RSP • No. 55 • 2017: 79-88

Data Protection Officer - a new profession in public administration?

Andra Maria Brezniceanu*

Abstract
The new European regulation of personal data protection domain is a real reorganization of the specific system, with profound effects on public administration staff or on labor market actors causing the emergence of new opportunities but of limitations too. The institution of the personal data protection officer, although not new, needs some clarification in the new setting.

Keywords: *data protection officer, Regulation 2016/679, public administration, European Union, personal data*

* University assistant, University of Craiova, Faculty of Law, Phone: 0723154085, Email: andra_brezniceanu@yahoo.ro.

The purpose of this paper is to clarify the institution and the attributions of the data protection officer, taking into account the aspect of relative novelty which the Compulsory European Law presents in this matter and the relationships of this institution with public authorities, too.

In January 2012 the European Commission initiated the reform of the private data protection. In December 2015 the European Parliament, Council and Commission established the new rules for the private data protection, which had a unitary legal frame in the European Union as a result. In April 2016 the Council and the Parliament adopted the regulation, about which we are to talk, this act being the normative expression of the reform in the domain of private data protection. On May 4th, 2016, the European Union Regulation Official Newspaper (EU) 2016/679 of the European Parliament and Council of April 27th, 2016 published an article on the protection of individuals with regard to the processing of personal data and on the free movement of these data and the repealing of Directive 95/46 / EC (General Data Protection Regulation).

In this introductory phase of our paper, it is useful to ask ourselves two questions: first, why was it necessary to change the legal framework of the processing of personal data, and the second question, why was it necessary to adopt a regulation, abandoning the old system based on the rule of law under the European directive?

The first question can be answered simply - lack of confidence. Apparently, the population of the European Union, irrespective of the state of which they were citizens, displayed a strong lack of trust in the old rules (for example Civile Code art.77, Low no.677/2001, art.2) that organized and sanctioned the way in which various entities processed personal data (for example Commission Decision of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina). This lack of confidence had a powerful effect on the digital economy and on the business in this area (Answer given by Mrs Reding on behalf of the Commission, Written questions by Members of the European Parliament and their answers given by a European Union institution). The effect was noticed at both economic and financial level, as well as at the legal level (for example Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce). See in this last direction the judgment of the European Court in the case of Google Spain SL and Google Inc. against Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (CJUE, Judgement of The Court -Grand Chamber, 13 May 2014). Another good, and extremely complex with the ongoing effects, source of information that fully justifies the distrust of the population, is the evolution of Edward Snowden's business.

The second question can be answered in a succinct way - the efficiency and effectiveness of applying the rules. As it is well known, the regulation is a compulsory European Union legislative act. This legislative act must be applied entirely by all the Member States of the European Union. Unlike a regulation, the directive is a legislative act setting an objective that all the Member States of the European Union must meet, but each of them has the right to decide on how to meet the established objective. The

distinctions between the mode of application and the effects of the two types of European legislative act also show us why the regulation option is more effective. If by using a directive there are 28 sets of national rules (for example Low no.677/2001, art.21) , one for each Member State of the European Union, each with the inherent bureaucracy –"The new legislative framework to be implemented from 2018 will impose, under certain conditions, the appointment of such independent officials who will take over some of the bureaucratic duties of the national authorities for the protection of personal data and which could thus concentrate their resources and efforts on fulfilling other important legal obligations, on effective intervention in respecting this right" (Șandru, 2016: 262). If we use the regulation we have to deal with a single set of rules, aggregated in that single regulation, universal and binding applicable in all Member States of the European Union. ”By choosing this type of legal instrument, the European Commission reaffirms the need for a uniform and fully harmonized legal regime for the protection of personal data in all Member States, given the direct applicability of a regulation under Art. 288 T. F. U. E” (Șandru, 2016: 171). Thus, through the General Data Protection Regulation, the European forums created a single framework for both the data processors and those whose data are processed. Such single regulation targets much more effectively - "... the regulation is considered to be the most appropriate legal instrument to reduce legal fragmentation." (Șandru, 2016:177) - providing a more urgent response to the issues in the field and removing the European public's mistrust of the way their personal data are processed.

As the consumers in all Member States seem to be increasingly interested in obtaining the most effective conditions for respecting the right to privacy, the European bodies considered this issue, using as a means the new rules introduced by the General Data Protection Regulation. In this way, on the path to this legal framework, new tools to protect the interests of those consumers are to be created. In addition to technical instruments, the regulation also introduces human-related instruments, respectively the European Data Protection Officer's European Law Institution.

The Data Protection Officer concept is not a new one in the European institutional landscape but has been somewhat ignored because Directive 95/46 / EC, which was repealed by the new European Regulation, did not contain mandatory provisions for persons involved in the processing of personal data to appoint a person for this, but it only mentioned it in article 18 as an alternative solution to the notification system. Within the framework provided by Directive 95/46 / EC, it was the responsibility of this person to ensure the compliance with the legislation on the protection of personal data within the entity for which he is active, an entity that was necessarily involved in data processing operations. This possibility to choose between alternative legal solutions (notification versus responsible) was also forwarded to the national legislation specific to the field of personal data protection, many of the Member States of the European Union choosing not to regulate such a profession and preferring to implement the already well-known notification system. Other countries, such as France, Germany, Sweden and the Netherlands, chose to introduce into their national legislation the institution of the Data Protection Officer probably because they considered that this system has several safeguards for respecting the right to privacy. In the well-known German spirit (before they were convicted by European Commission in the case C-518/07 European Commission v Federal Republic of Germany), the authorities of this state preferred to transpose into national law the possibility of voluntary appointment of the responsible person in an obligation, so that legal persons with more than 10 employees who process personal data systematically are obliged to appoint such a person. In the same spirit, it was

apparently found that individuals who are in charge of personal data protection have a good collaboration with state authorities, so the law is functional and the sanctions are rare. The diligence of those persons is also recognized by consumers, the signals transmitted about this function being positive. The data protection officer mechanism appears to have emerged as a result of the influences from the self-regulatory rules of public or corporative entities in the United States of America (for example Șandru, 2016:97), but ultimately it seems that the German model (for example Șandru, 2016: 267), is the basis for the new legislation that finalizes The European Union's Personal Data Protection Reform, the person in charge with such data becoming a national official with a voluntary status a European institution.

As we have previously shown, the voluntary nature of the appointment of the Data Protection Officer turns into a mandatory one by already mentioned European regulation. In these circumstances, certain distinctions in relation to persons and activities have to be made, in order to discern the burden of the entity's obligations. According to the provisions of article 37 paragraph 1of the Data Protection General Regulation, the appointment of the Officer is mandatory for public administration authorities. The rule of Article 37 paragraph 1 of this regulation does not expressly define what is meant by ' public authority or body', so that in the absence of a specific definition we must refer to the broadest legal framework provided by the national administration to understand the concept, the European legislator omitting to regulate this issue. On the other hand, the lack of distinction of the national legislature in relation to the various levels on which various public authorities, bodies and institutions are organized, we believe that it was intended to treat them equally, each of them having the obligation to appoint The Data Protection Officer. This regulation also lists two categories of entities that have the obligation to implement the responsible person in their own organization and functioning, but these are not relevant to this paper. However, from the perspective of these latter two categories, a question arises: do private law entities have an obligation to appoint a data protection officer when carrying out data processing operations in the exercise of a public power or public service. Our view is that a private entity that behaves similarly or identically to a public authority in relation to the processing of personal data must be subject to the same rules on the principle of the right *ubi eadem ratio, ibi idem jus*. In such a case, the data protection staff needs to extend their activity to all the personal data processing processes and not just to those that are directly related to the public authority of that private entity.

As a person who watches for the application of the Data Protection General Regulation, the person in charge should act as an intermediary between the people with an interest in this activity, and between the citizens (or consumers, if we want to keep some terminology distinctions) and the public authorities processing the personal data belonging to the first. As it follows from the provisions of article 37 paragraph (3) of this regulation, the European legislator has permissively legislated for public authorities, thereby enabling them to collectively appoint a single data protection officer. Such an option to simplify the organization of the administrative staff must nevertheless be passed through the rational filter of the two principles that we will set out below. Also, although it refers to public authorities, we believe that the possibility of conflicts of interest should be ruled out when two or more public authorities come into contact with a sole data protection officer.

Since it is for the purpose of this paper to clarify the duties of the Data Protection Officer, we believe that we must first remove some terminological blur. Indeed, the term "person in charge" may create the impression that an individual entity, either a civil

servant or a contract staff member, or an contractor external to the public authority, in charge of the position in question, has a responsibility in relation to the way in which the legal framework for Personal data protection is respected to the authority that hired him. We think that this is an erroneous idea, derived from a purely grammatical, prima facie interpretation, the term "person in charge" being improperly chosen by the Romanian translators of the Data Protection General Regulation. From a systematic interpretation of the normative act represented by that European regulation, in particular the provisions of paragraph 74 of its preamble and of article 24 par. 1 of its content, it results that the data protection operator represents one of the measures that must be taken by the public authority as a personal data processor and not by a vehicle that takes over the responsibility of the person for whom it works, such as a public authority. In other words, data protection is the responsibility of their operator and not of the controller. However, we believe that in some situations, we will come back to below, the Data Protection Officer may end up being penalized for the way he has done his business in his relationship with the employing entity.

A second issue that needs to be clarified in regards to the tasks of the Data Protection Officer is that of the effective framework in which he is operating. We believe that the entities processing personal data have a real obligation to provide the data protection officer with an adequate environment for the performance of the benefits that have been contracted or attributed to him. The Data Protection General Regulation introduces two determinant principles for the framework to be provided to the operator by the entity for which it operates. The first principle is that of the autonomy of the responsible person. The second principle, much easier to overlook, is to ensure that the entity for which the operator carries out his / her activity has the necessary means for the protection to become a permanent and effective exercise. We will return to the first principle where we will present the issue of the conflict of interest that may affect the objectivity of the Data Protection Officer. Regarding the second principle, we believe that the environment in which he/she will operate in favor of the authority that processes personal data is best outlined by the provisions of article 38 paragraph 1-6 of the Data Protection General Regulation.

The Data Protection Officer must receive a covering mandate to carry out its work from the public authority processing personal data. This mandate should also allow the operator to act in due time, especially if the data processed by the authority are some that can be disseminated to the public or may be approached by malicious third parties by electronic means. This mandate should not be limited to certain personal data chapters, which would imply a restriction of the powers of the officer. The Data Protection Officer must benefit from all the contest of the management of the public authority that processes the personal data, the alternative being that in which the mandate sent to the responsible person is an apparent one, being emptied of the content of power.

In order to carry out its activity, the Data Protection Officer must be provided with a material basis appropriate to his / her duties by reference to the complexity and the volume of tasks established with the management of the authority that processes personal data. It should be noted the wording the European legislator gave to the provisions of article 38 paragraph 2 of the Data Protection General Regulation - the officer should be given tasks which in a general form are set out in the mentioned regulation by the authority not in relation to the volume and complexity of the data to be protected, but in relation to the tasks drawn by the authority. Thus, the public authority will not be able to invoke its defense if it does not comply with, or breaches the provisions of the Data Protection

General Regulation as a justification for the poor endowment of the officer, that he/she does not carry out a large and complex processing of personal data.
It is obvious that the Data Protection Officer must access that data. A limitation to their access through the mandate received from the authority that processes them is a circumvention of the provisions of the Data Protection General Regulation. The same a hindrance by any means, including those of an organizational or technical-functional nature, to the access of the controller to the actual data processing operations should be seen.

Until we reach the ethical background specific to the person in charge with data protection, we need to clarify his / her skills necessary to carry out his / her work with the public authority. The provisions of article 37, paragraph 5 of the Data Protection General Regulation indicate as criteria for the selection of the person in charge of data protection: (i) the professional qualities and (ii) the ability to perform the tasks provided for in article 39 of the same Regulation. Indeed, it can be argued that these are too general to allow the human resource manager to identify the most suitable candidates for such a function, but we believe that precisely such general criteria are the most beneficial for choosing the best staff to occupy a function that is new. The express reference to the professional qualities of expert knowledge of the right of personal data protection and related practices seems to reveal that the intention of the European legislator was that the national public authorities called upon to implement the regulation in question should assign the posts of Data protection to persons with juridical studies. We believe it is a mistake to look strictly at the graduates of law faculties and even in the direction of the graduates of any faculty to find the most suitable candidates for the position of data protection officers because some of the tasks of art. 39 of the Data Protection General Regulation may prove to be practical in some cases requiring high technical training, such as that provided in article 39, paragraph 1, letter C, which is a reference to article 35 of the same article. Our view is that the European legislator has rather pursued the occupation of data protection officers with professionally trained people but in a varied and interdisciplinary manner, capable of technical and ethical reasoning alike. In support of a good selection of staff for this function may be criteria such as: knowing the specifics of the activity of the public authority, the organization of the apparatus of the public administration, the processes and operations in certain domains of the activity carried out by means of the electronic information and communication equipment, the technical protection of the data, etc. Another argument against the choice of lawyer for the person who will be in charge of data protection is also that of the loyalty they are expected to manifest to the public authority employing their services. The subject in charge of data protection has to turn its loyalty less to the public authority and more to the citizens (or consumers) whose personal data are processed by the public authority. If the European legislator had intended that the Data Protection Officer would be an obedient employee to the payer, then he would explicitly mention this condition of loyalty in the Data Protection General Regulation and would not have made the mention of the institution of the conflict of interest over to which we will come back below. Moreover, if we do not lose sight of the fact that the purpose of the person in charge can be translated into the form of the protection of personal data from the citizens of 28 nations, then we can see as obviously exaggerated the expectation that the person in charge of this post manifests first loyalty to a particular state and government.

Coming back to the ethical issue of the person in charge of data protection in relation to a public authority, we note that the Data Protection Officer is in direct

relationship with two relevant entities: (i) the public administration entity processing the data (and which is his / her employer) and (ii) the supervisory, control and sanctioning authorities specifically empowered by the national state for personal data protection. Of course, the Data Protection Officer has the primary responsibility towards the persons whose personal data are processed by the public administration entity that hired him, but does not establish a direct relationship with them.

In relation to the first subject with which the data subject is involved, the respective public authority processing the personal data, the Data Protection Officer must show maximum firmness to the staff and management of the data because its interests are secondary to the purpose of its function - the application of the European regulation on the processing of personal data within that authority, i.e. the very reason for the existence of its function and its object of activity. It is very likely that in some situations, the data processor's interests become insignificant compared to the data whose data they process, so that the person in charge of these data is required to lean through his views (and possible decisions) in favor of those whose data are processed and not to the public administration that is employing and rewarding him/her. This interpretation results from the provisions of article 38, paragraph 2 and 3, 39 paragraph 1 letter A and B of the Data Protection General Regulation.

In relation to the second subject with which it comes into relationship, it must firstly be observed with maximum acuity and full understanding of all the consequences of the provisions corroborated by article 38, paragraph 5 and 6 and article 39 paragraph 1 letters D and E. It is clear from these rules that it is imperative for the Data Protection Officer to fully cooperate with the supervisory authority. If the wording of the provisions of letter A - C from par. 1 of art. 39 of the Data Protection General Regulation with those of letter D of the same paragraph shows not only a difference in the firmness of the European legislator's tone, but also a difference in the nature of the regulatory tasks assigned by the same legislator to the Data Protection Officer and his employer in the national administration. The first three rules, namely those at letters A-C, establish for the Data Protection Officer non-decisional tasks, but to monitor the work of the national authority regarding the observance of the provisions of the General Regulation on Data Protection and counseling the same authority in the reference field of the same normative act. Contrary to these three tasks is that from letter D, the task of which is reduced to its binding nature by the drafting of the European legislator. The consequence of the imperative of this rule is that the Data Protection Officer must effectively cooperate with the supervisory authority and its interests in relation to those of the public authority that hired the Data Protection Officer. It becomes easy to understand such a hierarchy of relations between the subjects involved in this organizational scheme, if we give constant attention to the subject of regulation of the General Regulation on data protection, respectively the protection of personal data. This immutable objective determines the collaboration between the officer and the supervisor, even to the detriment of the public authority that hired the responsible person, through his/her status f personal data processor, the latter being subject to the constraint and sanction of the other two (the officer and the supervisor). Collaboration between the officer and the supervisory authority for the purpose of sanctioning the public authority processing the personal data is an accessory to the monitoring operation of the compliance with the Data Protection General Regulation of the Data Protection Officer on the public authority processing the personal data. The legal obligations to monitor and collaborate (including for the purpose of sanctioning their own employer) of the data protection officer are also preconditioning

the evidence against the public authority for processing personal data. This is clear from what the European legislator pointed out at point 82 of the preamble to the Data Protection General Regulation. In order to be able to prove that it complied with the provisions of the Data Protection General Regulation, namely that it properly implemented its obligations under this set of European rules, the national public authority processing personal data "should keep records of the processing activities under his/her responsibility". The immediate operation in the collaboration process between the Data Protection Officer and the Surveillance Authority is to communicate the evidence from the first subject to the second - "Each operator and each person empowered by the operator should have an obligation to cooperate with the authority and to make available on request these records in order to be used for the purpose of monitoring the processing operations concerned. "The purpose of the transmission of records is only temporary that of monitoring, because if the monitoring and research of the respective records generates the premises of a sanctioning of the public authority for the processing of personal data, then the mentioned purpose is transformed into the one of the formation of the proof to support the punishable act. The cooperation between the Data Protection Officer and the Surveillance Authority takes place as a matter of urgency, as is apparent from the wording of the reason from point 86 of the Preamble to the Data Protection General Regulation - "Communications to the competent persons should be made as soon as possible in a reasonable manner and in close cooperation with the supervisory authority, in compliance with the guidelines provided by it or by other competent authorities, such as law enforcement authorities. "As the interest to be protected is that of the person whose personal data are processed by the national public authority that is responsible for the protection of those data, it follows that the operations that form the object of the collaboration with the supervisory authority must be carried out within the time period completed with the communication to the targeted subject. Or that means a maximum urgency that the Data Protection Officer could not ensure if the interests of the data processing authority prevailed.

A last but important issue for defining the institution of the Data Protection Officer and the framework for acting in this role is the conflict of interest situation in which this subject of law can be placed. In order not to be in such a situation, i.e. to act in an independent and not autonomous or even dependent manner, the data protection officer employed within a national public authority has to prove a particular morality in the relations with the employer. It should also be his employer's understanding of the importance of personal data protection and the severity of the risks that can occur if this protection is not achieved but, as the purpose of our paper is not to clarify the obligations that the Data Protection General Regulation gives to these, we will not give any expectation to the subject that processes the personal data.

The first condition for ensuring his/her own independence and avoiding conflicts of interest is that the Data Protection Officer should not accept instructions about how to perform his data protection activity from the national public authority that has hired him. Achieving this obligation effectively turns that person into an objective guarantor of how the employing public authority understands to treat the protection of personal data he has in the processing. In other words, prior to the sanctioning intervention of the supervisory authority, the Data Protection Officer is the first filter (including the legality) of how the provisions of the Data Protection General Regulation within the public authority that hired him are respected. Such a condition may be difficult to put into practice if it is chosen that the duties of data protection officer to be entrusted to an employee who has other duties

from another job that he carries out within that employing authority. The best examples are represented by lawyers or by computer scientists. We anticipate that these people, at the intersection of their core and that of data protection functions, have the best chance of conflicting interests, and the distinctions between the two sets of tasks cannot be easily perceived either at the level employee or employer.

A second condition for maintaining the accountability of the person responsible for the duration of his / her duties is that the person in charge of this position not to be sanctioned, including dismissed, by the public authority employing for the way they perform their data protection activities. Of course, it can be questioned whether the sanction can be applied for failing to comply with the tasks deriving from the Data Protection General Regulation. We are inclined to argue that such a sanctioning hypothesis is viable, but we believe that the evidence must be substantial and conclusive. An interesting perspective on the facts is opened when the manager has known the conflict of interest or has been induced into this state by the leaders of the public authority of the staff to which he belongs.

A third and most important condition is to avoid conflicts of interest in relation to other attributions held by those who will be in charge of data protection positions. As some of these attributions may be somewhat significant to the way in which the personal data processing system is organized and operated within the national public authority of the officer, such as those of lawyers who design the principles and rules under which it is organized or that of the programmers and operators who conceive it or make it work, we anticipate as an optimal solution to avoid conflicts of interest those of new staff recruitment, avoiding the overlapping of tasks from different functions or contracting by outsourcing the duties and tasks of the responsible position.

Normally, the rules for making the works such as this one would force us at this point to draw a conclusion from the previous ones. Our view is that the subject of the paper only places us at the beginning of a long chain of such works, any conclusion being premature.

References:

Answer given by Mrs Reding on behalf of the Commission, Written questions by Members of the European Parliament and their answers given by a European Union institution. Retrieved from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOC_2013_361_E_0001_01&qid=1498678943013&from=EN.

Judgment of the Court (Grand Chamber) of 9 March 2010 - European Commission v Federal Republic of Germany Case C-518/07. Retrieved from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2010.113.01.0003.02.ENG&toc=OJ:C:2010:113:TOC.

CJUE, Judgement of The Court -Grand Chamber, 13 May 2014, case of Google Spain SL and Google Inc. against Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. Retrieved from: http://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A62012CJ0131.

Commission Decision of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina. Retrieved from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003D0490&qid=1498674006860&from=EN

Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce. Retrieved from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000D0520&qid=1498674006860&from=EN

Directive 95/46/EC, art. 18. Retrieved from: http://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:31995L0046&from=RO.

Șandru S. (2016). Personal Data and Privacy, Bucharest: Hamangiu Publishing.

Low no.677/2001, Monitorul Oficial no.790/12.12.2001, art. 2, 21.

Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (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).

Retrieved from: http://eur-lex.europa.eu/legal-content/RO/TXT/?uri=OJ:L:2016:119:TOC, art. 37(1),(3) (5), 74, art. 24(1), art. 38 (1-6), art. 39, art. 35.

Romanian Civil Code–Law no.287/2009. *Monitorul Oficial* no. 505/15.07.2011, art.77.

Article Info

Received: June 30 2017
Accepted: July 20 2017