THE LEGAL REGIME OF THE PROCESSING OF PERSONAL DATA IN THE PUBLIC SECTOR, IN THE CONTEXT OF THE GENERAL DATA PROTECTION REGULATION

Ancuţa Gianina OPRE*
Simona ŞANDRU**

Abstract

As of the 25th of May 2018 a new regulation on data protection will directly apply in all European Union's Member States, that is the Regulation (EU) 2016/679. The current national legislation (Law 677/2001) will be replaced by these rules, so a new legal regime on the processing of personal data shall be established. Although in general, the same rules apply for both public and private data controllers (or data processors), there are a number of specific features for the processing carried out in the public sector in terms of legal duties and applicable exceptions. For instance, all the public institutions will have to appoint a data protection officer. However, the processing made by the courts when they are acting in their judicial capacity shall not be covered by some of the new legal norms. In the present paper, an overview of the new legal regime of data protection in the public sector will be outlined, in order to assess the most relevant novelties on the matter.

Keywords: *Data protection, new regulation, European Union law, public sector, data controller.*
JEL Classification *[K38]*

1. Introduction

The year 2018 will be marked by the important changes to be made in the personal data protection field, once the new European Regulation on Personal Data Protection[1] shall become applicable[2].

Although the general principles of the Directive 95/46/EC [3] remain applicable, new rules are established in order to enhance the data subjects' control

* Associate Professor, PhD., Faculty of Legal and Administrative Sciences, "Dimitrie Cantemir" Christian University Bucharest, National Authority for Surveying the Processing of Personal Data.

** PhD., National Authority for Surveying the Processing of Personal Data.

[1] 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) (Text with EEA relevance), OJ L 119, 4.May (2016), p. 1–88. For the purpose of the present study, we shall refer to it as the "Regulation" or "GDPR".

[2] See also Buttarelli (2016: 77–78).

over their personal data, on the one hand, and the responsibility on the part of data controllers and processors, on the other. The objective of the regulation is to consolidate the legal regime of the fundamental right to personal data protection facing the dynamic evolution of technology in the digital age, while also ensuring the free movement of information in the internal market, part of the present globalised world, but still embracing the European Union values.

The regulation shall be directly applicable in all Member States in a uniform way, starting 25 of May 2018. This is why there is no obligation (in fact, it is forbidden, with a few exceptions[4]), to implement its legal norms, except where the regulation imposes or allows the Member States to regulate by domestic pieces of legislation. From this point of view, the Regulation sets the same rules for both private and public data controllers and processors, but with a number of notable exceptions, as regards the public sector. Some particular features of the new legal regime on data protection, in the public sector, is strictly left to the Member States to be regulated, taking into account their sovereign right to manage internal matters.

Moreover, the Regulation has no overall applicability, as Art. 2 para. 2 excludes from its scope the processing of personal data which falls outside the scope of Union Law, the activities of the Member States related to the common foreign and security policy, the processing by a natural person in the course of a purely personal or household activity, the processing by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, and the processing of personal data by the Union institutions, bodies, offices and agencies (in this case, Regulation (EC) No 45/20015 will also be replaced by a new regulation, adapted to the GDPR). As concerns the criminal law matters, Directive (EU) 2016/680[6] has to be transposed by all the Member States until 6th of May 2018.

---

[3] 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 (OJ L 281, 23.11.1995, p. 31-50)

[4] For instance, in its preamble the Regulation states the following:
"(8) Where this Regulation provides for specifications or restrictions of its rules by Member State law, Member States may, as far as necessary for coherence and for making the national provisions comprehensible to the persons to whom they apply, incorporate elements of this Regulation into their national law."

[5] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December (2000) on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (O J L 008, 12 January 2001, p. 1-22).

[6] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal

The scope of our study will be restrained to the analysis of the distinct legal regime applicable to the public sector, as it results strictly from the Regulation, with special emphasis on the following issues: legal basis for data processing, data privacy impact assessment, data protection officer, competence of the data protection authority.

2. Public data controllers

As previously mentioned, the GDPR contains legal rules which are both applicable for the private and public sector, as concerns the subject of the legal obligations (data controllers and data processors). In this regard, a data controller is defined as ”the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law” (Art. 4 point 7). Also, the data processor means ”a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller” (Art. 4 point 8).

The Regulation does not contain a specific definition of the ”public authority” or ”agency”, as other European Union’s legal instruments[7] do, so their scope remains to be determined under the national law of each Member State. For instance, in Romania there are a number of laws which define a public authority for the specific purpose of that piece of regulations: Law 554/2004 on contentious administrative matters, Law 544/2001 on free access to public information, Law 500/2002 on public finances, Law 215/2001 on local public administration. Therefore, for the purpose of the implementation of GDPR in Romania, a distinct legal definition of the ”public authority/ agency/body” is needed, in order to have a clear delimitation of the legal

offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89–131).

[7] For the purpose of the Directive 2003/98/EC of the European Parliament and of the Council of 17 November (2003) on the re-use of public sector information (O J L 345 , 31.12.2003, p. 90 – 96), the following definitions shall apply:

1. ”public sector body” means the State, regional or local authorities, bodies governed by public law and associations formed by one or several such authorities or one or several such bodies governed by public law.

2. ”body governed by public law” means any body:

(a) established for the specific purpose of meeting needs in the general interest, not having an industrial or commercial character; and

(b) having legal personality; and

(c) financed, for the most part by the State, or regional or local authorities, or other bodies governed by public law; or subject to management supervision by those bodies; or having an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional or local authorities or by other bodies governed by public law”.

obligations imposed to this category of data controllers and processors. The definition might have as a starting point the constitutional provisions on the public authorities, taking into account the organisation of the State power. The special legal norms on the structure and organization of the public administration are to be considered, as well.

An example on that matter could be the German law. Thus, the national law implementing the Regulation and transposing the Directive (EU) 2016/680[8] defines the public bodies of the Federation and of the *Länder*[9] from the first articles of the law.As for the territorial scope, it has to be mentioned that the Regulation shall also be applicable outside the European Union borders, whenever the international law is enforceable. This is the case of the diplomatic missions and consular offices of the Member States which process personal data during their ordinary activity abroad.

So, a general remark may be drawn up: unless their activity falls outside the material scope of the Regulation, as stated above, all the public authorities are in principle subject to the obligation to respect and implement the new rules on data protection. This process started (for the private data controllers and processors, too) two years ago, as the GDPR came into force on 24th of May 2016 and established a two years interval in order to allow all the interested actors to adapt their procedures and/or norms to the future legal framework.

However, one single public authority may be facing two separate legal regimes, whenever it processes a set of personal data for a prosecution purpose

[8]Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 (DSAnpUG-EU) of 30 June (2017).

[9] "Section 2 Definitions.

(1) Public bodies of the Federation are the authorities, judicial bodies and other public law institutions of the Federation, of direct federal corporations, statutory bodies and foundations established under public law and of their associations irrespective of their legal form.

(2) Public bodies of the Länder are the authorities, judicial bodies and other public law institutions of a Land, a municipality, an association of municipalities or of other legal persons under public law subject to Land supervision and of their associations irrespective of their legal form.

(3) Associations of public bodies of the Federation and the Länder which are established under private law and perform tasks of public administration shall be regarded as public bodies of the Federation irrespective of the participation of private bodies if

1. they operate beyond the borders of a Land, or

2 The Federation holds the absolute majority of shares or controls the absolute majority of votes.

Otherwise they shall be regarded as public bodies of the Länder.

(4) Private bodies are natural and legal persons, societies and other associations established under private law unless they are covered by subsections 1 to 3. If a private body performs sovereign tasks of the public administration, it shall be a public body as defined in this Act.

(5) Public bodies of the Federation shall be regarded as private bodies as defined in this Act if they take part in competition as enterprises governed by public law. Public bodies of the Länder shall also be regarded as private bodies as defined in this Act if they take part in competition as enterprises governed by public law and carry out federal law, and if data protection is not governed by Land law."

(that is under Directive (EU) 2016/680) and some other sets of personal data for administrative purposes (for instance, in accordance with staff and fiscal regulations, which shall fall within the GDPR scope).

3. Legal basis for data processing

Art. 6 of GDPR establish the legal ground for the processing of (ordinary) personal data and Art. 9 set distinct rules for the processing of sensitive data[10].

As for the public data controllers, they may ground their processing on all the provisions of Art. 6 para. 1, except for the legitimate interest which is now (Directive 95/46/EC did not rule out this possibility) expressly forbidden for the public authorities when performing their tasks. Probably, the most common basis to rely on shall be the compliance with a legal obligation and the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (letters c) and e) of Art. 6 para. 1). For those two cases, the Regulation allows Member States to further maintain or introduce more specific provisions to adapt the application of the rules of this Regulation by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing. In any case, the legal basis, laid down by the European Union law or Member State law has to comply with the conditions provided by the GDPR, in the terms of setting the purpose of the processing and in addition a few other elements, such as: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations (such as freedom of expression, free access to information, employment, identification number, public archiving, scientific activities, religious associations); the law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

As for the sensitive data, a public data controller can rely its processing on one or several of the legal basis cited by Art. 9 para. 1 letters a)-j). Some of these legal bases seem to be construed in particular for the situations of processing made by a data controller from the public sector, such as in cases of preventive medicine, public health or the management of health or social care systems and services. In this context, the preamble gives the following example: ”Some types of processing may serve both important grounds of

[10] Sensitive data are considered as being personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. The processing of these data is in principle prohibited.

public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters."

Another case concerns the processing of personal data relating to criminal convictions and offences or related security measures that shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Moreover, any comprehensive register of criminal convictions shall be kept only under the control of official authority, according to Art. 10 of the GDPR.

4. Data privacy impact assessment

One of the novelties of the GDPR refers to a new obligation imposed on data controllers, to carry out a data privacy impact assessment (DPIA), before starting a data processing, whenever it is about a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons[11]. Whenever the controller considers that, after making this evaluation, the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, the competent supervisory authority will be consulted (for residual risks). The Regulation provides in Art. 35 a few examples of cases when a DPIA is mandatory: a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; processing on a large scale of sensitive data or of personal data relating to criminal convictions and offences; a systematic monitoring of a publicly accessible area on a large scale.

However, a complete and public list of the processing operations requiring a DPIA is to be established by the national data protection authorities, in close co-operation with each other, under the "umbrella" of the European Data Protection Board (this is a new European Union body that will come into existence after 25th of May 2018, by replacing the current Article 29 Working Party - WP Art. 29, comprised of the representatives of the national data protection authorities). The criteria to be taken into account when creating those lists are already set up in a guideline on this matter[12], issued by the WP Art. 29.

[11] See also "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679", WP 248 rev.01, adopted by the Article 29 Working Party, on 4 April (2017), as last revised and adopted on 4 October 2017, available at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 (last accessed on 8 March 2018).

[12] The above mentioned Guidelines (footnote 12).

As for the public data controllers, in their most frequent activities involving the processing of personal data, they exercise their competence already established by law. In these cases, if a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, there is no need to make a DPIA, unless provided so by the national law of a Member State. In their common guidelines, the supervisory authorities recommended as a good practice to publish a DPIA where members of the public are affected by the processing operation, especially when a public authority has been carried a DPIA.

5. Data subjects' rights

In general, all the rights provided by the GDPR have to be respected by the data controllers, regardless of their nature, whether private or public. So, the obligation to comply with the rules related to the right to information (Art. 13 and 14), the right of access to data (Art. 15), the right to rectification (Art. 16), the right to erasure (Art. 17 and 19), the right to restriction (Art. 18 and 19), the right to data portability (Art. 20), the right to object (Art. 21), the right not to be subject to a decision based solely on automated processing, including profiling (Art. 21) and to the general conditions for transparency and exercise of those rights (Art. 12) is also incumbent upon the public data controllers.

However, a few considerations need to be made, when it comes about the exceptions provided for by the GDPR, in case of some of these rights.

Thus, a data controller does not have to comply with the obligation to inform data subjects where personal data have not been obtained from the data subject, when obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests or the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

As for the right to erasure or the "right to be forgotten"[13] a data controller shall not be compelled to delete data if these are processed for the compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. A second exception regards the processing of personal data for reasons of public interest in the area of public health, especially when it comes about the processing of sensitive data in preventive medicine, for the provision of health or social care or treatment or the management of health or social care systems and services (these are just a few examples).

Where processing of data has been restricted, following a data subject request (based on the right to restriction), such personal data shall, with the

[13] Before GDPR, the European Court of Justice already recognised this right, based on the Directive 95/46/EC provisions, in the Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González EU:C:2014:317.

exception of storage, only be processed for a few limited reasons, among them being also an important public interest of the Union or of a Member State.

The right to data portability is also a new right introduced by the GDPR (as the right to be forgotten[14] and the right to restriction) in order to confer more control of the data subjects over their personal data, by making available to them data in a structured, commonly used and machine-readable format. However, this right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. On the other hand, in their common guidelines[15], the supervisory authorities recommended as a good practice" to develop processes to automatically answer portability requests, by following the principles governing the right to data portability. An example of this would be a government service providing easy downloading of past personal income tax filings".

Where a data subject exercises the right to object, on grounds relating to his or her particular situation, to processing of personal data concerning him or her which is based on the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or on a legitimate interest pursued by the controller or by a third party, the controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims. In the particular situation of the processing for scientific or historical research purposes or statistical purposes the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

As regards the right of a data subject not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her[16], one of the applicable exceptions is related to the case when the respective decision is authorised by Union or Member State law to which the controller is subject (fraud prevention or money laundering, for instance) and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.

---

[14] See Haga (2017: 97-126).

[15] See also "Guidelines on the right to data portability", WP 242 rev.01, adopted by the Article 29 Working Party on 13 December 2016, as last revised and adopted on 5 April 2017, available at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 (last accessed on 8 March 2018).

[16] See also "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679", WP 251, adopted by the Article 29 Working Party on 3 October 2017, available at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 (last accessed on 8 March 2018).

Besides all these exceptions which create a more favourable legal regime for the public data controllers when they receive a request from a data subject for exercising a right, the Art. 23 of the Regulation establish the premises for setting a general exception[17]. Thus, GDPR allows a significant number of cases where Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Art. 12 to 22 (listed above), and Art. 34 (notification of the data subject when a security breach occurred[18]), as well as Art. 5 (principles of data processing).

When it comes about restrictions to the rights of the data subjects, the Regulation allows them only under strict conditions: respecting the essence of the fundamental rights and freedoms, the measure should be necessary and proportionate in a democratic society to safeguard a limited number of important values, such as national security defence, public security, and other reasons expressly provided by Art. 23. Whenever the European or national legislator would make recourse to these provisions, they should take into account all the safeguards enshrined in the international legal instruments for human rights and established by the case law of the European Court of Human Rights and the European Court of Justice[19].

6. Data protection officer

The Regulation has lifted the obligation of the data controllers to notify the processing to the supervisory authorities. Instead, they are obliged in some cases[20] to designate a data protection officer (DPO) who will be an internal (or

[17] For a deeper discussion on the processing for public security or national security purposes, see Vermeulen, Lievens (2017: 171-251), Van Puyvelde, Coulthart, Hossain (2017: 1.397-1.416).

[18] See more in "Guidelines on Personal data breach notification under Regulation 2016/679", WP250, adopted by the Article 29 Working Party on 3 October 2017, available at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 (last accessed on 8 March 2018).

[19] As for the protection of the fundamental rights to privacy and data protection in the European Union, relevant judgments of the European Court of Justice are, for instance: Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others EU:C:2014:238, Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Davis and Others EU:C:2016:970.

[20] Art. 37 (1): "The controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10."

outsourced) *advisor* for the controller as regards the important tasks related to keeping of records, notification of data breaches, data privacy impact assessment, a *trainer* for the staff, a *point of contact* for data subjects and supervisory authorities, but also an inside *supervisor* for monitoring the compliance with the data protection provisions.

In case of the public data controllers, any public authority or body is compelled to appoint a DPO. The single exception allowed by the GDPR concern the courts acting in their judicial capacity, so for other types of processing activities (for administrative purposes, for instance), they shall also be obliged to appoint a DPO. Moreover, Directive (EU) 2016/680 allows Member States to exempt courts and other independent judicial authorities when acting in their judicial capacity from the obligation to designate a DPO.

Both EU legislative acts establish that a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

Even when there is no express obligation to appoint a DPO, it is however recommended to do so, his/her expert knowledge on data protection being an important asset for a due diligence processing of personal data. This is also the recommendation, as a good practice, of the supervisory authorities set out in the guidelines on DPO[21], when private organisations carrying out public tasks or exercising public authority[22] should designate a DPO.

7. Control by the supervisory authorities

In each Member State an independent data protection authority (DPA) is established in order to monitor the compliance of the GDPR (in Romania, the National Supervisory Authority for Personal Data Processing) and it has to be fully equipped with human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.

Three types of competences are allocated to the DPAs: investigative powers; corrective powers; authorisation and advisory powers.

[21] ”Guidelines on Data Protection Officers (‘DPOs’)”, WP 243 rev.01, adopted by the Article 29 Working Party on 13 December (2016), as last revised and adopted on 5 April (2017), available at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 (last accessed on 8 March 2018).

[22] In the WP Art. 29 Guidelines, the following examples are given: ”A public task may be carried out, and public authority may be exercised not only by public authorities or bodies but also by other natural or legal persons governed by public or private law, in sectors such as, according to national regulation of each Member State, public transport services, water and energy supply, road infrastructure, public service broadcasting, public housing or disciplinary bodies for regulated professions.” (p. 6 of the ”Guidelines on Data Protection Officers”).

The lead DPA shall be the sole interlocutor of the data controller or processor for the cross-border processing carried out by that controller or processor. The main rule for establishing the lead DPA is related to the main or single establishment of a data controller in one of the EU Member States, where the cross border processing substantially affects or is likely to substantially affect data subjects in more than one Member State.

However, where processing is carried out by public authorities or private bodies acting on the basis of a legal obligation, for the public interest or in the exercise of official authority, only the DPA of the Member State concerned shall be competent.

There is only one category of data controllers falling out of the competence of a DPA: the courts acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making.

In any case, the Regulation indicates the ”possibility” to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations” (para. (20) of the Preamble). In Romania, the Superior Council of Magistracy may take over this task.

Among the corrective powers to be exerted by the DPAs administrative fines is maybe the most important, as regards their effectiveness, proportionality and dissuasiveness, taking into account the maximum limits established by the GDPR (10 mil. or 20 mil. EUR/up to 2 % or 4% of the total worldwide annual turnover of the preceding financial year) and the criteria for applying them on a case-by-case basis.

As concerns the public data controllers, the GDPR has let each Member State to decide whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

Conclusions

The Regulation establishes a new set of rules for all the data controllers in order to ensure a uniform application and limit the legal fragmentation between the Member States. For instance, keeping internal records for the personal data processing activities is a general obligation with just a few exceptions. However, the public data controllers (public authorities and bodies, private entities carrying a public task) are exempted from a number of obligations (for instance, when it comes about the exercise of data subjects' rights or making a DPIA), on the one hand, and are compelled to execute others, without exception, on the other hand (for instance, to appoint a DPO). More specifications for public data controllers may be regulated by national laws of the Member States, when implementing the GDPR provisions.

Bibliography:

1. Buttarelli, G. (2016), ”The EU GDPR as a clarion call for a new global digital gold standard”, *International Data Privacy Law*, Volume 6, Issue 2, p. 77–78.
2. Haga Y. (2017) “Right to be Forgotten: A New Privacy Right in the Era of Internet”. In: Corrales M., Fenwick M., Forgó N. (eds) *New Technology, Big Data and the Law. Perspectives in Law, Business and Innovation*. Springer, Singapore, p. 97-126.
3. Lievens, E. and Vermeulen, G. (Eds) (2017), *Data Protection and Privacy under Pressure Transatlantic tensions, EU surveillance, and big data*, Antwerp, Apeldoorn, Portland Maklu.
4. Van Puyvelde, D., Coulthart, S., Hossain, M.S. (2017), ”Beyond the buzzword: big data and national security decision-making”, *International Affairs*, vol. 93, no. 6, p. 1.397-1.416.