# A NEW PERSPECTIVE ON THE LEGAL ADMINISTRATIVE BURDENS ON DATA CONTROLLERS WITHIN THE EUROPEAN UNION

***Ancuţa-Gianina OPRE*** [*]
***Simona ŞANDRU*** [**]

Abstract

*For almost twenty years the legal regime on personal data protection within the European Union was mainly regulated by 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. According to the provisions of this act, one of the legal obligations of the data controllers was to notify the processing operations they carry out to the supervisory authorities established in the Member States. Each Member State transposed this legal provision in different ways, and some of them stipulated a series of exceptions from the obligation to notify, among which being the appointment of a data protection official at the level of the data controllers. The process of notification results in administrative burdens, both for the data controllers and the supervisory authorities, in some cases. Therefore, the latter ones (associated within the Article 29 Working Party) and the European Commission supported the idea of simplifying the current system. Against this background, the legislative reform proposed by the European Commission in 2012, which intends to replace Directive 95/46/EC by an overall mandatory regulation, sets up a new way of thinking the administrative burdens on data controllers, from a double perspective: on the one hand, by lessening the obligations in relation to the supervisory authorities (for instance, no obligation to notify subsists), and on the other hand, by multiplying the legal requirements to internally implement a number of measures aiming at enhancing the level of protection of the personal data processed by a certain data controller. This paper will focus on the main changes adduced by the recent legislative proposal as regards the administrative obligations of the data controllers.*

Key Words: *right to personal data protection, legislative proposal, European Commission, data controller, data protection official, principle of accountability.*

## 1. Introduction

The European legal regime of personal data protection was firstly established by 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 [1] (hereinafter "Directive 95/46/EC"), considered as being the first European Community act regulating a fundamental right. Once the Lisbon Treaty entered into force, the right to personal data protection (and

[*] Associate Professor, Ph.D., The Faculty of Law and Administration, "Dimitrie Cantemir" Christian University, Bucharest, Romania.

[**] Ph. D., Faculty of Law, University of Bucharest, Romania.

[1] OJ L 281, 23.11.1995, pp. 31-50.

the right to privacy, as well), gained universal legal value across the former "pillars" (internal market, common foreign and defence policy, freedom, security and justice), as it is enshrined in the Charter of Fundamental Rights of the European Union[2] (hereinafter "Charter") - Art. 8[3], and in both of the treaties - Art. 16[4] of the Treaty on the Functioning of the European Union[5] (hereinafter "TFEU") and Art. 39[6] of the Treaty on European Union (hereinafter "TEU"[7]).

Three main elements form the said legal regime: the principles of a legal and fair processing of personal data, the rights of the data subjects and the control carried out by an independent authority, the latter ensuring the efficiency of the former ones. All these elements are clearly and expressly provided by Directive 95/46/EC and are reflected in detail in the Member States national legislation on data protection. On the other hand, as the directives are mainly an instrument for harmonization of the legal acts and administrative practice within the European Union, which aims at a binding result (in this case, the protection of privacy and the free movement of personal data), some differences may be noted, for instance, in relation to the means of transposing some of the principles of processing sensitive data, the procedures for enforcing data subjects' rights, or the tools which are made available to the supervisory authorities in order to carry out their prerogatives. From this point of view, a regulation may ensure a more comprehensive uniform approach of the legal regime on data protection, and consequently, better guarantees for this right all over the European Union. Against this background, in 2012 the European Commission proposed to the European Parliament and to the Council a reform package[8] that repeals and replaces Directive

[2] OJ 2010/C 83/02, 30.03.2010.

[3] "Art. 8 Protection of personal data 1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.

[4] "Art. 16 (ex Art. 286 TEC) 1. Everyone has the right to the protection of personal data concerning them. 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union."

[5] Consolidated Version of the Treaty on the Functioning of the European Union, OJ C 83/47, 30.03.2010.

[6] "Art. 39 In accordance with Article 16 of the Treaty on the Functioning of the European Union and by way of derogation from paragraph 2 thereof, the Council shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities which fall within the scope of this Chapter, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities."

[7] Consolidated Version of the Treaty on European Union, C 83/13, 30.03.2010

[8] The reform package consists of a „Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and a „Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or

95/46/EC by a new regulation[9]. The main objectives set out by this proposal[10] are the following: to modernise the European Union's legal system for the protection of personal data, in particular to meet the challenges resulting from globalisation and the use of new technologies; to strengthen individuals' rights, and at the same time reduce administrative formalities to ensure a free flow of personal data within the European Union and beyond; to improve the clarity and coherence of the European Union's rules for personal data protection and achieve a consistent and effective implementation and application of the fundamental right to the protection of personal data in all areas of the Union's activities. As this proposal, which is still under debate, comprises many new provisions likely to be subject to a distinct analysis, our paper will mainly focus on some of the newly established administrative obligations of the data controllers, compared to the existing ones.

## 2. Obligations in relation to the supervisory authorities

According to general data protection rules, a data controller has to comply with two categories of obligations: towards the supervisory authorities, on the one hand, and towards the data subjects, whose personal data they are processing, on the other hand.

Once a data controller (a natural or legal person), established or carrying out business in the European Union's territory, chooses to process personal information in the course of his/her/its current activity or otherwise, establishing the purpose and the means to do it, he/she/it has to obey the European data protection rules. In order to ensure enough transparency on the conditions surrounding the processing, two important obligations have been set upon the data controllers: to inform data subjects at the time the data are being collected or at a later stage (at first disclosure) and to notify such processing to the supervisory authorities. The result of the notification process is reflected in the publicly available register kept by the data protection agencies, so that any interested party may check whether a specific processing has been made known by the data controllers, or if the information they provided is true or complete. Based on the information therein, the supervisory authorities may decide to conduct an investigation (*ex post*) in order to remedy the possible deficiencies or to make a prior check before the processing begins (*ex ante*), so it may prevent excessive operations on personal data or other type of infringement of the individuals' rights and freedoms.

In certain circumstances, compliance with the duty to notify may represent an excessive administrative burden for the data controllers, especially when they process different types of personal data for different purposes, which requires repeated

---

prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data".

[9] For a global analysis on the proposal, see Danagher, L., *An Assessment of the Draft Data Protection Regulation: Does it Effectively Protect Data?*, European Journal of Law and Technology, Vol. 3, No. 3, 2012.

[10] See http://ec.europa.eu/justice/data-protection/review/index_en.htm, accessed on May 21th 2015.

notification. Therefore, the European and national legislators laid down specific provisions for simplifying or even exempting from the duty to notify, in some cases.

Besides this, Directive 95/46/EC provided the possibility to have an alternate procedure to the one involving the notification obligation, when a data protection official has been appointed by a data controller.

The European Union's Directive left room for the Member States to establish the system they consider to be more appropriate, so the current situation varies deeply, from states like Italy when only some categories of processing operations have to be notified, to states like Spain when there is no exemption from the notification duty. In the same respect, a number of Member States[11] decided to take on board the other solution provided by the Directive 95/46/EC, namely, establishing a data protection official who was partly entitled to exercise a few of the powers traditionally assigned to the supervisory authorities: keeping the register of the processing operations carried out by the data controller and making the prior checking of the operations likely to pose specific risks to the rights of individuals.

Although one role of the data protection officials is to make the administrative burdens easier, even the burdens on the "shoulders" of the data protection authorities, the "officials" do not replace the "authorities". According to Art. 18 (2) of Directive 95/46/EC, the data protection official is vested with the main power to ensure in an independent manner the internal application of national dispositions transposing the directive. At the level of the European Union, Regulation 45/2001/EC[12] stated from the beginning that all the European Union's institutions and bodies have to appoint a "data protection officer".

Ten years after Directive 95/46/EC came into force, the European Commission and the national data protection authorities in the European Union concluded that this latter model is functioning very well in the countries embracing it and encouraged all the rest to adopt it.[13] Therefore, it came as natural to provide in the new text of the regulation, aiming at replacing Directive 95/46/EC, the obligation for some categories of data controllers to appoint a data protection officer.

According to Art. 35 of the proposal, a data protection officer must be designated by data controllers or data processors, in case they pertain to the public sector, and in the private sector, also, but only for large enterprises (employing 250 persons or more) or where the core activities of the private controller or processor consist of processing operations which require regular and systematic monitoring of data subjects. In other cases, it is also possible to appoint a data protection officer, if the data controllers or processors so wish. The proposal of regulation establishes in the Section 4 a complete legal regime of this (kind of) new profession, by setting up

---

[11] States where a data protection official (under different names) may be appointed are as follows: France, Germany, Luxemburg, The Netherlands, Sweden, The Slovak Republic, Poland.

[12] Regulation (EC) No 45/2001 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, OJ L 8, 12.01.2001, p. 1.

[13] "Article 29 Working Party report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union" - WP 106, 18 January 2005, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp106_en.pdf, accessed on May 23th 2015.

the conditions of the appointment, the minimum term of mandate, his/her position and tasks. The supervisory authorities and the public have to be properly informed about the name and contact details of the data protection officers, so the data subjects may exercise the rights towards them. The data protection officers are also compelled to develop a good collaboration with the supervisory authorities, within specific consultation or inspection activities. These rules are partly inspired by the model of the data protection officer already existing in some Member States (especially, Germany); on the other hand, the European Commission created a "European-like" model where the supervisory authorities are not directly involved in the procedure of appointment of a data protection officer, as it is the case in Luxemburg or Slovakia, for instance, or in France, where the opinion of the data protection authority, in case the data protection officer („correspondant informatique et libertés"/"correspondant à la protection des données personnelles")[14] failed to comply with his/her legal obligations, must be taken into account by the data controller, in order to release him/her from function.

As a result of the adoption of the proposal, in all the Member States no duty to notify the processing operations will subsist, the data protection officers being compelled to monitor the implementation and application of data protection legislation, as a reflection of some of the supervisory authority's duties, on a smaller and particular scale.

Nevertheless, a new type of obligation to notify the supervisory authorities has been introduced by the proposal, which was until now applicable only in the electronic communications sector[15]: the notification of the breaches of security (in the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority). A similar notification will have to be also sent to data subjects when the breach is likely to adversely affect the protection of privacy of the data subjects or if so requested by the supervisory authority.

Moreover, there is a series of other administrative obligations on data controllers in relation to the supervisory authorities, provided by the proposal, such as: to consult the data protection authority in order to process personal data which, by virtue of their nature, scope or purposes, may present specific risks to the rights and freedoms of data subjects, according to a previous data protection impact assessment made by the controller or to the public list established by the supervisory authority; to obtain, as the case may be, a prior authorization for transferring personal data outside the European Union, based on *ad hoc* contractual clauses or some other not legally

[14] See http://www.cnil.fr/, accessed on May 23th 2015.

[15] This is according to Art. 3 of the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance), OJ L 337, 18.12.2009, pp. 11–36.

binding instrument; to submit for approval of the data protection authority the binding corporate rules which allow the transfer of personal data to third countries.

In Romania, under the current legal framework on data protection, there is no general legal obligation to appoint a data protection officer. Nevertheless, there is the sectorial case of the processing operations made by the Ministry of Home Affairs and its territorial offices[16], where a special body or responsible person for data protection has to be designated at the level of each controller or processor functioning under the authority of this ministry. The criteria for appointing a body or just a person are related to the quantity and frequency of the processing operations, and the number of the users involved in this kind of operations, as well. However, this model is not entirely similar to the one provided by the legislation in some other Member States, as the supervisory authority is not involved in the procedure of appointing or exercising the functions by the ”responsible person for data protection” who is not carrying out his/her duties in an independent manner; moreover, the Ministry of Home Affairs and its territorial offices are still obliged to notify the processing operations they carry out to the national supervisory authority.

### 3. Other internal administrative obligations

Apart from the obligations that data controllers will have to comply in relation to the supervisory authorities, the proposal of regulation provides additional administrative obligations which have to be put internally in place.

The obligation to notify the processing operations to data protection agencies, currently provided by many national legal acts, will be replaced by the obligation to maintain documentation on the processing falling under the responsibility of the data controllers (but also on their representatives and data processors), which requires to contain the same information as in the notification forms presently used (according to Directive 95/46/EC). The only controllers not subjected to this obligation are the natural persons processing personal data without a commercial interest and the small organizations processing data as additional to their main activities.

Under the future legal framework on data protection, data controllers and processors will still be under the obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation. These measures also refer to the instructions that a data controller must give in writing to a data processor. Two more principles have been expressly added to this legal regime (“privacy by design” and “privacy by default”[17]), thus enhancing the responsibility of

[16] Instructions no. 27/2010 on the organizational and technical measures for ensuring the security of the personal data processing operations carried out by the structures/units of the Ministry of Administration and Interior, OJ, Part I, no. 98 of 12 February 2010.

[17] Some scholars are rather skeptical about the use of these principles: “”Privacy by design" consists of a number of principles that can be applied from the onset of systems development to mitigate privacy concerns and achieve data protection compliance. However, these principles remain vague and leave many open questions about their application when engineering systems.” – Gürses, S., Troncoso, C., and Diaz, C., „Engineering Privacy by Design”, K.U. Leuven/IBBT, ESAT/SCD-COSIC, available at https://www.cosic.esat.kuleuven.be/publications/article-1542.pdf (accessed on May 21th 2015).

data controllers from the time of determination of the means of processing till the time of effective implementation. These principles have also the role of ensuring that only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage, and, in particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.

As already mentioned above, the new rules on data protection oblige data controllers to carry out an assessment of the impact[18] of the envisaged processing operations on the protection of personal data, based on criteria such as: the specific means of processing which are involved and their legal effects, the nature of data (sensitive data), the intended purposes or some categories of data subjects. The processing operations carried out by a public authority or resulted from a legal obligation are not subjected to the obligation to make such an impact assessment.

## 4. Conclusions

Once the regulation proposed by the European Commission in 2012 will be adopted, the data protection legislation all over the European Union will be completely harmonized, in order to achieve „a better data governance" [19] and accountability from data controllers and processors. While some of the current administrative burdens (notification of the processing operations to the supervisory authorities) will disappear, some other new obligations will have to be respected, such as the impact assessment, documenting internally all the processing operations, the notification of a data breach, the implementation of the principles of "privacy by design" and "privacy by default".

This new perspective on the legal regime on data protection in the European Union, reflecting a mixture between external and internal duties on data controllers and processors, will have a positive effect as regards the consolidation of the fundamental rights and freedoms of individuals, especially, their rights to privacy and personal data protection, thanks to the legal certainty and uniformity intended to be brought about by the regulation.

## References

1.L. Danagher, "An Assessment of the Draft Data Protection Regulation: Does it

[18] The subject of the assessment of the impact on data protection is older than the proposal of regulation (see Clarke, R., "An evaluation of privacy impact assessment guidance documents", International Data Privacy Law (2011) 1 (2): 111-120. doi: 10.1093/idpl/ipr002).

[19] These objectives were also expressed by the Art. 29 Working Party in its document "The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data", WP 168 of 1 December 2009, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf, accessed on May 23th 2015. The principle of responsibility and liability of data controllers may also be found in the Opinion 3/2010 on the principle of accountability, adopted by the Article 29 Working Party on 13 July 2010, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf, accessed on May 23th 2015.

Effectively Protect Data?", European Journal of Law and Technology, Vol. 3, No. 3, 2012;
2. S.Gürses, C. Troncoso, and C. Diaz, Engineering Privacy by Design", K.U. Leuven/IBBT, ESAT/SCD-COSIC, available at https://www.cosic.esat.kuleuven.be /publications/article-1542.pdf;
3. R. Clarke, "An evaluation of privacy impact assessment guidance documents", International Data Privacy Law (2011) 1 (2): 111-120. doi: 10.1093/idpl/ipr002.