RedFame

International Journal of Law and Public Administration
Vol. 3, No. 1; June 2020
ISSN 2576-2192 E-ISSN 2576-2184
Published by Redfame Publishing
URL: http://ijlpa.redfame.com

How Has the General Data Protection Regulation Changed the Routine of a Public Authority in Romania?

Kajcsa Andrea

Correspondence: Kajcsa Andrea, Faculty of Economics and Law, Department of Law and Public Administration, University of Medicine, Pharmacy, Sciences and Technology "G.E. Palade" of Târgu-Mureș, Romania.

Received: December 6, 2019 Accepted: February 10, 2020 Online Published: February 12, 2020

doi:10.11114/ijlpa.v3i1.4643 URL: https://doi.org/10.11114/ijlpa.v3i1.4643

Abstract

The changes that have been brought about by the General Data Protection Regulation starting with May 2018 are complex and ambitious. The General Data Protection Regulation is one of the most wide ranging pieces of legislation passed by the EU in recent years, and it introduces many concepts that are yet to be fully discovered in practice, such as the right to be forgotten, data portability and data breach notification. This paper intends to analyze the main obligations that public bodies, particularly, have after the GDPR has entered into force, and to evaluate the impact this legislative act has on the routine activities carried out by public authorities in Romania. To reach our goal, we will make reference to the obligations that are specific to public administration authorities as well as to those that public bodies are exempted from. We will also analyze the national legislative measures adopted in Romania after GDPR started to be in force, and the degree to which these have particularized the way public bodies are allowed and obliged to process personal data in Romania.

Keywords: personal data, public authority, General Data Protection Regulation, technology

1. Introduction.

It is uncontested that the public sector has reached a point in time and evolution when it encompasses a wide range of services and enterprises, all having various natures, thus leading to a great amount of personal data processed. Personal data refers to anything that identifies a person, including: name, date of birth, home address, racial or ethnic origin, religious belief, health conditions, level of education, family members, income level, photographs etc. It is clear then that public authorities often deal with very delicate personal data, making it all the more critical that personal information is kept secure and processed in such a manner that the right to private life is complied with (Ploesteanu, 2018) (Sava, 2018).

Recitals 6 of GDPR expressly cover the issue of the great degree in which technology has become intrinsically a part of every single aspect of our lives, the administrative part of it not being exempted: "*Rapid technological developments and globalization have brought new challenges for the protection of personal data. (...) Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities.*" If we were to take a look at law through the lenses of its extra-legal sources, science and technology have been perhaps the strongest extra-legal sources of law in the last decades. The radical and extremely rapid evolution of technology, besides the undisputed advantages and benefits brought to the administration, to business environment, to law and to scientific research, raises a series of social, economic and legal issues. (Kajcsa, 2018) It is of great importance that modern technologies are not allowed to objectify the human or to harm in any way the right to private life, and law provides one strong path towards this goal.

In this context, the entering into force of the General Data Protection Regulation (EU) 2016/679 was a huge step forward, the role of law being to ensure that breakthroughs in science are properly applied to social relations. (Zanfir, 2014) After many years of debates, the EU Parliament has approved, on the 14th of April 2016, the General Data Protection Regulation, setting the enforcement day for 25th of May 2018, almost two years ago. The EU General Data Protection Regulation (GDPR) replaced the Data Protection Directive 95/46/EC and was designed, according to the official standing of European bodies, to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations approach data privacy. For sure, the GDPR developed and increased the obligations of data controllers set out through previous European and national legislation. It also introduced some completely new standards and individual rights which required all processors to re-assess how they process data and most probably improve the already existing safeguards for processing personal data.

Being a Regulation, the GDPR became directly effective in Member States without the need for implementing through further national legislation. However, throughout its provisions, the GDPR does allow/impose Member States to legislate on data protection matters, meaning that national legislation has most likely been adopted by all Member States, even if not necessarily (Commission, 2019), to implement the European legislative act and to create the framework for its application and compliance. For example, the GDPR allows Member States to legislate at national level on matters such as: the processing of personal data is required to comply with a legal obligation, the processing relates to a public interest task or is carried out by a body with official authority. Numerous articles also state that their provisions may be further specified or restricted by Member State law, as is the case of article 90 that allows Member States to adopt specific rules to set out the powers of the supervisory authorities in relation to controllers or processors that are subject to an obligation of professional secrecy or other equivalent obligations of secrecy.

2. Obligations Set by the GDPR Specific to Public Administration Authorities

GDPR includes terms and obligations specifically concerning public authorities and public bodies. Certainly, the GDPR does not address the public authorities or bodies in particular. However, public authorities handle personal data in their day-to-day activities, and thus are, in terms of GDPR, controllers. The processing carried out by public authorities will frequently involve sensitive (or special category) personal data, to which even stricter rules apply. Public authorities also have all the responsibilities that are present in the private sector businesses: they are employers, they operate IT systems and engage in marketing (for administrative purposes but mostly for political ones), and thus need to pay extra attention to all the requirements imposed by GDPR.

2.1 The Obligation to Appoint a Data Protection Officer

Controllers and processors may decide to appoint a Data Protection Officer ("DPO"). However, this is mandatory for public sector bodies (art. 37 (1) GDPR), the nature of the data they process being irrelevant. The DPO is meant to facilitate and help the organization to comply with the provisions and requirements of the GDPR. In the context of our analysis, and from our practical experience dealing with local public bodies while the GDPR entered into force, we believe it is important to underline that DPOs are not personally responsible in case the public authority they are employed at is found non-compliant with the GDPR. The GDPR states clearly that it is the controller or the processor who has to ensure and to be able to demonstrate that the processing is performed in accordance with its provisions, stating at article 24: "*(1) Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary. (2) Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller."* Data protection compliance is a responsibility of the controller or the processor, thus of each public authority or public body, and not of the data protection officer itself.

Article 37 (5) of GDPR provides that "*The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfill the tasks referred to in Article 39*." Although the Regulation does not specifically outline particular qualities a DPO should have, the following are to be taken into consideration (WP29, 2017): knowledge of the activities carried out and services provided by the public body, in depth knowledge of the organization itself, a solid understanding of what personal data are and how the public body processes these, a good understanding of information systems and data security, a perfect understanding of administrative procedures and rules. Some of the core personal traits a DPO should have are integrity, ethics, an understanding of the spirit of the law, not merely the wording of the law. Given the great complexity of this job's requirements, we believe that a public employee with seniority would be best fitted, instead of a newly employed person. This way, the nominated DPO would stand a greater chance of gaining the respect of the entire staff of the public body in question as well as of the leaders of that authority, thus ensuring compliance more likely by using his/her personal qualities and prestige. Although, as already shown, the DPO is not personally responsible for non-compliance with the GDPR, he/she is however responsible for properly carrying out the professional duties, being thus, first of all, liable on disciplinarily grounds. Therefore, each public authority should develop, enforce and, of course, respect, internal procedures that gradually guide the DPO in his/her activity. The DPO should always be able to prove that the leaders of the public body were made aware of any potential GDPR non-compliance issues, or of any potential threats or good practices that should be implemented and that they decided otherwise than the DPO advised.

2.2 The Obligation to Identify the Proper Legal Basis for the Processing of Personal Data

GDPR changes the legal basis on which public authorities can process personal data in order to carry out their specific activities or services. The GDPR does no longer permit public authorities to use legitimate interest as legal grounds for

processing personal data. Article 6 (1) of GDPR establishes the situations in which the processing of personal data is lawful, providing at point f) the following grounds: "*processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child*", only to immediately after outline that "*Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks."* Recitals 47-50 add more detail on what may be considered a *"legitimate interest".* First, the European law-maker appreciated that it is the responsibility of the national legislator to provide by law the legal basis public authorities should use to process personal data and thus those legal basis should not apply to the processing done by public authorities in the performance of their tasks. Second, if the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Therefore, all public authorities should have, by this time, found and used another legal basis for the processing of personal data and stop relying on *"legitimate interests"*.

The most relevant lawful basis for public authorities is the one provided at Article 6 (1) point e): "*processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*". This basis is applicable when exercising official authority, such as a public body's tasks, duties, powers or when carrying out a specific task in the public interest, in both cases provided by the law, coupled with the demand that processing is 'necessary' for that particular purpose. Recitals 41 of GDPR bring clarifications, outlining that a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons that are subject to it, not restricting the scope to acts adopted by the Parliaments of EU member states. We can therefore conclude that this basis is materialized in statutory laws for the public administration, laws that provide common law tasks, functions or powers for public bodies, even if no reference is particularly made to the processing of personal data.

Article 6 further allows EU Member States to introduce specific provisions to provide a basis under Article 6(1)(e). In Romania, Law no. 190/2018 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) has been the legislative measure adopted shortly after the GDPR started to produce legal effects, and regulated some of the issues allowed by the GDPR to be regulated by national legislative bodies. In its introductory part, the law mentions that it establishes the measures necessary for the implementation, at national level, in particular, of the provisions of Article 6 (2), Article 9 (4), Articles 37-39, 42, 43, Article 83 (7), Article 85 and Articles 87-89 of Regulation 2016/679. Law no. 190/2018, in its article 2, deals with definitions and, at paragraph f), defines the phrase "performing a task that serves a public interest" as including those activities of political parties or citizens' organizations belonging to national minorities, non-governmental organizations that serve the fulfillment 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 the promotion of the principles and values of democracy. Although we would argue that this is not a definition, *per se*, but more likely an addition to a pre-existing notion, we consider such an inclusion made in our national legislation to be appropriate, given the importance of political parties and citizens' organizations in the mechanism of any democratic state.

Regarding the issue of processing personal data for the performance of a task carried out in the public interest, Law no. 190/2018 provides in its article 6 for a series of safeguards that must be met, cumulatively: the implementation of adequate technical and organizational measures for the observance of the principles mentioned in Article 5 of General Data Protection Regulation, in particular the one referring to data minimization, respectively the principle of integrity and confidentiality; the designation of a data protection officer; the establishment of retention periods 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 deletion. Of course, we can immediately conclude that none of these safeguards are new, and that all these measures are provided for by GDPR itself. However, we believe that since this legal basis concerns public authorities first of all, having these safeguards mandatory, as underlined through the provisions of the national law, compliance with the provisions of the GDPR and the processing of all personal data in a lawful manner becomes easier for public authorities in Romania.

It is important that public authorities understand whether processing is performed in relation to tasks carried out in the public interest, in the exercise of official authority, or for other purposes, as different rules apply. In day to day activities, this translates into the responsibility of public authorities in Romania to find the correct legal grounds to rely upon when processing data. All Romanian public authorities should, if they have not yet done this, review the processing activities they carry out and determine their lawful basis and, consequently, determine the applicable rules and safeguards, or whether a particular type of processing is exempted, or if a derogation applies. At the same time, it is just as important for

all organizations to keep in mind that, once compliant, a watchful eye should still be active, since changes occur constantly and adjustments could become needed.

2.3 The Obligation to Ensure Safeguards Exist If/When Dealing With (International) Data Transfers

Consent represents one of the legal grounds for processing personal data, grounds that present certain restrictions for the public sector. Recital 43 of GDPR indicates that it is unlikely for public authorities to use consent as a legal basis for processing personal data due to the issue of imbalance of powers, meaning that whenever the controller is a public authority, there is often an imbalance of power in the relationship between the controller and the subject/citizen. Since the GDPR requires that consent must be" freely given" (Article 4 of GDPR – Definitions, states: *'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*), the imbalance between the government and its citizens stands in the way of a true free given consent of the citizen. Although this possibility cannot be excluded for good, it is clear that public authorities can find other lawful bases, more appropriate to their specific nature, duties and activities.

The GDPR does allow, as a general rule, data transfers based on the consent of data subjects. However, since public bodies cannot rely on consent as basis for processing, public authorities can rarely use this exemption. The GDPR does provide that governmental bodies can exchange data with non EU countries without suitable safeguards (such as availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country), if there is a legally binding and enforceable instrument between the two states' government authorities. Recitals 108 mentions that transfers may also be carried out by public authorities or bodies with public authorities or bodies in third countries or with international organizations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding providing for enforceable and effective rights for data subjects.

3. Exceptions from GDPR the Public Authorities Are Subject to

Not all changes brought about by GDPR had an equal impact on organizations operating in the public area vs. organizations operating in the private one. The GDPR provides certain exceptions that are only applicable to public authorities and not to the private bodies. Moreover, several new obligations will have a smaller impact in the public sector compared to the private one, as we will show in the following paragraphs.

3.1 Right to Be Forgotten

According to article 17 of the GDPR "*the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay.*" Practically, this means that any person that has its personal data processed can request the organization that processes these data to delete any personal information about them. (Sandru, 2018) Individuals can request to have their personal data erased in certain situations, specified in the provisions of the GDPR, all of these situations referring to cases where the processing of those particular data does not meet the requirements of the GDPR. Individuals can exercise this right against controllers, who are obliged, under GDPR, to respond without delay.

The right to be forgotten will play a less relevant part in the public sector, compared to the private one, as a consequence of the grounds provided by the texts of the GDPR when the right to erasure does not apply. The right to erasure is not applicable if processing is necessary for the performance of a public interest task or exercise of official authority, or if the processing is executed for compliance with a Union or Member State legal obligation. It is clear that processing relying on the before mentioned legal grounds occur quite frequently within public sector organizations. So, all the more, as already mentioned before, it is paramount for public authorities to find the correct legal grounds to rely upon when processing data. If, however, the grounds that stand at the basis of their lawful processing of personal data are different, consent for example, this exemption is no longer applicable.

3.2 Data Portability

Data portability is one example of the new concepts that GDPR has introduced, compared to the previous European Directive in this matter, and, of course, a much debated new right that data subjects enjoy. (Graef, et al., 2018) This new right refers to the possibility of data subjects to recover their personal data in a machine readable format, in an electronic form that is commonly used. This new concept of data portability needs the support of controllers, since it requires these to provide the information they posses in a structured, commonly used and machine readable form so that the data subject may transfer it to another data controller.

Data portability is not, however, an absolute right of the data subject. The right to data portability applies in one of these two situations: the processing has been done based on consent or the performance of a contract or by automated means. The scope of the right to data portability is narrowed down to the data the subject itself has provided to the controller.

Thus, data portability is not applicable if the lawful basis for processing is represented by the performance of a public interest task or exercise of official authority and this is in fact the basis most commonly public authorities should rely on when processing personal data. Given that contractual relations are the exception in public law, in our case in administrative relations, the probability of data portability becoming applicable against a public body becomes significantly narrow. However, in such cases where contractual relations do rise between a public body/controller and a citizen/data subject, we believe it does not make any difference whether that contract is governed by public law or private law. The rules that govern these two types of contracts are fundamentally different (the equality of the parties, ways of closing such contracts, the degree in which the law regulates the specific clauses to be included in these contracts), but it makes no difference from the perspective of processing personal data. To conclude, since different grounds are used, as a common practice, for processing personal data by public authorities than the grounds private organizations have at their disposal, data portability will not weigh as much in the day-to-day activities of public organizations in Romania.

3.3 One-stop-shop

One of the new concepts introduced by the provisions of the GDPR refers to the so-called "one-shop-stop" mechanism. What does this mean? Given the typical nature of organizations that process personal data, this mechanism allows organizations that carry out operations European-wide to have to deal with merely one data protection supervisory authority of all the competent ones (from all EU states they have operations in). This supervisory authority is called the lead supervisory authority. Public authorities and bodies, by their very definition and nature operate in one country (the country that created the organization), and thus this possibility will not be applicable, as a general rule, in the public sector.

4. The Regime of Administrative Accountability of Public Authorities

In case of non-compliance, supervisory authorities have the power and prerogative to impose administrative fines on both data controllers and data processors. Article 83 of GDPR allows, however, EU members – states to determine the extent to which public authorities themselves should be subject to administrative fines. Law no. 190/2018 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 regulates this issue in articles 13 and 14. According to these legal provisions, in those cases when a public authority or body is found non-compliant with the provisions of the General Data Protection Regulation, the National Supervisory Authority will conclude a report to this end in which it will describe in what the non-compliance consists of and it will apply, in this first step of the procedure, the administrative sanction of reprimand.

To this report that is in fact an individual administrative act having mandatory force, the Authority will also attach a remedial plan that is determined by the risks found at the sanctioned public authority, containing the steps the authority in question needs to take in order to become compliant with the provisions of GDPR when processing personal data. The remedial plan is an annex to the report on the finding and sanctioning of the contravention that contains a series of remedial measures, which are nothing else but solutions ordered by the National Supervisory Authority, the only administrative authority specialized in personal data and their lawful processing, that need to be fulfilled by the sanctioned public authority. The remedial deadline is of no more than 90 days from the date the report is communicated, 90 days in which the public entity has the possibility to remedy the detected irregularities and become compliant.

The public authority bears the responsibility of carrying out all the measure contained in the remedial plan. The National Supervisory Authority has the possibility to resume control for the second time, 10 days before the remedial deadline expires. This means, *per a contrario*, that it also has the possibility not to resume control for the second time and allow a possible scenario of the same public entity being non-compliant further more. If however the National Supervisory Authority resumes control only to discover that the public entity did not entirely carry out the measures provided for in the remedial plan, it may, depending on the circumstances of each case, apply the administrative sanction of the fine, taking into account the criteria provided in Article 83 (2) of the General Data Protection Regulation.

Therefore, if at the end of the procedure presented above, the final result is that the public entity did not fully implement the measures provided for in the remedial plan, the supervisory authority can and will apply the sanction of the fine, varying from the minimum of 10.000 lei (approximately 2.100 euro) to the maximum of 200.000 lei (approximately 42.000 euro). Taking into considerations the amount of the fines provided by the GDPR itself, applicable as such to private organizations, and the ones regulated through the provisions of Law no. 190/2018, the sanctioning regime provided for public bodies seems to be discriminatory. (Alexe, 2018) However, this choice is not singular among EU member states: Czech Republic has set a maximum fine that can be imposed on public authorities in case of failure to comply of 358.000 euro, the maximum administrative fine for breach of the GDPR by public authorities and public bodies set in Ireland is 1.000.000, the Belgian legislative act states that the administrative fines of Article 83 GDPR cannot be imposed on public authorities, except when the latter is a public-law legal entity offering goods or services on a market, while the French Data Protection Act reiterates the penalties provided for in Article 83 of the GDPR, providing that these penalties do not

apply to processing done by the State. Moreover, as it has been pointed out (Boanta, 2019), there needs to be a better correlation between all the legislative acts in Romania that regulate the issue of the sanctioning regime in the area of personal data, namely between Law no. 102/2005 regarding the setting up, organization and functioning of the National Supervisory Authority for Personal Data Processing, G.O. no. 2/2001 on the general framework in matters of administrative offences, Law no. 190/2018 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 Decision no. 161/2018 on the approval of the procedure for conducting investigations.

5. Conclusions

The scholarly literature has analyzed the progress of implementing GDPR one year after entering into force and has pointed out the good and the improvable. The positive outcomes include increase in the citizens' awareness concerning data protection and users' rights and consequently an increase in the number of complaints and data breach notifications. The aspects that need improvement include the risk of legislative fragmentation and the slow resolution of complaints addressed by individuals. (Massé & Lemoine, 2019) (Commission, 2019). Scholarly literature has covered issues such as the impact of GDPR on journalistic news gathering, access to information and right to private life (Sanders, 2019) (Reventlow, 2020) but has paid little attention to its impact on public authorities. We must not forget, however, that this is partly natural given that, as already stated in the previous paragraphs, the GDPR is not designed for public authorities or bodies in particular, and thus the focus of researchers was mainly on private entities and the impact GDPR has on private organizations and their current way of doing business.

After establishing those obligations specific to public administration authorities as well as the exceptions public authorities are subject to, in the light of the provisions of the GDPR, we believe the following recommendations would help public authorities in Romania maintain a certain level of efficiency in carrying out day-to-day specific public tasks and activities while also complying with the provisions of GDPR.

First, all Romanian public authorities should analyze whether the data they hold are relevant or not. More often than any organization would be willing to admit, data bases are filled up with huge amounts of data that are either outdated or have become unnecessary or irrelevant. In this context, GDPR should be first of all seen as an opportunity to clear data systems of any irrelevant and old data. This is even more necessary for the public sector in Romania, where technology is often outdated, hard-wares and soft-wares being both not able to cope with the new requirements and safeguards that the lawfulness of processing data imposes on controllers.

Second, public bodies in Romania will need to ensure that proper data processing systems are in place to cope with the new rights of data subjects. This translates into more investments and public financial allocations in the technological area, but also into additional administrative work for all organizations within the public sector. For example, as we have already pointed out, the right to be forgotten is not applicable to public entities if it hinders the performance of a task carried out in the public interest of health or safety. However, GDPR allows individuals to have access to their personal data on request, and consequently all Romanian public entities must be prepared to comply with such requests in due time.

Third, Romanian public bodies must correctly identify all people within the organization that come in contact with personal data and ensure they are fully aware of their own personal responsibility in dealing with personal data. This implies well trained staff members, and consequently the appropriate budgeting policy, as well as clear internal operational procedures that guide employees step by step when dealing with personal data.

Final, public bodies in Romania need to make sure that the security of data is an ongoing concern and to this end will need to plan regular risk assessments to discover any risks and threats in their data processing activities. The need for compliance exists in both private and public sectors. And once compliant, there remains the ongoing management of all data processing activities, including regular risk assessments.

Public authorities in Romania must (re)place their focus on the data subject, and use this opportunity to tidy-up their data bases of old and unneeded information while keeping up with a digitalized society where citizens demand more and more secure and modern services. For sure, the standards imposed by the GDPR continue to represent a challenge and public authorities will need to consider the appropriate financial allocations in this regard, to improve technology used in their day-to-day agenda, the need to train all its staff members and have in place efficient internal operational procedures.

References

Alexe, I. (2018). Regimul sancţionator prevăzut de Regulamentul (UE) nr. 2016/679 privind protecţia datelor cu caracter personal.. *Curierul Judiciar, 1,* 36-42.

Boanta, A. (2019). The role of the national authority in protecting personal data. *The Juridical Current, 4,* 47-51.

Commission, E. (2019). *Data protection rules as a trust-enabler in the EU and beyond – taking stock,* Brussels: EU.

Graef, I., Husovec, M., & Purtova, N. (2018). Data Portability and Data Control: Lessons for an Emerging. *German Law Journal, 19*(6), 1359-1398. https://doi.org/10.1017/S2071832200023075

Kajcsa, A. (2018). Approaching Technology as a Material Souce of Law.. *The Juridical Current Journal, 4*, 55-62.

Liard, B., & Hainsdorf, C. (2019). *GDPR Guide to National Implementation. A practical guide to national GDPR compliance requirements across the EEA*, s.l.: s.n.

Massé, E., & Lemoine, L. (2019). *One Year under the Eu GDPR. An Implementation Progress Report*, s.l.: AccessNow.Org.

Ploesteanu, N.,(2018). *Protectia datelor cu caracter personal si viata privata – Jurisprudenta CEDO si CJUE*, Bucharest: Universul Juridic Publishing House.

Reventlow, N. J. (2020). Can the GDPR and Freedom of Expression Coexist?. *American Journal of International Law, 114*, 31-34. https://doi.org/10.1017/aju.2019.77

Sanders, A. K. (2019). The GDPR One Year Later: Protecting Privacy or Preventing Access to Information?. *Tulane Law Review, 93*(5), 26.

Sandru, M. (2018). Protecţia datelor în cadrul autorităţilor şi organismelor publice în România.. *Pandectele Romane., 2*, 11-19.

Sava, R. (2018). *Regulamentul General privind Protectia Datelor (GDPR) pe intelesul tau*, Bucharest: Universul Juridic Publishing House.

WP29 (2017). *Guidelines on Data Protection Officers ('DPOs'),* s.l.: s.n.

Zanfir, G. (2014). Regândirea dezvoltării în generaţii a reglementărilor privind protecţia datelor personale.. *Romanian European Law Journal., 1*, 56-72.