) in the light of the request for a preliminary ruling from the Conseil d'État (France) lodged on 21 August 2017 — Google Inc. v CNIL (Case C-507/17)]. *Pandectele române*, No.*1*.

Şchiopu, S.-D. (2018b). Obligația de păstrare a evidenței activităților de prelucrare a datelor cu caracter personal [The obligation to keep a record of processing activities for personal data]. *Revista română de drept al afacerilor*, No.*1*.

⁂ *Directive 95/46/EC* of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, published in the Official Journal of the European Communities L 281 from 23rd of November 1995.

⁂ *Decision no. 132 from 20th of December 2011* of the National Authority for the Supervision of Personal Data Processing on the conditions for the processing of the personal numeric code and other personal data having an identification function of general applicability, published in The Official Journal of Romania, Part I, no. 929 from 28th December 2011.

⁂ *Law no. 677 from 21st of November 2001* on the protection of individuals with regard to the processing of personal data and the free movement of such data, published in The Official Journal of Romania, Part I, no. 790 from 12th of December 2001.

⁂ *Law no. 190 from 18th of July 2018* on implementing measures for Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation), published in The Official Journal of Romania, Part I, no. 651 from 26th of July 2018.

⁂ *Regulation (EU) 2016/679* of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation), published in the Official Journal of the European Union L 119 from 4th of May 2016.

⁂ *The Explanatory Memorandum to the Bill on implementing measures for Regulation (EU) 2016/679* […]. Retrieved from http://www.cdep.ro/proiecte/2018/100/60/7/em219.pdf.

⁂ *Guidelines on the implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*, WP 225, adopted on 26 November 2014. Retrieved from http://ec.europa.eu/justice/ article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf. Accessed on 15.09.2018

⁂ *Opinion 2/2017 on data processing at work, WP249*, adopted on 8 June 2017. Retrieved from http://ec.europa.eu/newsroom/ document.cfm?doc_id=45631. Accessed on 03.10.2018.