The General Data Protection Regulation: what does the public authorities and bodies need to know and to do? The rise of the data protection officer

Associate professor **Marta-Claudia CLIZA**[1]
Assistant professor **Laura-Cristiana SPATARU-NEGURA**[2]

Abstract

On 25 May 2018, the General Data Protection Regulation will come into force in all the Member States of the European Union, replacing the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data and, additionally, in Romania, the Law no. 677 dated 21 November 2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data. This paper intends to analyse the regulation's provisions regarding the public authorities and bodies of a Member State, in order to discover how Romanian authorities should envisage to organise the processing of personal data. We shall reveal the steps that have to be taken by the respective entities of the State. Among the most important steps, we consider it essential to designate a data protection officer. Having in view that the European regulation expressly provides that those entities must designate a data protection officer, in this paper we shall emphasize what are the tasks, the role, the responsibilities, the qualities of the data protection officer.

Keywords*: data protection, DPO, GDPR, public authority, public body.*

JEL Classification: K00, K23, K33

1. Introductive considerations regarding the General Data Protection Regulation

It is obvious that nowadays the law experiences a growing development and assertion in the most varied areas of the society, appearing new legal branches, out of which the most important at the European level, the European Union law, which leads to a widening of the action sphere of the law.

There is a real process of legal ideological and institutional contamination. In this reality marked by the encounter of the legal civilizations, lawyers can no longer approach the phenomenon only from the perspective of national legal traditions, but also from the point of view of the interdependencies imposed by the competition of the legal values belonging to the various spaces of law.

[1] Marta-Claudia Cliza - Faculty of Law, "Nicolae Titulescu" University of Bucharest, Romania, cliza_claudia@yahoo.com.
[2] Laura-Cristiana Spătaru-Negură - Faculty of Law, „Nicolae Titulescu" University of Bucharest, Romania, negura_laura@yahoo.com.

For the purposes of this study, we underline that in the European Union, the data protection field is regulated by both primary and secondary EU law[3].

The General Data Protection Regulation[4] (hereinafter the "*GDPR*"), published on 27 April 2016 in the Official Journal of the European Union and which will come into force on 25 May 2018, replacing the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data[5] and, in Romania, the Law no. 677 dated 21 November 2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data[6]. Having in view the importance of the data protection field, the EU legislator has decided to adopt this piece of legislation through a regulation (instead of a directive), because unlike a directive, the regulation is directly binding and applicable in the Member States.

Many of the changes brought by the GDPR will affect the current information governance practices of Romanian public authorities[7]. We consider that the GDPR will increase the risks of processing personal data given the significant increase of the financial penalties due for violating the GDPR's legal provisions.

2. Specific requirements for the public authorities and bodies under the GDPR

Although the GDPR was designed to enable individuals to better control their personal data in a simplified manner, in some areas, its precise interpretation is unclear, fact that raises uncertainty regarding the authorities and the businesses compliance obligations. In order to address this issue and therefore to offer guidance for the GDPR, an advisory body was made-up of representatives of the national Data Protection Authorities of each EU Member State – the Article 29 Working Party (hereinafter the "*Working Party 29*").

What steps should the public authorities and bodies take in order to be prepared for the GDPR? It is obvious that several steps are required to be taken for

---

[3] For more information on sources of EU law, please see Nicolae Popa, *Teoria generală a dreptului*, fifth edition, C.H. Beck Publishing House, Bucharest, 2014, p. 172 and following; Augustin Fuerea, *Manualul Uniunii Europene*, sixth edition, revised and supplemented, Universul Juridic Publishing House, Bucharest, 2016, p. 230 and following; Laura-Cristiana Spătaru-Negură, *Dreptul Uniunii Europene – o nouă tipologie juridică*, Hamangiu Publishing House, Bucharest, 2016, p. 96 and following.

[4] Published in the Official Journal of the European Union no. L 119 dated 4 May 2016, please see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679, consulted on 15.03.2018.

[5] Published in the Official Journal of the European Union no. L 281 dated 23 November 1995, please see http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046, consulted on 15.03.2018.

[6] Published in the Romanian Official Journal no. 790 of 12 December 2001, please see http://legislatie.just.ro/Public/Detalii Document/ 32733, consulted on 15.03.2018.

[7] For more information on public authorities according to the Romanian legislation, please see Marta-Claudia Cliza, *Drept administrativ. Partea I*, revised and supplemented edition, Pro Universitaria Publishing House, Bucharest, 2017, p. 13 and following.

GDPR compliance, but, from the beginning, we underline that, for the economy and purpose of the present paper, we shall limit our research only to make general remarks, insisting on the most important step out of all, which will be left on purpose to the end.

Firstly, the public authorities and bodies should conduct a personal data audit in order to analyse the legal basis on which the personal data is currently processed. All relevant stakeholders should be involved in this special audit.

Secondly, the public authorities and bodies should organise trainings for promoting GDPR awareness in order that all staff members understand the public authority's obligations under the GDPR, especially the responsibilities and the process of reporting data breaches.

Thirdly, the public authorities and bodies should review and update their privacy policies, if they exist, in order to be GDPR compliant. A specific policy relating to data sharing should be created.

Fourthly, the public authorities and bodies should be prepared to handle data subject access requests within 30 days from the request date [Article 12 paragraph (3) of the GDPR]. Romanian authorities might be considering in investing in new technologies for facilitating searching and extraction of the relevant data within the legal timeframe.

Fifthly, the public authorities and bodies should prepare themselves to deal with security breaches likely to affect the rights and freedoms of a natural person, which should be notified in maximum 72 hours after having become aware of it, according to Article 33 paragraph (1) of the GDPR:

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay[8].

Sixthly, the public authorities and bodies should be prepared for data subjects to exercise their existing rights (e.g. right to erasure) or their new rights (e.g. the right to data portability).

Seventhly, the public authorities and bodies must prove that they are compliant under the GDPR with the principles of accountability and privacy by design.

Lastly, but left on purpose to the end, the public authorities and bodies should ensure that data protection officers (hereinafter the "*DPO*"s) are designated and compliant with the GDPR. This step solves many of the points above, reason for

[8] In the Romanian version there is a repetition which could be a translation error, since in other language versions verified, no such error existed. For more information on divergences between the official languages of the European Union documents, please see Laura-Cristiana Spataru-Negura, *The European Union and the Tower of Babel: Official Language Versions with Diverging Meanings*, „Romanian Journal of European Law" no. 2/2014, p. 31 and following.

which we have dedicated the rest of this paper for the understanding of the GDPR with respect to the DPO's role.

3. Public authorities and bodies' obligation to designate a DPO under the GDPR

Under the GDPR, DPOs are a cornerstone of data protection compliance, regulated by Section 4 of the Chapter 4 of the regulation (entitled specifically *Data protection officer*), applying to both controllers and processors with respect to the designation of a DPO.

We additionally underline that the controller is required to designate a DPO, but the processor is not necessarily required to appoint one. Although this is not requested by the GDPR, we consider it to be a good practice that can be instituted in the European Union.

The GDPR provides in Article 37 paragraph (1) the cases in which mandatory designation of a DPO is required:

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.

According to Article 37 paragraph (1) letter a) above, if the relevant data processing activity is carried out by a public authority or body, then a DPO must be designated. Please note that a single DPO may be designated for several public authorities and bodies.

Unfortunately, the GDPR does not define the expression "public authority or body", therefore we consider that it leaves it to each EU Member State to determine which organisations are public authorities and which are public bodies. We consider that this expression includes national, regional and local authorities, on one hand, and a range of other bodies governed by public law, on the other hand. From the European Union law, we are aware that the European legislator has already defined this term in Article 2 paragraphs (1) and (2) 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[9]:

[9] Published in the Official Journal of the European Union no. L 345 of 31 December 2003, please see https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32003L0098, consulted on 15.03.2018.

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 anybody:

(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.

We emphasize that *courts or independent judicial authorities when acting in their judicial capacity*[10] shall be exempted from complying with the rules of the GDPR.

Additionally, from the teleological interpretation of the GDPR, by reading Article 6 carefully we discover that this regulation is also applicable to natural or legal persons[11] governed by public or private law which perform *of a task carried out in the public interest or in the exercise of official authority vested in the controller* (e.g., in sectors such as public transportation, water supply, energy supply, road infrastructure, public service broadcasting, disciplinary bodies for regulated professions, public housing). In all these cases, the situation of the data subjects is similar to those cases when personal data are processed by a public authority or body. In such situations, when a private business or an individual performs outsourced public functions, on behalf of a public authority or a public body, we ask ourselves if a DPO should be appointed? Should it be a mandatory requirement in order to be in the spirit of the regulation?

In this respect, we salute the recommendation made by the Working Party 29:

> *Even though there is no obligation in such cases, the WP29 recommends, as a good practice, that:*
>
> - *private organisations carrying out public tasks or exercising public authority designate a DPO*

[10] Recital 97 of the GDPR.

[11] In this category are included also the companies set up by the Romanian town halls (for example, in 2017, the Bucharest Mayor announced the incorporation of 21 companies – please see http://www.mediafax.ro/social/cele-21-de-societati-infiintate-de-pmb-au-primit-buget-la-ce-valoare-se-ridica-investitia-si-ce-angajati-vor-avea-acestea-gabriela-firea-vom-spune-adio-unui-model-de-admi nistratie-invechit-16746624, consulted on 15.03.2018. In this respect, have been incorporated, among others, Compania Municipală Energetică Bucureşti S.A., Compania Municipală Iluminat Public Bucureşti S.A., Compania Municipală Dezvoltare Durabilă S.A., Compania Municipală Turistică Bucureşti S.A., Compania Municipală Pază Şi Securitate Bucureşti S.A., Compania Municipală Parcuri Şi Grădini Bucureşti S.A., Compania Municipală Medicală Bucureşti S.A. For more details, please see on the Bucharest town hall website the list of the companies incorporated http://www.pmb.ro/institutii/primaria/societati_comerciale/holding_mun_buc.php, consulted on 15.03.2018.

and that

- *such a DPO's activity should also cover all processing operations carried out, including those that are not related to the performance of a public task or exercise of official duty (e.g. the management of an employee database)*[12].

We fully agree with the Working Party 29 recommendation that the DPO should be appointed not only in relation to those outsourced public functions, but also including for all the processing activities that are unrelated to the outsourced public functions.

The concept of "data protection officer" is not new[13]. Even if the Directive 95/46/EC[14] did not provide any organisation to designate a DPO, in several Member States of the EU there was a practice of appointing a DPO (*e.g.*, Germany, Sweden). A DPO shall be a person, either an employee or an external consultant, who shall be given formal responsibility for data protection compliance within a public authority or a business. If a service contract is chosen, then two situations can be envisaged – the function of the DPO can be exercised either by an individual consultant, or by an organisation outside the controller's/processor's authority/body. In this latter case, we consider that each member of the respective organisation should fulfil the conditions provided for DPOs[15], especially that no one has a conflict of interests[16] in order to act independently.

The conflict of interest mentioning is required because the DPO is allowed to also fulfil other functions, with the condition that those tasks and duties do not give rise to conflicts of interests. The 29 Working party underlines in this respect that:

As a rule of thumb, conflicting positions may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing."[17]

---

[12] Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers ('DPOs')*, adopted on 13 December 2016, page 6, available at https://ec.europa.eu/info/law/law-topic/data-protection_en, consulted on 15.03.2018.

[13] Please see article 32 of the 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 offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=147 8857976436&uri=CELEX:32016L0680, consulted on 15.03.2018.

[14] Please see https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex:31995L0046, consulted on 15.03.2018.

[15] Please see Chapter 4, Section 4 of the GDPR.

[16] Please see Article 38 paragraph (6) of the GDPR.

[17] Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers ('DPOs')*, adopted on 13 December 2016, p. 15, available at https://ec.europa.eu/info/law/law-topic/data-protection_en, consulted on 15.03.2018.

These Guidelines provide us with useful information on the role and designation of DPOs.

But we query what qualities should a DPO have?

According to Article 37 paragraph (5) of the GDPR:

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 fulfil the tasks referred to in Article 39.

Of course, that a DPO must have suitable professional qualities and expert knowledge of data protection law, in order to be able to fulfil his or her role. The required level of expertise will vary depending on the public authority or body – the more complex or risky are the data processing activities, therefore the greater the DPO's expertise will need to be.

Reading together the Recital 97[18] and Article 38 paragraph (3)[19] of the GDPR, it is obvious that the DPO must be autonomous (*i.e.*, the public authority or body must not instruct the DPO on how to complete his or her tasks) and independent (*i.e.*, he or she must avoid any conflict of interests).

In this respect, public authorities should create internal rules and safeguards to ensure that the DPO is able to act independently and without any conflicts of interests.

In the Recital 97 of the GDPR, the European legislator expressly provides that "*[t]he necessary level of expert knowledge should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor*".

Moreover, the Working Party 29 underlines that: *the required level of expertise is not strictly defined but it must be commensurate with the sensitivity, complexity and amount of data an organisation processes. For example, where a data processing activity is particularly complex, or where a large amount of sensitive data is involved, the DPO may need a higher level of expertise and support. There is also a difference depending on whether the organisation systematically transfers personal data outside the European Union or whether such transfers are occasional. The DPO should thus be chosen carefully, with due regard to the data protection issues that arise within the organisation*[20].

Although the GDPR does not clearly specify the professional qualities that a DPO should have for being designated for such position, we consider that this person should have expertise in European and national data protection laws, especially a fully understanding of the GDPR. Additionally, knowledge of the business sector, of the public authority/body of the controller, and of the administrative rules and procedures of the organisation should be recommended. It

---

[18] *(...) Such data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.*

[19] *The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. (...).*

[20] Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers ('DPOs')*, adopted on 13 December 2016, p. 11, available at https://ec.europa.eu/info/law/law-topic/data-protection_en, consulted on 15.03.2018.

is also important that the DPO has knowledge of the information systems held by the controller.

We underline that most senior positions within a public authority or within a business (*e.g.*, chief executive, chief operating, chief financial, chief medical officer; head of marketing; head of HR or Head of IT) are likely to conflict with the duties of the DPO.

But what would be the effective role of the DPO? Please note that the public authorities/bodies or businesses must involve the DPO, *properly and in a timely manner, in all issues which relate to the protection of personal data*[21]. For this reason, the DPO should be seen as a discussion partner who would facilitate compliance with the GDPR. The DPO should be invited and must attend all relevant meetings at which decisions about personal data processing are made. In order to be able to make recommendations according to the GDPR, he or she should receive timely all the relevant information. It is necessary that the DPO be promptly informed and consulted every time that a data breach or a potential incident occurs.

Given the specific activity of each DPO, we consider that each public authority or body should develop data protection procedures or guidelines that establish when the DPO must be consulted.

Article 39 of the GDPR emphasizes the tasks of the DPO. Firstly, a DPO should assist the controller or the processor to monitor the internal compliance with the GDPR. This means that the DPO may collect information on processing activities, analyse the compliance of these activities, inform and issue recommendations to the controller or the processor on the results of the analyse.

The DPO shall also have the role to assist the controller in carrying out data protection impact assessments, according to Article 45 paragraph (1) of the GDPR. The controller should seek the DPO's advice on whether or not to carry out such an assessment, the methodology to follow, whether to proceed to an in-house or an outsourced assessment, on the specific safeguards, whether the assessment has been correctly carried out, and especially if its conclusions are compliant with the GDPR.

It is possible that the respective authority or body to disagree with the DPO's advice and therefore not to follow exactly the DPO's advice (being therefore incompatible with the GDPR). In such circumstances, the Guidelines require to documenting in writing the reason for not following the DPO's advice, while the DPO *should be given the possibility to make his or her dissenting opinion clear to those making the decisions*[22].

As for the DPO's tasks, according to Article 30 paragraphs (1) and (2) of the GDPR, each controller or processor shall maintain a record of processing activities under its responsibility. Thus, we ask ourselves if, for this obligation, the DPO could be held liable? Although the controller or the processor would have this obligation, therefore not the DPO, we consider that in practice the DPO could be the one to

[21] Article 38 paragraph (1) of the GDPR.

[22] Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers ('DPOs')*, adopted on 13 December 2016, p. 15, available at https://ec.europa.eu/info/law/law-topic/data-protection_en, consulted on 15.03.2018.

create the inventory and to hold this register. The DPO could be assigned officially with this task, since it could enable his or her tasks of monitoring compliance, being a prerequisite for compliance.

As previously mentioned, the DPO must be given sufficient autonomy and appropriate resources in order to carry out his or her tasks effectively. In order to fulfil his or her tasks, the DPO should be officially communicated to all staff members, and he or she should be provided with all necessary resources available for his/her role, for example full support from the management, appropriate financial resources, continuous training (in order to constantly increase his/her level of expertise), sufficient time to carry out his responsibilities, infrastructure (premises, equipment), and staff. The DPO shall also need access to other services departments (*e.g.* legal, IT, human resources).

From the analysis of Article 24 paragraphs (1) and (2) of the GDPR, we consider that the task of the DPO to monitor the public authorities or bodies' compliance with the GDPR does not conduct to DPO's individual liability for non-compliance by the respective authority or body, the liability remaining on the public authority/body:

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 organisational 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.

Therefore, the *data protection compliance is a corporate responsibility of the data controller, not of the DPO*[23].

Considering the strategic role of the DPO, mirrored even in the reporting system provided in Article 38 paragraph (3) of the GDPR, there were thought several protections for DPOs in order to help ensure that they are autonomous and independent. For example, under the GDPR they are protected from unfair dismissal / termination for reasons relating to their performance of the DPO role. If the DPO is under an employment agreement, therefore he or she may also benefit from the protections provided by national employment law, making it even more difficult to removing the DPO from his or her job.

However, the GDPR does not protect a DPO from dismissal or termination for reasons that are not connected with the performance of the DPO role (*e.g.*, gross misconduct, sexual harassment, theft). We consider that a DPO cannot be removed merely because he or she adopts a risk-averse approach towards data protection compliance (for example, if the DPO, considering that a particular data processing is highly risky and asks the public authority to carry out a data protection impact

[23] *Idem*, p. 16.

assessment, and the management does not agree with the DPO's assessment, then the DPO cannot be dismissed for providing the respective advice).

It is however interesting that the GDPR does not provide how and when a DPO can be replaced by another person.

Having in view all the above, it is vital for the public authorities or bodies, as well as for the businesses to ensure that they select a suitable DPO.

What if it is appointed an external contractor as a DPO? Then the protections afforded by the GDPR shall also apply to the respective external contractor (*e.g.*, no unfair termination of the service contract for activities as DPO).

What about the relation between the data subjects and the DPO? Data subjects should be able to contact the DPO of each organisation, reason for which the GDPR expressly provides in Article 37 paragraph (7) the obligations to publish the contact details of the DPO and to communicate them to the relevant supervisory authorities:

The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

This obligation is provided in order that the data subject and the supervisory authority can easily and directly contact the DPO. We consider that *de minimis* the following information regarding the DPO should be provided: postal address, direct telephone number and e-mail address. Of course, that other means of communication could also be provided (e.g. a special hotline, a contact form addressed directly to the DPO).

It is interesting that the name of the DPO is not expressly required[24]. We suggest that publishing the name of the DPO would be a good practice, but this remains a decision to be taken by the controller or even by the DPO.

Additionally, please note that, as „*a matter of good practice, the WP29 recommends that an organisation informs the supervisor authority and employees of the name and contact details of the DPO. For example, the name and contact details of the DPO could be published internally on organisation's intranet, internal telephone directory, and organisational charts*"[25].

What about the applicable sanction under the GDPR for non designating a DPO when mandatory? The GDPR changes fundamentally the level of the potential sanction for breaching the legal provisions on data protection, and for failure to designate a DPO, the GDPR provides that the administrative fine is up to 10,000,000

[24] In another legal provision of the GDPR regarding the obligation of the processor to notify a personal data breach to the supervisory authority, Article 33 paragraph (3), expressly provides that the name of the DPO has to be communicated:

3. The notification referred to in paragraph 1 shall at least:

(…) (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; (…)

[25] Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers ('DPOs')*, adopted on 13 December 2016, p. 12, available at https://ec.europa.eu/info/law/law-topic/data-protection_en, consulted on 15.03.2018.

EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher[26].

By *undertaking* in the EU law[27], public authorities are not exempted, therefore these administrative fines could be also applicable to public authorities, if not stated otherwise in the domestic legislation.

According to Article 83 paragraph (7) of the GDPR, each Member State shall be entitled to lay down the rules on whether and to what extent administrative fines may be imposed on its public authorities and bodies. For transparency, they are obliged to notify to the European Commission the legal provisions which they adopt by 25 May 2018 and, without delay, any subsequent amending law or amendment affecting them.

On 14 March 2018, the Romanian Senate published on its website a bill of law in application to the GDPR[28], initiated by two senators, which appears to be more restrictive than the GDPR in certain aspects (e.g. Article 3 prohibits the processing of biometric or genetic data other than by public authorities). With regards to the sanctions for the public authorities, a recent case comes to our mind: "the shaming list" published by the Romanian Fiscal Authority in 2016[29]. Having in view the fine applied in the respective case, please note that this bill of law proposes that fines applicable to public authorities will be no greater than 200,000 RON (approximately 43,000 EUR). This bill of law has been withdrawn from the Senate's agenda on 3 April 2018 and registered on the agenda of the Chamber of Deputies. It is very interesting to peruse the advisory opinion of the Romanian Legislative Council, in which it is underlined the need to establish the maximum levels of the fines foreseen for the public authorities in proportion to the maximum levels of the fines foreseen in Article 83 of the GDPR[30]. This is necessary because, since the GDPR establishes fines for the public authorities amounting to 20.000.000 euros [Article 83 paragraphs (4) -(6)], the bill of law establishes a cap to 200.000 lei. The beneficiaries of such cap are only the public authorities, the private entities not being subject of such limitation, for them being applicable the fine amounting to 4% of the turnover. From this perspective, having in view the purposes of the European legislator at the GDPR adoption, we do not consider it to be appropriately to impose

[26] Please see Article 83 paragraph (4) letter a) of the GDPR.

[27] Please see for more details https://wikis.fu-berlin.de/display/oncomment/Art.+101+para.+1+TFEU+-+Undertaking and https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/284407/OFT1389.pdf, consulted on 15.03.2018.

[28] Please see https://www.senat.ro/legis/lista.aspx, consulted on 15.03.2018.

[29] In May 2016, the Romanian Fiscal Authority published a list of all citizens having outstanding tax payments at that time, entitled "the shaming list". Certain payables were contested in the Romanian courts of law, therefore they were amended or even cancelled. In this respect, the Romanian data protection authority applied a fine on the Fiscal Authority based on fine capping under current Data Protection Law, amounting to 16,000 RON (approximately 3,500 EUR). Please see for more information https://economie.hotnews.ro/ stiri-finante-21000512-fiscul-publicat-lista-persoanelor-fizice-datorii-peste-1-500-lei-peste-187-230-romani-restante-fiscale-care-insumeaza-3-4-miliarde-lei.htm, consulted on 15.03.2018.

[30] Please see http://www.cdep.ro/proiecte/2018/100/60/7/cl167_2018.pdf, p. 7, point 14, consulted on 15.03.2018.

a derogatory responsibility, less punitive, for the public authorities. We recommend to the Romanian legislator to adopt an equitable approach for both public and private entities, imposing like this a sanctionatory regime common to all the actors in the data protection field. This is also the point of view expressed by the Romanian Economic and Social Council[31]. We shall follow interestedly the legislative process in order to find out the final version of this piece of legislation.

It is obvious that the administrative sanction regime will require a case by case assessment of the circumstances of each individual GDPR infringement.

In the legal systems which do not provide for administrative fines (*i.e.* Denmark, Estonia), the GDPR expressly regulates that in such Member States, the fine shall *"be initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive*"[32].

4. Final remarks

From 25 May 2018, the European Union's data protection legislation will change dramatically. Are the relevant actors (data subjects, controllers, processors, supervisory authorities, courts of law) ready for these changes? DPOs will be at the heart of the GDPR for all the public authorities and bodies, facilitating compliance with the data protection regulation's provisions. As previously mentioned, from this date, it is mandatory for these state entities, irrespective of what data they process, to appoint such a key player.

DPOs act as intermediaries between relevant stakeholders: supervisory authorities, data subjects, public authorities, public bodies or businesses. According to the GDPR, the controller or the processor has an important role in enabling the effective performance of the DPO's tasks, and we consider that the first step in this regard is appointing a DPO, which should be given sufficient autonomy and resources to carry out his/her tasks effectively. As mentioned in the recital 97 of the GDPR that DPOs should be in a position to perform their duties and tasks in an independent manner.

In order to train DPOs in the letter and in the spirit of the GDPR, we fully advise the supervisory authorities to promote accessible, adequate and regular training for DPOs.

Given the size of the controller or the processor, we also support the service contracts concluded with organisations, because combining the individual skills of several informed individual working in a team could serve more efficiently the interests of the parties whom they will represent, obtaining a more significant expertise on GDPR. However, we fully recommend mentioning in the service

[31] Please see http://www.cdep.ro/pls/proiecte/upl_pck2015.proiect?cam=2&idp=16976, p. 9, point 4, consulted on 15.03.2018.

[32] Please see Article 83 paragraph (9) of the GDPR.

contract a clear allocation of tasks within the "DPO team" and the designation of a person in charge for each entity represented.

It is crucial that the public authorities and bodies understand the need to designate a DPO and to involve him or her from the earliest stage possible in all issues relating to data protection. The sooner they do that, the safer their position is!

And, as the Working Party 29 underlines, "*the more stable a DPO's contract is, and the more guarantees exist against unfair dismissal, the more likely they will be able to act in an independent manner*"[33].

Therefore, the question is: who shall be your data protection officer?

Bibliography

1. Augustin Fuerea, *Manualul Uniunii Europene*, sixth edition, revised and supplemented, Universul Juridic Publishing House, Bucharest, 2016.
2. Laura-Cristiana Spătaru-Negură, *Dreptul Uniunii Europene – o nouă tipologie juridică*, Hamangiu Publishing House, Bucharest, 2016.
3. Laura-Cristiana Spataru-Negura, *The European Union and the Tower of Babel: Official Language Versions with Diverging Meanings*, „Romanian Journal of European Law" no. 2/2014.
4. Marta-Claudia Cliza, *Drept administrativ. Partea I*, revised and supplemented edition, Pro Universitaria Publishing House, Bucharest, 2017.
5. Nicolae Popa, *Teoria generală a dreptului*, fifth edition, C.H. Beck Publishing House, Bucharest, 2014.

[33] Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers ('DPOs')*, adopted on 13 December 2016, p. 15, available at https://ec.europa.eu/info/law/law-topic/data-protection_en, consulted on 15.03.2018.