The effects of Regulation no. 679/2016 on the Romanian commercial environment. The new obligations in the field of personal data

Student **George-Cristian IOAN**[1]

Abstract

The entry into force of 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, commonly referred to as the General Data Protection Regulation will lead to significant changes in the domestic commercial environment. The present study aims to analyse the main problems that Romanian companies will face. In this respect, a section is dedicated to the theoretical and practical aspects of the new regime of consent, which, under the rule of the Regulation, can no longer be tacit. Similarly, attention is paid to problems concerning the obligation to appoint a Data Protection Officer. This obligation implies significant changes in the companies' internal affairs. The final part of the article is dedicated to the systematization of a generally applicable compliance rules, to aid Romanian in their feat of insuring proper respect for Personal Data. The main purpose of the present study is to create a proper practical plan to facilitate the fulfilment, by Romanian businesses, under the Regulation.

Keywords: *GDPR, personal data, consent, Data Protection Officer, operator.*

JEL Classification**:** K22, K23, K29

1. Introductory remarks

To both public and commercial law specialists in the European Union, the entry into force of a Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[2], appears as a turning point in the matter of personal data protection. The Commission's proposal to revaluate the legal provisions governing an area often subject to the attention of the Court of Justice of the European Union was not without criticism or controversy. This is reflected both in the long process and the adoption[3], as well as virulent

[1] George-Cristian Ioan – Faculty of Law, Babeș-Bolyai University, Cluj-Napoca, Romania, georgecristianioan@gmail.com.

[2] Further referenced as, Regulation 2016/679 or The General Regulation for protection of Data (GDPR).

[3] The process of reviewing the personal data protection legislation was started by the Commission in 2009 and formally announced only in 2010. In 2012 the first draft for Regulation 679/2016 was created. Following the release of information on the Commission's efforts in March 2015, the Council took a position, which resulted in a tripartite negotiation between Parliament, the Commission and the Council. The regulation was finally adopted only on 27 March 2016.

criticisms made prior to the adoption of the Regulation[4]. Romanian legal doctrine has aligned with the European trend of awareness of the importance of the proposed changes, including the relevance of the change in the legal nature of the act of codifying the rules on the protection of personal data[5]. The controversial nature was maintained after adoption, and some authors argued that the burdens imposed on companies would be detrimental to the development of the business environment[6]. Although the Regulation is equally applicable to public institutions, the present study will focus on the potential problems that may be encountered in the private sector, given the specificity of legal relationships in commerce, that deserve separate attention.

The general consensus is that the operation of commercial companies and their relations with customers and other participants in the commercial circuit will be deeply affected, starting in May 2018. Changes are necessary in both internal procedures and the external means of negotiation and undertaking of legal obligations. Certainly, in relation to the sanctions provided by the Regulation, which will be analysed *infra*, a proactive conduct of companies is desirable. It must be emphasised that, according the sanctioning system imposed by the Regulation, any sanction applied for violation of regulatory provisions by a Romanian subsidiary of a multinational company will be calculated based on the global turnover figure. The purpose of this article is to analyse the changes brought about by the entry into force of Regulation 679/2016 and how it will change the domestic commercial climate. In the end, we will pursue the development of principles of good commercial practices in the light of Regulation. The utility of the paper results from the lack of a case study on the effect of the Regulation on the internal market. We consider, in this regard, that a correct understanding of the provisions of the Regulation is indispensable at the present time, for Romanian traders.

2. Analysis of the nationally applicable legal framework

However, before we begin to analyse (i) the immediate effect of the Regulation, in relation to its legislative nature and its correlation with changes in the

[4] Jennifer Baker, *Privacy? What privacy? EU's draft law on your data is useless, say digital rights orgs*, „The Register", 4th of March 2015. The document is available online at http://www.theregister.co.uk/2015/03/04/data_protection_what_data_protection proposed_ new_law_is_as_good_as_useless_say_digtal_rights_orgs, consulted on 1.07.2018. In this sense, the open letter set to President Jean Claude Juncker by *European Digital Rights*, and backed up by another 70 international NGOs, including the Romanian Association for Internet and Technology, expresses simillar worries. The document is available for consultation online at: https://edri.org/files/ DP_letter_Juncker_20150421.pdf, consulted on 1.07.2018.

[5] Daniel- Mihail Șandru, *Regimul juridic al protecției datelor cu caracter personal este în proces de regândire*, „Revista Română de Drept al Afacerilor", no.3/2015.

[6] James Brooks, Jr., *Why Europe's Stance on Data Privacy is Bad for Business*, „Huffington Post", 13 September 2017. The document is available for consultation online at the adress https://www.huffingtonpost.com/entry/why-europes-stance-on-data-privacy-is-bad-for business_us_59b98eb5e4b02c642e4a1378, consulted on 1.07.2018.

domestic business market and (ii) its content, we consider that a brief revision of the national legislation currently applicable.

At the present time, the main normative act of primary legislation governing the issue of personal data in Romania is Law no. 190/2018 *on measures implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing of Directive 95/46 / EC (General Data Protection Regulation)*[7]. This is complemented by Law no. 102/2005 *on the establishment, organization and functioning of the National Supervisory Authority for Personal Data Processing*[8]. The secondary legislation, the main administrative acts with normative applicable are, on the one hand, the instructions issued by the Minister of Interior, and on the other, the instructions and decisions of the *National Supervisory Authority for Personal Data Processing* (ANSPDCP), binding for both public institutions and for privates. Such acts are either individual or normative[9]. With regard to purely individual administrative acts, the most important are Authorizations issued by the ANSPDCP Chairman, which authorizes data processing in particular situations. Finally, the optional acts of law explanation are the Opinions and Recommendations.

It has been shown[10] that the principles enshrined in the national legislation largely coincide with those resulting from Directive 95/46/EC, not only with regard to its content, but also with the interpretation given by the Court of Justice of the European Union. These include (i) the immutability of the purpose; (ii) the principle of accuracy; (iii) the right to information and transparency; (iv) the principles of limited proportionality and preservation, and (v) the principle of loyalty, according to which the consent of the data subject is necessary for data processing. It has also been shown that Romanian law enshrines the right to be forgotten[11], which must be seen as a manifestation of openness towards current developments in the field[12].

As to the responsibility for the implementing personal data protection legislation, the National Supervisory Authority for Personal Data Processing was set up by the Law no. 102/2005, precisely for the purpose of taking over these tasks.

Regarding the potential alignment of domestic legislation with the Regulation, two specifications must be made: on the one hand, the legislative immobility is not relevant to the applicability of the EU provisions, given the legal

---

[7] Published in the Official Gazette, Part I, no. 651 of July 26, 2018.

[8] Published in the Official Gazette, Part I, no. 391 of May 9, 2005, as amended.

[9] Marius Petroiu, *Protecţia datelor cu caracter personal în România, prin intermediul atribuţiilor autorităţii naţionale de supraveghere*, „Pandectele Române", no. 9/2012.

[10] Ovidiu Ungureanu, Cornelia Munteanu, *Dreptul la protecţia datelor cu caracter personal, un drept autonom?*, „Revista Română de Drept Privat", no. 1, 2014.

[11] *ibidem.*

[12] In this respect, although at EU level, the exponential decision for the right to be forgotten is Case C-131/12 Google Spain SL and Google Inc. against the Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, as noted in the doctrine, it covers only a small part of what it means to be forgotten, which is much larger and older right. In this sense, Giovanni Sartor, *The right to be forgotten: balancing interests in the flow of time*, in the „*International Journal of Law and IT*", vol. 24, no. 72, 2016, p. 96.

nature of Regulations and their role in the legislative system of The EU. In other words, regardless of the position of the Romanian authorities and their conduct, the Regulation is fully applicable as of the 25th of May 2018, both in respect of them and any other subjects of law. On the other hand, there is no impediment to supplementing the rights provided by the Regulation and extending their applicability as long the legal solutions do not contradict the Regulation. In other words, what is contrary to the Regulation will be inapplicable, but the protection of rights is not limited by the Regulation. The GDPR only sets a minimum standard, in principle. However, it should not be forgotten that any right of the data subject has a correlative obligation on behalf of the controller. Thus, instilling new rights or extending the present ones should be carefully done, so it does not become contrary to the EU legislation.

Concerning remedies, the Romanian legislation stipulates both the possibility of the data subject to repair the damage suffered through the controller's liability, as well as a series of contraventions, enshrined by art. 12-15 of the Law no. 190/2018, between 10000 and 200000 RON.

3. The main changes made by the Regulation to the provisions of Directive no. 95/46/EC

The most important difference stems from the nature of the normative act governing the matter. Regulations are means of law that must be distinguished from Directives, and the most important difference is that they have direct effect[13]. The main features of a Regulation are (i) general applicability, they are applicable to any matter subject to Union law; (ii) full applicability, as they cannot be used in a truncated manner, and (iii) direct applicability in all Member States, as it is not necessary to transpose it into national law to the extent of clarity and unconditional formulation[14]. As such, the first major change in the climate of personal data protection derives from the legal nature of the normative act of union affiliation. The implications of this change were reported early in the legal doctrine[15], pointing out that much of the national legislation will become redundant as the entry into force of the Regulation does not invalidate it, but the European Law provisions will be applied with priority. It has also been shown that the legislative harmonization will be almost complete. One last issue concerns countries where national legislation, following the transposition of Directive 95/46 /EC, offers higher standards of protection than those required by the Regulation. An example in this sense is Germany. In such situations, it is considered that higher standards of protection will

[13] Bruno de Witte, in Paul Craig, Grainne de Burca, *et. al*., *The Evolution of EU Law*, ed. a IIa, Ed. Oxford University Press, 2011, p. 335.

[14] Alina Kaczorowska, *European Union Law*, 3rd ed., Ed. Routledge, 2013, pp. 124-125.

[15] Henri de Waele, *Implications of replacing the Data Protection Directive with a Regulation - a legal perspective*, „Privacy and Data Protection", vol. 12, no.4, 2012, pp.3-5.

be applicable, but only in that State and only to the extent that they do not contravene statutory provisions[16].

However, the most important changes regard the content of the Regulation, as there are substantial changes to the provisions of Directive 95/46/EC. The normative act encompasses eleven chapters and eighty-nine articles. It was underlined[17] that the most important changes concern (i) the establishment of obligations to appoint a Data Protection Representative and a Data Protection Officer; (ii) modification of the consent regime; (iii) express codification of the right to be forgotten; (iv) introduction of the obligation to notify the data subject and the authority of the breach of personal data security; (v) the obligation of transparency with regard to internal data processing procedures; (vi) the introduction of fundamental principles and new rights and (vii) the establishment of a single supervisory authority, with the modification of the sanctions regime.

We will note that there are two kinds of modifications, in principle: on one hand, clear legal texts are created based on the rules deriving from the jurisprudence of the Court of Justice of the European Union. On the other hand, *actual* changes, resulting from the tripartite negotiations, through which obligations and rights resulting from practical needs are added. However, the codification of rules established by the Court's jurisprudence is not superfluous, as important clarifications and explanations are made. The best example of this is the right to be forgotten, where the possibility of restricting access to data is added. This is a necessary nuance that could not be deduced from the solution in *Google Spain*[18]. For a coherent structure of the proposed analysis, this article will first deal with the changes made to the general regime of principles, rights and justifications, and consequently the new organizational obligations imposed on the companies will be achieved.

4. Changes in rights, obligations and justifications

As it has been shown, no significant changes have been made concerning the definitions of personal data, data processing or the controller and the processor. The legislative framework is maintained within the parameters established by Directive 95/46/EC. Some authors have stated, therefore, that despite the contrary perception, the new Regulation does not fundamentally alter the protection of personal data, since, in general, those companies which have made their own internal procedures in good faith of the Directive, will rather have to make minor and surface changes[19]. This is correct and fully applicable to commercial companies operating in Romania. Unfortunately, however, we believe that the number of companies that

[16] *ibidem.*

[17] Sana Khan, *Practitioner's insight into the new EU Data Regulation, „Compliance and Risk Journal”,* vol. 5, no. 1, 2016, pp.7-8.

[18] C-131/12 *Google Spain SL și Google Inc. versus Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*.

[19] David White, Tom Morrison, *Mind the GDPR - Legal Update Data Protection,* „The New Law Journal”, vol. 167, 2017, p. 8.

have voluntarily aligned their procedures with the provisions of the Directive is sufficiently low that they are the exception rather than the rule[20]. However, for a complete perspective, we have to mention that the state of *unpreparedness* is omnipresent at a European level. According to a survey of 400 of the *leading* companies in their fields, only 8% of managers declared themselves ready for the entry into force of the Regulation, with 28% unaware of it. Another 26% said they would not be able to complete their internal measures by May 2018[21].

On the other hand, although the core of the rights of the data subject, controller obligations and justifications are maintained, some essential changes are made. There is an extension of liability concerning the obligations and the direct burden of the data processor. It is only existent, however, to the extent the processor failed to comply with the obligations which its specific obligations or acted in contradiction or otherwise carelessly in regard to the legal instructions given by the controller.

4.1 Consent of the person concerned to the processing

Probably the most important change, unanimously observed at the level of legal doctrine, is that which concerns the rules of consent of the data subject. Differences from Directive 95/46/EC result from the definition of consent provided by the Regulation. Thus, in the common structure of the two definitions, it is established that any manifestation of free, specific, informed and unambiguous agreement for processing of data is a form of valid consent. However, the Regulation added the condition that it be *taken through a statement or unequivocal action*. This seemingly benign and minor change is likely to completely reform the landscape of personal data in the European Union. The immediate effect is clear: the agreement can not be tacit, but only express. It is also added that it is unambiguous, that is, it must be taken in such a way as to leave no room for interpretation as to its content and subject matter. However, the general consensus is that there is no impediment for the declaration of consent to be oral and not necessarily written. However, we consider that such an approach will raise issues concerning proof of consent, which, although not insurmountable, are to be avoided. Tightening the consent regime will raise major issues in a field where controllers already have difficulties in meeting the tasks. According to a study in 2013, less than 17% of the UK's most popular e-commerce platforms were compliant with European law on consent to data

[20] The general consensus in the media is that Romanian companies are not ready for the entry into force of the Regulation. In this respect, Gabriel Munteanu, *the General Data Protection Regulation (GDPR): a Gordian node for Romanian companies and authorities*, „Marketwatch" no. 194/ 2017, Document consulted online at http://www.marketwatch.ro/articol/15639/Regulamentul_privind_Protectia_Generala_a_Datelor_(GDPR)_un_nod_gordian_pentru_companiile_si_autoritatile_romanesti/, consulted on 1.07. 2018. In the same sense, we reference the position held by Ciprian Păun on the Show Legal 100% on June 11, 2017, which can be seen online at the aderess: https://www.youtube.com/watch?v=6qJOMxkfj34, consulted on 1.07.2018.

[21] Richard Curtis, *European businesses unprepared for GDPR*, „Taxation Magazine", vol. 18, no. 4626, November 2017, p. 2.

processing for advertising purposes[22]. One important point to consider is that the Regulation is also applicable to consent obtained before its entry into force[23]. In other words, if the manifestation by the data subject was taken under the old legislation, the provisions of the Regulation are applicable to him. After the 25th of May, 2018, processing of this data will no longer be legal, even if it has been until then. Therefore, consent must, in order to be legalized, be taken again from all the users that have already consented so far. From this finding, a generally valid rule should be noted, namely that any change in the manner and purpose of the processing implies a new consent or confirmation of the original one.

This difference, that is, between simple consent and express consent, was underlined by relevant legal doctrine[24]. It has been shown that while consent, *lato sensu*, can be taken through generic means, where it is implicit, for example *data entered will be used for marketing purposes* followed by an e-mail box, express consent requires an affirmative, clear statement. An example of this might be to require the user to electronically tick a box, which shows that *I agree that my personal data consisting of the email address is used by the company to distribute bulk e-mail advertising material and stored on the controller's internal network.* Starting from this example, we can observe the following: (i) the consent is taken in the form of an affirmative statement; (ii) the data to be processed is indicated; (iii) the purpose and mode of processing are expressly indicated; (iv) is formulated in a clear, easily understandable language by any person. The latter condition is one whose importance needs to be highlighted, since the language in which consent is sought must be adapted to the target audience, especially in cases involving vulnerable groups such as non-native speakers or children. In such cases, it is even necessary to classify the persons concerned and obtain a personalized consent for each target group[25].

Last but not least, one aspect that results from the provisions of the Regulation is that the minimum valid consenting standard is now an *opt-in* consent. The legal doctrine in the matter has shown there are three common ways of obtaining consent in the online environment. The *opt-in* consent is the one in which the user freely chooses the option of accepting the declaration of consent. In the *opt-out* type, which is very common in practice, it is offered the option of refusing to process personal data, assuming the assumption of non-refusal. This method becomes prohibited by the provisions of the Regulation. Another commonly used method, incompatible with the Regulation, as set out in point 32 of the Preamble to the Regulation, is that of pre-selection of the acceptance option, which the user can de-

[22] Maurizio Borghi, Federico Ferretti, *Online data processing consent under EU law: a theoretical framework and empirical evidence from the UK*, „International Journal of Law and IT", Vol. 21, no. 2, p. 153.

[23] David White, Tom Morrison, *Mind the GDPR - Legal Update Data Protection (2)*, „The New Law Journal", vol. 167, 2017, p. 11.

[24] Chantelle Taylor, Reed Smith, *UK regulator's guidance on GDPR consent - is the definition any clearer?*, „Privacy and Data Protection Journal", Vol. 17, no. 5, p. 14.

[25] Peter Given, Matt Harris, *The ICO's new Privacy Notices Code of Practice - a review*, „Privacy and Data Protection Journal", Vol.17, no. 1, p. 8.

register if he so desires. As such, of the above-mentioned examples, only the *opt-in* option is acceptable in the legal regulatory environment. Consequently, it is preferable that any companies that have online platforms that include the ability to identify the user through orders, requests, complaints, bidding and counterfeiting, and *so on* to integrate this system.

In order to ensure predictability for participants to the processing of personal data, the English National Authority, The ICO *(Information Commissioner's Office)* took preventive measures prior to the entry into force of the Regulation[26]. These include the design of a practical guide[27], which includes rules on consent. We consider that, in relation to the legal nature of the Regulation, coupled with the lack of implementing measures in the Union, these rules can provide a useful basis for Romanian traders. The rationale behind this statement is based on two considerations: firstly, there are no obvious shortcomings in the ICO criteria. Secondly, we consider that, until clear positions are adopted by the ANSPDPC or outlined case-law in this respect, in the early stages of the implementation of the Regulation, discussion of compliance with it will often be predictive and diligent. Although, obviously, no Romanian authority is directly held by the ICO's guide, consultation and observance should be sufficient to establish the minimum diligence. In addition, given the overall application of the Regulation, any controller may rely on legitimate expectations deriving from the representation that compliance with a guide drawn up by a supervisory authority in a Member State is sufficient to ensure compliance with the requirements imposed by the Union normative act.

According to this guide, consent to data processing must be dissociated. This condition has, in turn, two valences. Consent must first be taken separately from any other terms and conditions of use of the service. Personal data must be distinguished from any other provisions that must be accepted by the user. Secondly, the use of the service can not be conditional upon obtaining the consent, unless the data processing is absolutely necessary for that service[28]. Also, the manifestation of will must be of the *opt-in* type, as we have shown *above*.

Although there are other, more secure, methods of obtaining consent, such as electronic signatures or handwriting, the imposition of such an obligation could lead to a paralysis of the commercial circuit. It is considered that *opt-in* is a sufficient and good practice. The consent must be granular. That is to say, where appropriate, the user must consent separately for different types of processing or processing

---

[26] The Regulation will affect, the data protection approach in the United Kingdom, even after Brexit, as the position of the ICO seems to be in the sense of not reversing the standards imposed by the Regulation, regardless of the political situation. In this regard, https://www.privacylaws. com/Publications/enews/UK-E-news/Dates/20171/7/ICO-wants-a-strong-international-presence-regardless-of- Brexit/, consulted on February 10, 2018.

[27] Information Commissioner's Office, *Consultation: GDPR consent guidance*, published on 2 March 2017, Document consulted online at https://ico.org.uk/media/about-the-ico/consultations /2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf/, consulted on February 10, 2018.

[28] Eduardo Ustaran, Hogan Lovells, *EU General Data Protection Regulation: things you should know*, „Privacy & Data Protection Journal", vol. 16, no. 3, 2016, p. 3.

purposes, with the freedom to choose between what they accept and what they refuse[29]. A particularly relevant example, especially in the field of advertising, where special consent is required, is profiling[30]. In such situations, the user should have part of an explanation, in simple terms, concerning what the type of profiling is and what the methods used are[31]. For example, in the case of *cross-device profiling*, it should be shown that by accepting, the data can be used to identify the devices the data subject uses, implicitly identifying the approximate location of the target person under certain conditions. In the declaration of consent, the controller who will process the data must be expressly appointed, as well as any other third party who will have access to, or will play, another role in their taking over, including in the course of exchanges of commercial information for purposes advertising. Consent should not be taken in conditions where there is an imbalance in power. In other words, when the person depends on the controller, he attention must be given to the way in which consent will be taken. The most obvious example is that of employers. When an employer asks for something, it can be presumed that the employee has is, at the very least, in a relationship of relative dependence, derived from the hierarchical work structure. In such situations, I consider that the best method to insure that this rule is respected is to expressly mention that the data subject is under no obligation to give consent and will not suffer any negative consequences in the case of a refusal.

The last point to be considered is one of the most important. Explicit character also implies respect for the right to be informed, because there is a near symbiotic interdependence between it and proper consent. The right to be informed must be seen as an extension of consent beyond the moment of its taking. It implies not only that the person is correctly, but also fully informed, because some omitted aspects can completely change the person's decision[32]. As such, the information obligation pre-exists and at the same time goes beyond mere consent. However, for the right to information to gain effectiveness, it is necessary, *inter alia*, that a person can easily withdraw their consent at will. The right of withdrawal, also recognized under Directive 95/46/EC, is absolute[33]. The controller may not refuse it to the data

[29] Chantelle Taylor, Reed Smith, *op.cit*., p. 15.

[30] This operation is defined by the Working Group in the Recommendation Document on the Essential Elements of a Definitions and a Profiling provision in the EU Data Protection Regulation 2013 as any form of automatic processing of personal data, analysis or prediction of behavior or certain personal aspects relating to a natural person, especially in the case of a person's health, situation, performance at work, personal preferences or interests, reliability or behavior, location or movements.

[31] Bridget Treacy, James Henderson, *Cross device profiling — ensuring compliance*, „Data Protection Ireland", vol. 8, no. 3, 2015, p. 10.

[32] Roger Brownsword, *Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality*, in Serge Gutwirth, *et.al*., *Reinventing Data Protection?*, Ed. Springer, 2009, p.100.

[33] Relevan legal doctrine has shown that the right to the protection of personal data is a relative one, Gloria González Fuster. Raphaël Gellert, *The fundamental right of data protection in the European Union: in search of an uncharted right*, in the International Review of Law, Computers & Technology, Vol. 26, No.1, p. 77. The statement made must be interpreted in this context. The

subject. However, this idea can be nuanced. On the one hand, we consider that personal data could nevertheless be further processed in so far as we are in the presence of any of the justifications provided by art. 6 of the Regulation. On the other hand, as any other right, absolute or relative, the right of withdrawal can be abusively exercised. Although in such cases the data, in absence of a legal justification, processing must be terminated. The controller could, however turn against the data subject in order to recover any pecuniary prejudice. In addition, the means of withdrawal of consent provided by the controller to the person concerned must be easy to use and easily accessible. The statement that the acceptance of processing can be revoked at any time should also be mentioned in the prior information. In addition to this, the withdrawal method used by a particular controller should (i) be expressly acknowledged at the time of acceptance and (ii) be public.

A final important point is for the controller to create a database in which to keep track of declarations of acceptance of data processing. Evidence should include at least the following four points: (i) identification of the person who consented to the processing; (ii) date and time of processing (with the highest possible accuracy); (iii) mentions concerning which method the statement was obtained and (iv) what the exact purpose for use is.

There are also special rules for minors, which the Regulation provides expressly. Without attempting an exhaustive analysis of these, we believe that some mention is required. If the person concerned is a child under the age of 16, such processing is lawful only if and to the extent that such consent is granted or authorized by the holder of parental responsibility for the child. It is further added that a practitioner must make every reasonable effort to verify in such cases that the holder of parental responsibility has granted or authorized consent, taking into account the available technologies. The issue raised in the doctrine concerns the lack of legal criteria to understand the *reasonable efforts* to be made. It noted in that regard that according to US law, such a method could be *age gating*[34]. However, the question remains open as to what solutions might be found to ensure the compliance of the parent or guardian's approval. Among the methods used, based on American law, are the request for bank card data or even the identification of the parent through a selfie, although obviously this method raises issues of biometric data protection[35].

5. The obligation to appoint a Data Protection Officer

With the entry into force of the Regulation, the obligation to appoint a Data Protection Officer[36] becomes effective. Imposing this obligation s one of the most perceptible changes. The concept of a DPO is not a new one, as it was recommended

premise that the right of withdrawal exists in a concrete situation is that the right to the protection of personal data is applicable. If applicable, there is no justification for refusing to withdraw.

[34] Laura Scaife, *The GDPR and consent - A matter of child's play?*, „Compliance and Risk Journal", vol. 5, no. 5, 2016, p. 7.

[35] *ibidem*.

[36] Hereinafter, DPO.

but not mandatory under Directive 95/46/ EC. However, some countries, such as France or Germany, have opted for a higher degree of protection than the minimum required by the Directive, expressly codifying a legal obligation to appoint a responsible person and before the entry into force of Regulation[37]. This change was not without controversy. Among other things, it has been shown that the number of practitioners with expertise in personal data is insufficient in relation to the needs of the market and that the only real possibility for companies to fulfil their obligations is to resort to *outsourcing*[38]. According to a study, over 75,000 data protection officers will have to be employed worldwide[39].

Appointing a DPO is mandatory in three situations, although Member States may impose this obligation in other cases as well. At present, there is no manifestation from the Romanian authorities in the sense that they would seek to extend the minimum protection provided by the Regulation in this respect. Thus, appointment is mandatory for the controller and the processor where: (i) processing is carried out by a public authority or body, with the exception of courts acting in their judicial role; (ii) the principal activities of the controller or of the person in charge of the controller consist of processing operations which, by their nature, scope and/or purposes, require regular and systematic monitoring of the large-scale targeted persons; or (iii) the main activities of the controller or the processor by the controller consist scale processing of special categories of data referred to in Articles 9 and 10. It should be noted, however, that when an organization will opt voluntarily for the appointment of a responsible, although the law does not compel him, rules Art 37-39 of the Regulation are applicable to said controller[40].

The main questions arising from these definitions concern the notions of *main activity*, *large scale* and *periodic and systematic monitoring*. The first notion refers to the operations necessary to achieve the social or lucrative purpose of the controller or processor. The concept does not exclude situations where data processing is logically interlinked to the nature of the controller's business. For example, although a hospital would not be able to function without data processing, it remains a major activity. However, where processing is an adjoining activity necessary for the operation of any organization in general, such as the use of bank accounts for the payment of wages, it does not fall under the notion[41]. The notion of *large scale*, however, remains volatile enough to not be explicitly defined. Consequently, this will need to be considered *in concreto*, on a case by case analysis. Finally, monitoring is *periodic* when it is continuous for certain periods of

[37] Katalina Bateman, *GDPR series: The role of the DPO — overcoming a GDPR hurdle*, „Privacy and Data Protection Journal", vol.17, no. 5, 2017, p. 9.
[38] Rezzan Huseyin, *Explosion in requirement for DPOs*, „Privacy and Data Protection Journal", vol. 12, no. 5, 2012, pp. 17-18.
[39] Rita Heimes, Sam Pfeifle, *Study: GDPR's global reach to require at least 75,000 DPOs worldwide*, Document consulted online at https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/, consulted on February 10, 2018.
[40] Article 29 Working Party, *Guideline on Data Protection Officers*, p. 5.
[41] *idem*, p.7.

time or repeated at specified and *systematic* intervals when organized, follows a specific method, is part of a data or strategic data collection program. In addition to profiling, which is mentioned expressly in the statement of reasons, determining location by applications, health status through devices or telecommunications services are forms of monitoring.

A problem that arises, however, concerns the professional qualities of the designated person. It was noted that although a minimum standard should be established, it is only after a factual analysis that it can be determined what the necessary capabilities are. They must be adapted in each case. The diligence requirements for the controller or designated person will differ from a smaller company that performs small-scale processing to a large one. Also, the resources made available to the representative, in order to comply with the obligation stipulated by art. 38 (1) will differ[42]. One thing to remember, however, is that the Regulation does not impose the need for a specific professional qualification. An already engaged person may be appointed as responsible if: (i) the existing duties do not interfere with the responsibilities imposed by the Regulation or the law; and (ii) there is no conflict of interest with the pre-existing duties. In such a situation, the manager will practically act *part-time* on two positions, having to determine how long he should allocate to each type of task. Employing a new person or outsourcing are alternatives, as we have shown *above*. However, regardless of the choice chosen, the DPO answers directly to the highest level of management of the controller or processor. Legal doctrine has pointed to the fact that, *de facto*, this obligation is not feasible, as it is excessive. For example, in a large company, it is unreasonable for the CEO to handle tasks of the DPO, directly[43]. Also, regardless of the chosen variant, the provisions of art. 38 (3) are applicable. Even in the case of outsourcing, the service contract could not be discontinued to fulfil the responsibilities of the DPO, even if many of his findings are inconvenient or lead to the need for additional unwanted expenses.

One important thing to remember is that even if the responsibilities of the DPO are added to those an employee already has, he/she has independence as to the manner in which he conducts his obligations concerning supervising data protection. They can not be forced to interpret the law, in a certain manner. About responsibility, it should be noted and remembered that DPO is not personally liable, for violation of the company's legal provisions regarding personal data. Responsibility remains societal in such a situation , which is deduced from the art. 24 (1)[44]. Two conclusions must be drawn, referring to the architecture of responsibility in Romanian law. The injured person will not have a choice between going against the controller or the DPO. A right of regress of the controller should not be excluded in the case of a DPO's culpable fault, as he does not have a legal cause of exclusion of liability. Thus, the DPO is responsible for errors in their own

[42] Anita Bapat, James Henderson, *The role of the DPO - what you need to know*, „Privacy and Data Protection Journal", vol. 16, no. 8, 2016, p. 16.
[43] Katalina Bateman, *op.cit.*, p. 10.
[44] Article 29 Working Party, *Guideline on Data Protection Officers*, p. 7.

activities. In any case, its liability for errors by the controller's mistaken implementation of the DPO's proposals or by failing to comply with them.

In general, the responsibilities of the DPO can be summarized in two categories: (i) advice and (ii) relationship with the supervisor. The first category involves informing the controller about its obligations and monitoring the activity, reporting violations, finding and proposing solutions. It also has a fundamental role to play in the impact assessment on data protection. As regards the supervisory authority, the contact person will be the contact point, with contact details communicated to it.

A practical model was proposed for choosing the best option for appointing the responsible person[45]. First of all, the company bodies should consider whether they fall into one of the situations provided by art. 37 of the Regulation. Then he should proceed to the appointment of the person in charge to whom the DPO will report and to which person he will answer. Next, the budget for ensuring the protection of personal data should be established, according to which the best option is to be established between (i) hiring a new person; (ii) the appointment of an employee, possibly reducing the already assigned tasks, so that he can also exercise his / her basic function and the role of responsible or (iii) outsourcing. It has been shown that, prior to appointment, an audit of personal data should be carried out, as a result of which the future responsible should be solved. Finally, the contractual conditions, depending on the chosen option, should be established between (i) a contract of employment; (ii) an addendum to the employment contract, or (iii) a service contract.

6. Obligation to carry out impact assessment on data protection

The Regulation requires that if a type of processing, in particular that based on the use of new technologies, is likely to create a high risk for the rights and freedoms of individuals, the controller must, before beginning to process personal data, carry out an impact assessment of the processing operations. In this field, the provisions are unitary and do not raise big questions. The evaluation mustn't necessarily comply with any formal requirements[46]. In addition to the exemplary situations referred to in paragraph 35(3), other situations in which this obligation exists are: *individual profiling , automatic decision-making systems of legal value (for example, when analysing the formal admissibility of a request addressed to a public authority), systematic monitoring of sensitive or vulnerable subject matter, innovative technologies, data exchanges outside the Union or where processing in itself prevents the data subject from exercising his right or from using a service or*

[45] Monica Salgado, *DPOs - top ten tips for making better appointments*, „Privacy and data protection Journal", vol. 14, no. 2, 2013, p. 10.

[46] Samantha Sayers, Kayleigh Clark, *GDPR series: Demystifying DPIAs*, „Data Protection Ireland", vol. 10, no. 4, p. 11.

contract[47]. It was suggested that the notion of a *high risk*, although evaluated on a case by case analysis, should be understood as any situation in which at least two of the above-mentioned situations are fulfilled[48]. It has also been shown that employee monitoring, whether video, audio or other means such as *time slots*, is a form of high-risk processing[49].

The ways in which the assessment is to be carried out are difficult to analyse from an abstract point of view, as the EU legislator left a wide margin of flexibility, as each controller is able to adapt its methodology to its needs. What is essential, however, is that it contains the elements provided by art. 36 (7). It has been argued that a good evaluation must (i) determine what data is being processed and what the purpose of the processing is; (ii) identify the mishaps with the applicable legal framework and determine the degree of risk for data security and the sanction for each violation; and (iii) propose a methodology for solving the problems raised[50]. It should be noted, however, that the controller can use both the assistance of the DPO and the National Authority to determine the necessity and content of the assessment. Another aspect worth mentioning is that in accordance with art. 35(4), the Authority shall draw up and publish a list of the types of processing operations subject to the requirement to carry out a data protection impact assessment, thus giving added legal certainty to the system.

We concur with the argument that in the absence of clear criteria on the methodology or the form of evaluations, they will be effective only to the extent that they will be adapted to each individual controller, making it undesirable that evaluations become simple *bureaucratic* exercises, consisting of standardized reports from the controller to the controller[51]. As such, national authorities should only proceed in extreme cases to censoring formal assessments, focusing primarily on their merits.

7. Developing a model to meet the requirements imposed by the Regulation in the case of indigenous companies

The fact that the Regulation, although often seen as restrictive, leaves a wide margin of discretion with regard to the internal implementation methodology, which must be transparent, leads to the conclusion that it is impossible to predefine a perfect, universal template, that can satisfy the needs of all controllers. However, a set of common rules can be formulated. There have been many attempts, both from

---

[47] Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, 4th of April, 2017, p. 7.

[48] *idem*, p.11.

[49] Ibrahim Hasan, *In Practice: Legal Update: Data Protection: GDPR and employee surveillance*, „Law Society Gazette", no. 28, 31 July 2017.

[50] James Clark, *GDPR series: building a compliance programme*, „Data Protection Ireland", vol. 10, no. 1, 2017, p. 8.

[51] Stephanie Pritchett, *Data Protection Impact Assessments: look before you leap*, „Data Protection Ireland", vol. 5, no. 5, 2012, p. 13.

practitioners and theorists, to establish some general reference points for the development of internal procedures. By synthesizing and corroborating these positions, but referring to the specificities of the Romanian commercial environment and the way in which the personal data is perceived at the national level, we propose the following guidelines, which we believe can structure the development of compatible internal and external procedures with Regulation. We will mention that although it has been stated that a holistic approach is the only one that can really satisfy the needs of the modern society in the matter of personal data[52], without denying this point, to which we agree, we consider that, in relation to the position adopted by the EU legislator in the Regulation, each potential issue must be considered separately. Note also that in the light of Regulation how data is managed is as important as not leaking data with meeting data subjects' expectations[53].

The first change that is required is the most difficult. It will not be further analysed in this article, as it does not concern the legal field, but it is undoubtedly worth mentioning. In order to properly respect the legislation, the mentalities concerning personal data must be changed. Its importance should be actually acknowledged. This change has to start from the leaders of companies.

Article 24 can makes it clear that the Regulation promotes the need for *data protection by design*, the concept that data protection should be the implicit mode of operation of a company[54]. The question arises as to how the controller can apply appropriate technical and organizational measures and then ensure that they operate *on the autopilot.* The conceptual approach has been shown to be the following: (i) setting personal data protection goals; (ii) determining the methods by which the goal can be achieved; (iii) choosing the right method[55].

The first step in starting the alignment procedure with the Regulation should be to conduct an internal audit[56]. Its purpose is to clarify the current state of data protection in society. As a result, at least the following should be established: (i) what kind of data the company processes and for what purpose; (ii) in which categories these data falls; (iii) what data subjects are there and whether they are part of a vulnerable category (iv) what kinds of data is process; (v) how, where and by whom is it stored and what safeguards exist; (vi) what form of consent has been given until then; (vii) which data are really useful to the business, as unnecessary ones can be deleted; (vii) what data is encrypted or anonymized. The list is not exhaustive.

Secondly, the organization must determine whether it has the legal obligation to appoint a Data Protection Officer. The rules outlined *above* apply in this respect. However, irrespective of the existence of the obligation, it must be determined which person in the management of the company will oversee the

---

[52] Samson Y. Esaya, *The idea of 'emergent properties' in data privacy: Towards a holistic approach*, „International Journal of Law & Information Technology", vol. 25, p. 148- 151 and 177- 178.

[53] Kate Brimsted, *GDPR series: accountability - a blueprint for GDPR compliance*, „Privacy and Data Protection Journal", vol. 17, no. 3, p. 12.

[54] Stefano Varotto, *The European General Data Protection Regulation and its potential impact on businesses: some critical notes on the strengthened regime of accountability and the new sanctions*, „Communications Law", vol. 20, no. 3, 2015, p.79.

[55] *Idem*, pp. 80-81.

[56] Sana Khan, *op. cit.*, p. 8.

compliance procedures. Also, in the absence of the controller, it should be determined which department will take over the tasks in the field. Even if, in the first instance, these tasks fall *ipso facto* under the responsibility of the legal department, we consider that two adjacent measures are required. On the one hand, as it has been shown, compliance with the Regulation requires a collaboration structured on a relationship of interdependence between several departments of a company[57]. Consequently, *de minimis*, the means of liaison between lawyers and IT professionals must be established. We consider that it should include consultation hours, clear internal regulations and mutual warning systems in the event of difficulties or irregularities. The concepts also apply to the appointment of a representative, since internal regulations or service orders must clearly establish relations between them and the legal and IT departments.

Furthermore, the governing bodies or the legal department should codify specific procedures for the protection of personal data. In this respect, a bivalent approach has been proposed, structured on internal procedures and external relations procedures[58]. The approach must be based on the rights of the data subject. Starting from the express rights set out in the Regulation, a set of specific procedures should be implemented, including conditions for requests, deadlines and settlement options, should any of these rights be exercised. Regarding the internal procedures, it is necessary to establish rules on: (i) procedures by which employees can check their processed data, according to art. 13 of the Regulation; (ii) the arrangements for resolving claims for the right of rectification, erasure and forfeiture, from employees or former employees; (iii) the arrangements for the release of data under the right of portability; (iv) the conditions for realising employee profiling, including by announcing them and presenting evaluation algorithms; (v) the Response Plan in the event of a breach of security, including the procedure of notifying the data subject and the National Authority[59].

With regard to external relations, the principle on should be presenting information and policies on data. They should be available to clients and business partners, including information on how their data will be processed and by whom, together with the conditions in which they can exercise their rights in relations with society. It has been shown that they should at least include: (i) the purposes for which data is processed; (ii) the legal basis on account of which it is processed; (iii) the right of withdrawal of consent; (iv) which are the external, state or private bodies that will have contact with the data; in this regard, express consent must be given; (v) information on the rights that the data subject has, with their express indication (*eg*. portability, deletion, correction), indicating the procedures for resolving applications; (vi) the conditions for profiling and the presentation of algorithms; (vii) estimated retention time of data; (viii) the notification procedure[60]. It is advisable to have these procedures written in a simple language to make them easy to

---

[57] Monica Salgado, *How to build a GDPR programme - a multidisciplinary approach*, „Data Protection Ireland", vol. 9, no. 4, 2016, p. 13.

[58] Ann Bevitt, *GDPR series: Creating and reviewing data protection policies Part 1: Internal-facing policies*, „Data Protection Ireland", vol. 10, no. 5, p. 7.

[59] *Idem*, pp. 7-9.

[60] Ann Bevitt, *GDPR series: Creating and reviewing data protection policies Part 2: External-facing policies*, „Data Protection Ireland", vol. 10, no. 5, p. 7.

understand. At the same time, access to these processing policies should be easy, through the site, where they can be highlighted by the font or web page layout[61]. As for *cookies,* there must be changes since, as the consent, the purpose of using the *cookie* must be indicated. It has been proposed to divide these obligations into the following categories: Essential, Functional, Analysis / Performance, Oriented / Advertising and Social Media , with an indication of the processing mode and a brief description of each purpose[62].

Regarding the relations of the company with the natural persons concerned and the rest of the participants in the commercial circuit, we consider that it is necessary to add contractual clauses /additional acts to the concluded contracts, with the modification of the adhesion contract template in this respect. The introduction of clauses should be treated similarly to unusual clauses, signed in their own right or reiterated at the end of the contract. However, it was pointed out that in the case of employment contracts, the use of additional contracts would be preferable, thus underlining that the clause is not a forced one[63]. Concerning consent, we refer to the explanations *above*.

Regarding the relationship between the controller and the processor, it was shown that the following aspects should be considered when drawing up the contract : (i) express mention of the fact that the processor will only process the data indicated by the controller, as instructed; (ii) the establishment of data protection mechanisms and deadlines and conditions for notification of the controller of any breaches; (iii) the establishment of data security safeguards, including security testing deadlines at regular intervals; (iv) the obligation to archive and keep track of the data processed and the purposes of the processing; (v) establishing the liability regime, given that any clauses excluding the controller's liability will probably be hardly accepted by the processor[64].

8. Conclusions

Certainly, starting with the moment the Regulation becomes effective, the commercial environment will be faced with the need to make changes. Although the sanctions tend to be presented as the centrepieces of the Regulation, a Damocles' sword, standing above the operator, it is difficult to admit that they applied at their peak points. The purpose of the Regulation remains one of protection, from our point of view. The dissuasive aspect of sanctions should be seen as a mean of ensuring data protection, not an end in itself. Indeed, genuine data protection, in line with the Regulation, requires important investment. However, we believe that for companies that do not process a large quantity of data, the investment will not be a financial one, but one of time spent with the purpose of understanding the Regulation and finding the best solutions.

---

[61] *Ibidem.*

[62] *Ibidem.*

[63] Ann Bevitt, Chris Stack, *Preparing for the GDPR - advice for employers*, „Privacy and Data Protection Journal", vol. 16, no. 6, p. 12.

[64] Rob Corbet, *Data protection clauses in contracts - adapting to the GDPR*, „Privacy and Data Protection Journal", vol. 16, no. 6, 2016, pp. 9-10.

In this respect, we believe that the best way to ensure that the Regulation is respected is to give due consideration to personal data. It should not be regarded as an accessory, and its protection should be seen civic obligations in the collective mentality, rather than a mere sterile and excessive legal obligation. Today, personal data ceases to be a simple mean of identification. It is a currency, a source of profit. This source of profit, however, involves more or less incisive intervention in the personal lives of the individuals concerned. As such, we consider that strict regulation of the processing is a judicious solution. We believe that an universal solution for compliance cannot be found, since Regulation in itself is based on the idea of *data protection by design*. However, we consider that the rules outlined in the final section of this study establish a basis (i) from which developing a system of protection can be constructed, for large controllers; (ii) sufficient, with minimal adjustments, for the controller who routinely processes data in a relatively small quantity, without using it for unusual purposes.

Bibliography

1. Bruno de Witte, in Paul Craig, Grainne de Burca, *et. al*., *The Evolution of EU Law*, 2nd ed., Ed. Oxford University Press, 2011.
2. Chantelle Taylor, Reed Smith, *UK regulator's guidance on GDPR consent - is the definition any clearer?*, „Privacy and Data Protection Journal", Vol. 17, no. 5.
3. Daniel- Mihail Șandru, *Regimul juridic al protecţiei datelor cu caracter personal este în proces de regândire*, „Revista Română de Drept al Afacerilor", no. 3/2015.
4. Eduardo Ustaran, Hogan Lovells, *EU General Data Protection Regulation: things you should know*, „Privacy & Data Protection Journal", vol. 16, no. 3, 2016.
5. Henri de Waele, *Implications of replacing the Data Protection Directive with a Regulation - a legal perspective*, „Privacy and Data Protection", vol. 12, no. 4, 2012.
6. Ibrahim Hasan, *In Practice: Legal Update: Data Protection: GDPR and employee surveillance*, „Law Society Gazette", no. 28, 31 July 2017.
7. James Clark, *GDPR series: building a compliance programme*, „Data Protection Ireland", vol. 10, no. 1, 2017.
8. Katalina Bateman, *GDPR series: The role of the DPO - overcoming a GDPR hurdle*, „Privacy and Data Protection Journal", vol. 17, no. 5, 2017.
9. Maurizio Borghi, Federico Ferretti, *Online data processing consent under EU law: a theoretical framework and empirical evidence from the UK*, „International Journal of Law and IT", Vol. 21, no. 2.
10. Ovidiu Ungureanu, Cornelia Munteanu, *Dreptul la protecția datelor cu caracter personal, un drept autonom?*, *„Revista Română de Drept Privat"*, no. 1, 2014.
11. Roger Brownsword, *Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality*, in Serge Gutwirth, *et.al*., *Reinventing Data Protection?*, Ed. Springer, 2009.
12. Sana Khan, *Practitioner's insight into the new EU Data Regulation*, „Compliance and Risk Journal", vol. 5, no. 1, 2016.
13. Stefano Varotto, *The European General Data Protection Regulation and its potential impact on businesses: some critical notes on the strengthened regime of accountability and the new sanctions*, „Communications Law", vol. 20, no. 3, 2015.