THE EU DATA PROTECTION REFORM - ANALYSIS OF THE NEWLY PROPOSED PROVISIONS AND THE IMPACT ON THE ROMANIAN DATA PROTECTION AUTHORITY

VALENTINA PAVEL BURLOIU,
L.LM Law and Technology graduate, Tilburg University, Tilburg, The Netherlands, valentina.pavel@gmail.com

DANA UDUDEC
Legal Adviser, ududecd@ecpi.ro

Abstract

In the context of today's technological advancements, the online environment poses a new set of privacy and data protection challenges, thus making users more vulnerable in the virtual space. With the aim of ensuring sufficient safeguards and minimizing privacy risks, EUlegislators are trying to keep up to date with the speed of developments and reform the 17-years old data protection legal framework.

In this sense, the European Commission recently proposed a data protection Regulation[1] which would have direct effect upon the national legal framework of EU Member States. Consequently, this would imply a substantial effort on behalf of each of the 27 countries to realign their data protection laws with the new European standards and make sure that their National Data Protection Authorities (NDPRs) are functioning in compliance with the Draft Regulation.

Having in mind the possible adoption of this legislative piece, the thrust of this paper relates to the changes the proposed Regulation would bring to the existing national laws on data protection and the impact the draft Regulation would have on the Romanian Data Protection Authority (RDPA).

Keywords: *data protection reform, proposal, privacy, regulation, Romanian Data Protection Authority*

1. Introduction

On the 25th of January 2012, the European Commission published a proposal to reform the 1995 data protection framework[2].

The aim of the proposal is to adapt data protection and the related privacy rights to the fast-developing online environment and encourage the growth of the European digital market. The newly drafted European data protection rules comprise of two legislative texts, namely a regulation and a directive. The new Regulation aims at

[1] 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 of the free movement of such data (General Data Protection Regulation), 25.01.2012, hereinafter the "Draft Regulation".

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, hereinafter the "Directive 95/46/EC".

building "more trust in online services"[3] by empowering users with stronger rights related to consent and by redirecting the control of their personal information into their own hands. As for the new Directive, it deals with general data protection rules in relation to law enforcement and judicial cooperation on criminal matters.

This paper focuses only on the text of the Draft Regulation as proposed by the European Commission on 25 January 2012, leaving out any remarks regarding the draft Directive and references concerning the revisions that recently took place[4]. The first section familiarizes the reader with the context of the Draft Regulation and provides a general overview of the most important newly proposed rights. The second section analyzes the implications the Draft Regulation will have concerning the Romanian DPA and addresses the necessary functional and structural changes. Last, the paper ends with a set of conclusions.

2. The context of the Draft Regulation and general overview of newly proposed rights

The Commission's proposal on a legal reform was welcomed by the other EU bodies as an ambitious attempt to modernize the EU data protection legislation. Being directly applicable in all Member States, there will be a single set of rules that will apply to all data controllers and processors, which consequently seem to benefit from a much more solid and harmonized regulatory approach.However, the initiative has also been received with considerable criticism. The European Data Protection Supervisor (EDPS) considers that the reform does not reach its goal of being comprehensive, since the rules regarding data processing by the EU bodies are still part of a different document (Regulation no 45/2001) and also because data processing in law enforcement falls within the scope of a different type of binding act, a directive.[5] Furthermore, some areas of data processing[6] were left unreformed. Another broadly expressed concern[7] has to do with the high number of delegate acts[8] that the Commission is empowered to adopt, which could possibly bring legal uncertainty and slowing down of the Regulation's implementation process.

[3] European Commission, EU Justice Commissioner Viviane Reding, *'Data protection: strengthening your online rights'* (25 January 2012) <http://ec.europa.eu/unitedkingdom/press/frontpage/2012/12_07_en.htm> (date of access 25 October 2012).

[4] The objects of the recent revision were articles 1-10 and 80(a) and 83.

[5] EDPS opinion on the data protection reform package, 7 March 2012 (hereinafter "the EDPS opinion")

[6] For example, specific acts in the area of police and judicial cooperation in criminal matters or Common Foreign and Security Policy.

[7] As uttered by the EDPS in the aforementioned opinion, by the Article 29 Working Party in Opinion 01/2012 on the data protection reform proposals, and by almost all the delegates in the DAPIX meetings of 23-34 February and 14-15 March 2012.

[8] Delegate acts are based on Article 290 of the Treaty on the Functioning of the European Union and represent and act of delegating to the Commission the power to adopt non-legislative acts of general application to supplement or amend certain non-essential elements of the legislative act in which it is mentioned.

The Draft Regulation is nevertheless engaged in a process of continuous debate and re-shaping. In fact, a leaked version[9] of the Commission's proposal published in January 2012 contains the revision of the Council of the European Union. The revision of the Commission's Draft Regulation was made following the DAPIX meetings of 23-34 February and 14-15 March 2012 and presented on June 22nd 2012.

As for the current situation of the legislative proposal, according to the DAPIX notice of the meeting's provisional agenda [10] from 31 October 2012, the draft Regulation is still under debate between the Member States, the European Commission and the Cyprus Presidency of the Council of the European Union. In addition, until the end of the year 2012, Jan Philipp Albrecht (the European Parliament's Rapporteur on Data Regulation) will present his draft report concerning the Regulation proposal. Negotiations between the European Parliament and the Council (the co-legislators) are envisaged to commence during 2013[11].

The Draft Regulation seeks to reinforce users' information control by introducing new specific privacy provisions[12]. In this respect, Article 15 introduces the right to an easier access by granting individuals the possibility to ask the data controller at any time whether their personal data is being processed; furthermore, paragraph (1) lists all the information a controller has to provide to the data subject[13]. Additionally, users are given the right to rectify any incorrect information related to them[14].

With few exceptions, Article 17 introduces the right to be forgotten and to erasure. Although not an absolute right, the right to be forgotten gives individuals the power to have their information permanently deleted from social media sites and bank databases. [15] Moreover, Article 17 paragraph (2) introduces the obligation for controllers to inform third parties about the data subjects' request to erase links, copies or replications of the processed data [16] and the same paragraph mentions that the controller is liable for the third party publication of data when the data subject authorized the data processing. Interestingly, Article 29 Working Party 191 expressed that the way the right to be forgotten and the right to erasure are constructed is in contradiction to the reality in which the internet functions.[17] Additionally, Article 29

[9] The Council of the European Union revised the draft regulations issued by the Commission and a leaked version of the document can be consulted here: http://www.gov.im/lib/docs/odps//council_euro_union_revised_regs_2206.pdf

[10] Council of the European Union Communication (31 October 2012) <http://www.parlament.gv.at/PAKT/EU/XXIV/EU/09/63/EU_96317/imfname_10381020.pdf>

[11] Working Document of the European Parliament, LIBE Committee, 6 July 2012 <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-491.322%2b01%2bDOC%2bPDF%2bV0%2f%2fEN>

[12] Articles 15 to 19 of the Draft Regulation.

[13] Article 15 of the Draft Regulation.

[14] Article 16 of the Draft Regulation.

[15] EurActiv, InfoSociety, 'Reding unveils new EU data protection rules' (25 January 2012) <http://www.euractiv.com/infosociety/reding-unveils-new-eu-data-protection-rules-news-510381> (date of access 25 October 2012)

[16] Article 26 (2) (f) of the Draft Regulation.

[17] Article 29 Data Protection Working Party, Opinion 1/2012 on the data protection reform proposals, WP 191, pg. 13, hereinafter "Working Party 191".

Working Party 199 listed the criteria and conditions which need to supplement the provisions of the Draft Regulation, namely regarding different sectors and specific data protection situations, deleting links, copies or replications of personal data and the rules for Article 17 (4). However, it also underlined that although it is appropriate to deal with these provisions in a delegated act, this legally binding act should be adopted simultaneously with the Draft Regulation.[18]

Another reform regards the individuals' possibility to move their data from a service provider to any other internet company. Awarding stronger control over personal data, Article 18 (1) and (2) state the obligation for data controllers to provide a copy of the data which is being processed and the possibility for data subjects to easily retransmit that data to another controller[19]. Thus, the Draft Regulation introduces the principle of data portability[20].Since data portability involves the development of certain standards, a commonality of all services will need to be agreed upon, to ensure that data portability is seen by everyone in the same way, but it will also mean that there will be certain elements that cannot be ported. Yet, a clarifying position regarding data portability is to be expected before the adoption of this proposal.

Additionally, Articles 19 and 20 of the Draft Regulation set forth the right to object and profiling. With limited exceptions, this means that users will be able at any time to object to their data being processed and to oppose to having their data collected and used for direct marketing purposes.[21] Furthermore, Article 20 details the safeguards put in place against the automated processing of data. In respect of profiling, Working Party 191 asks for further clarification regarding the extent to which this right gains application. [22] As to the enforcement of this right, operators who intentionally or negligently violate the provisions against profiling are subject to a substantial fine.[23] Additionally, the provisions of the e-privacy Directive still remain applicable[24], which means that consent needs to be obtained for online targeted advertisement and e-mail marketing.[25]

Another important aspect extensively referred to in the Draft Regulation is in relation to consent. Article 4 (8) and Article 7 specify consent must be given in a direct and explicit matter and several recitals refer to specific requirements to be considered when involving children (such as clear and easy understandable text when asking for consent)[26]. Among others, Recital 25 gives further details the ways consent could be

[18] Article 29 Data Protection Working Party, Opinion 8/2012 providing further input on the data protection reform discussion, WP 199, pg. 22, hereinafter "Working Party 199"

[19] Recital 55 of the Draft Regulation gives as an example the possibility to transmit the data from a social network site to another.

[20] Article 18 of the Draft Regulation. European Commission, 'How does the data protection reform strengthen citizens' rights?' <http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf> (date of access 25 October 2012)

[21] Article 19 and Recital 57 of the Draft Regulation.

[22] Opinion 1/2012 on the data protection reform proposals, WP 191, pg. 14.

[23] Article 79 (6) (d) of the Draft Regulation.

[24] As stated by Article 89 of the Draft Regulation.

[25] Opinion 1/2012 on the data protection reform proposals, WP 191, pg. 14.

[26] Among others, Recitals 29, 38, 46 make reference to specific measures when children are involved.

given "including by ticking a box when visiting an Internet website"and Recital 32 specifies that the burden of proof is on the data controller. The only exceptions that can be made relate to the legitimate basis Member States could establish according to Recital 31. Regarding the issue of consent, Working Party 199 fears that specifying the mechanism and conditions of obtaining verifiable consent might have as consequences inflexibility and distancing from the technology neutral principle.[27] Furthermore, Working Party 199 warns that by awarding Member States the possibility to separately intervene regarding the issue of consent there will be less chances to achieve a harmonized application of the Draft Regulation; and consequently leading to a situation nonconforming with the aim of the proposed Regulation.[28] Working Party 199 also draws attention to the fact that the Commission will draft specific rules for micro, small and medium size enterprises (MSMEs) regarding consent[29]; given the rationale of assuring a high degree of protection, particularly when children are involved, the Working Party finds this aspect unusual. As a matter of fact, as it is constantly stressed throughout the Opinion of the Working Party, if exemptions are not already included in the wording of the Draft Regulation, a delegated act cannot introduce further restrictions. Therefore, the Commission needs to clearly decide upon the conditions for MSMEs before the possible adoption of this Regulation since there will be no possibility to include future limitations via a delegated act.[30]

In relation to the issue of consent, the Draft Regulation establishes the principle of fairness and transparency, meaning that the notifications and the communication with data controllers should be in a clear and easy-understandable manner and the results of the data subject's actions should be openly stated and understood[31]. The data subject should be able to understand when and how data is collected, by whom and with what purposes. Furthermore, Recital 49 instructs that the data subject should also be informed about "how long the data will be stored, the existence of the right of access, rectification or erasure and the right to lodge a complaint". The same Recital also mentions the importance of understanding the consequences of the data subject refusal of not providing the requested data. As Recital 51 explains, the Draft Regulation strengthens the data subject's position in relation to the data controllers by giving the possibility to verify the legality of their data being processed[32].

Furthermore, one notes the possible major impact of the personal data breach notification introduced in Articles 31 and 32. The controller is obliged to inform both the relevant authority and the data subject without undue delay about the event of a security breach that involves its personal information. In the same manner, processors

[27] Opinion 8/2012 providing further input on the data protection reform discussion, WP 199, pg. 15.
[28] *Idem*.
[29] Article 8 (3) of the Draft Regulation.
[30] Opinion 8/2012 providing further input on the data protection reform discussion, WP 199, pg. (among others) 15, 17, 24.
[31] Recital 46 of the Draft Regulation
[32] Recital 51 of the Draft Regulation: "Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, for what period, which recipients receive the data, what is the logic of the data that are undergoing the processing and what might be, at least when based on profiling, the consequences of such processing."

have the obligation to immediately notify the controller after the acknowledgment of a data breach. Furthermore, controllers and processors need to pay extra attention to breaches seriously damaging the privacy of the data subject such as: identity theft or fraud, physical harm, significant humiliation or damage to reputation[33].Additionally, it has been clarified that in the event of data "accidentally or unlawfully destroyed, lost, altered, accessed by or disclosed to unauthorized persons", where feasible, the notification must be sent within 24 hours. Moreover, Article 30 (2) and Recital 66 mention as a prevention and security strategy mechanism that controllers and processors should firstly perform risk evaluations and, based on this analysis, take the next step of implementing the correct security measures. Working Party 191 has made several comments regarding the unrealistic 24-hour notice and the notification of minor security breaches, which would place unnecessary administrative burdens both on the controllers and on the data protection authorities.[34] Also, given the importance of the obligation to notify security breaches, Working Party 199 urges for clarity regarding what consists a personal data breach and for providing further explanations regarding the data breach notification in the actual text of the Draft Regulation and not in a separate act.[35]

A notable aspect is the introduction of direct liability regime for data processors[36]. Therefore, Article 77 of the Regulation indemnifies "any person who has suffered damage as a result of an unlawful processing operation" to receive compensation from the data controller, from the data processor or from both of them.[37] Moreover, it is important to underline that Recital 17 and Article 2 (3) of the Draft Regulation specify that "this Regulation should be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive".Therefore, both legislative texts represent a source of liability triggers; however the particularities of each Member State's application of Directive 2000/31/EC liability regime remain to be followed up and connected to the provisions of the Draft Regulation.

Equally important is the fact that the Draft Regulation eliminates the general obligation to notify the processing of personal data but introduces the obligation for controllers and processors to conduct an impact assessment "which should include in particular the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with this Regulation"[38]. Moreover, in sensitive data processing operations which involve a considerable amount of risks, this impact assessment should be made in consultation with the Data Protection Authority[39] which should have the appropriate expertise in such a matter.

[33] Recital 67 of the Draft Regulation.

[34] Opinion 1/2012 on the data protection reform proposals, WP 191, pg. 16

[35] *Idem*, pg. 29 and 30.

[36] Article 77 of the Draft Regulation.

[37] Additionally, in relation to business to business relationships, the Draft Regulation acknowledges binding corporate rules and drafts the minimum set of requirements they should contain. Particularly, Article 43 (2) (f) specifies that liability rules must be included in the policy.

[38] Recital 70 and Article 33 of the Draft Regulation.

[39] Article 33 (2) (e) and Recital 73 of the Draft Regulation.

In the series of new provisions introduced by the Draft Regulation, there is also the "one-stop-shop"[40] principle for business. As Article 51 and Recital 98 set forth, companies will only have to deal with a single data protection authority, the supervisory authority of the Member State in which the controller or processor has its main establishment. Furthermore, Recital 19 explains that the Draft Regulation is applicable regardless if the processing takes place within or outside the Union and that the determination of the company's establishment should be done considering the "effective and real exercise of activity through stable arrangements"[41]. Recital 27 reinforces the idea that the processing of personal data does not actually have to be carried out at the location of the establishment and explicitly states that "the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment".

The fifth chapter of the Draft Regulation stipulates the rules on the transfer of personal data to third countries or international organizations. These provisions seek to provide clear rules for international data transfers and make exchanges of information more secure.[42] The same chapter explicitly mentions binding corporate rules (BCR) as another instrument that will provide data controllers and processors with certain flexibility while strengthening the protection of individual rights and freedoms.[43] Therefore it should be stressed out that BCR would become legally binding for companies. In connection to this, Working Party 199 mentions that it will be among the attribution of the NDPA to approve the BCR; hence the Working Party fears that the independent status of the NDPA in relation to the EDPA might be affected because of the delegated acts concerning the requirements for approving the BCR.[44] Working Party 191 further expresses the fact that neither the Regulation nor the Directive deal with "the collection and transfer of data by private parties or non-law enforcement public authorities that are in fact intended for law enforcement purposes, as well as the subsequent use of these data by law enforcement authorities."[45]

Last, the establishment of rules regarding the data protection officer represents another important reform brought forth by the Draft Regulation. Article 35 specifies that companies with more than 250 employees will have to appoint a data protection officer who would have to assist the controller or the processor in monitoring the compliance of the organization with the Draft Regulation[46]. Moreover, Article 35 states

[40] Article 51 of the Draft Regulation.

[41] Recital 19 of the Draft Regulation.

[42] European Commission, Vice-President of the European Commission, EU Justice Commissioner Viviane Reding, 'The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age'(22 January 2012) SPEECH/12/26 <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26> (date of access 25 October 2012)

[43] Cloud Computing Hearing with Telecommunication and Web Hosting Industry, pg. 5 and Rohan, M. and others, National Law Review, 'Proposals for Reform of the Data Protection Regime and Binding Corporate Rules' (31 January 2012) <http://www.natlawreview.com/article/proposals-reform-data-protection-regime-and-binding-corporate-rules> (date of access 25 October 2012)

[44] Opinion 8/2012 providing further input on the data protection reform discussion, WP 199, pg. 37.

[45] Opinion 1/2012 on the data protection reform proposals, WP 191, pg. 5.

[46] Recital 75 of the Draft Regulation.

the fact that this obligation is directly targeted to public institutions but also to large private enterprises and companies which deal with "regular and systematic monitoring"[47] of processing operations.

3. How does the Draft Regulation envision the role and functioning of the NDPA?

If the Draft Regulation would be adopted, it would have considerable effects on the organization and functioning of National Data Protection Authorities and there is a number of supplemental mechanisms to be taken into account on a national level[48], when drafting a new law on the establishment, organization and functioning of the NDPA, or amending the existing one. For example, in the process of applying the Regulation, the States are encouraged to take into consideration the "specific needs of micro, small and medium-sized enterprises". Since the Draft Regulation provides a considerable number of reforms[49] concerning the functioning of NDPAs, for this section of the paper, we will focus primarily on the new provisions regarding the principle of complete independence and the cooperation mechanism.

Directive 95/46/CE instructed each Member State to provide one or more public authorities for monitoring and applying its provisions[50]. Consequently, Romanian Law no. 677/2001[51] for transposing the Directive stipulates in Article 21 that "Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal" (hereinafter "ANSPDCP" or "the RDPA") shall be the Supervisory Authority. Its establishment, organization and functioning are enshrined in Law no. 102/2005[52] that reiterates and expands on the general principles of the 1995 Directive, providing also administrative and procedural details regarding the RDPA.

Similarly, the Draft Regulation reserves an important space for provisions regarding the supervisory authorities[53]. Noting the positive aspects of the Commission's Regulation proposal with regard to the NDPAs, the Article 29 Data Protection Working Party considers that the document provides "for strengthened independence and powers, including administrative fines and the obligation to be consulted on legislative

[47] Recital 75 of the Draft Regulation.

[48] Indeed, both Recital 92 and Article 46 of the Draft Regulation stipulate that Member States establish one or more supervisory authorities which are responsible for the monitoring and application of the Regulation. Consequently, Member States must adopt a new legal framework for the establishment, functioning and organization of their NDPAs or amend the existing one.

[49] Other reforms refer to: the abolishment of the general notification obligation, considered to be an "administrative and financial burden" that did not "in all cases contribute to improving the protection of personal data" according to Recital 70; increasing the powers conferred upon the NDPA, including the power to administrative offences; increasing the duties of the NDPA, including that of conducting awareness activities among the general public addressing the risks, rules, safeguards and rights related to the processing of personal data; the power vested upon national authorities to apply administrative fines.

[50] Directive 95/46/CE, Chapter VI, article 28, pg. 1.

[51] Published initially in the Official Bulletin of Romania, Part I, no. 790 of 12 December 2001.

[52] Published initially in the Official Bulletin of Romania, Part I, no. 391 of 9 May 2005.

[53] The entire Chapter VI is entitled "Independent Supervisory Authorities" and lays down a series of principles, some of which are based on the Directive of 1995, but laid down in a more detailed manner.

measures, and provisions to ensure harmonized application and where necessary enforcement of the law, especially through the <<consistency mechanism>>"[54].

At the present moment, the core principle for the functioning of the NDPAs is ***complete independence***. However, the 1995 Directive does not elaborate on this principle set out in Article 28, leaving Member States to draw up national rules that would define and safeguard their NDPA's independence. This type of provision has brought two cases before the Court of Justice of the European Union (hereinafter "the Court"), where States were considered to have failed to fulfill their obligation under Article 28. In **Germany**[55], the monitoring of the processing of personal data outside the public sector at the level of the different *Länder* was subject to State (Federal) oversight, as opposed to the regional authorities monitoring the processing of such data in the public sector (by public bodies) who were solely responsible to their respective Parliament. The Commission and the EDPS supported the opinion that "complete independence" means "that a supervising authority must be free from any influence, whether that influence is exercised by other authorities or outside the administration"[56]. Reaffirming that Directive 95/46/EC indeed does not define the phrase, the Court also expressed the need to take into account the usual meaning of the words. Consequently, "In relation to a public body, the term 'independence' normally means a status which ensures that the body concerned can act completely freely, without taking any instructions or being put under any pressure."[57] The Court went on by stressing that the independence is "complete", meaning that it outlaws direct and indirect influence on the decision-making powers of the Authority. Thus, the principle of "complete independence" enshrined in Article 28 requires that the authorities and their decisions should be "above all suspicion of partiality"[58]. In the case of **Austria**[59], the managing member of the DSK (the Austrian DPA) is also a member of the Federal Chancellery, who is actually a federal officer, bound to follow instructions given by superiors. Moreover, the DSK is integrated with the departments of the Federal Chancellery, from which it receives its necessary equipment and staff and the Federal Chancellor has an unconditional right to be informed of all aspects related to the work of the DSK. All of these features of the Austrian DPA were dubbed by the Court to be in contradiction with the principle of "complete independence".

To sum up, the Court interpreted Article 28 from a negative point of view, exposing what "complete independence" does *not* mean: direct or indirect control exercised by another body, either by means of hierarchical supervision or staff and budgetary management. Following these two cases of failure to comply with European legislation, we will look at the content of the Draft Regulation and identify the new

[54] Opinion 01/2012 on the data protection reform proposals, WP 191.

[55] Case C518/07, Action under Article 226 EC for failure to fulfill obligations, brought on 22 November 2007.

[56] *Idem*, pg. 15.

[57] *Idem*, pg. 18.

[58] *Idem,* pg. 36.

[59] Case C614/10, Action under Article 258 TFEU for failure to fulfill obligations, brought on 22 December 2010.

provisions regarding the principle of "complete independence" and their effect on the RDPA's functioning.

The legal reform on data protection sheds a clearer light on the meaning of an independent supervisory authority, since the entire Section 1 of Chapter VI in the Draft Regulation (Articles 46-50) is entitled "Independent Status". Some of the new provisions are inspired by Regulation (EC) no. 45/2001[60], stating that members of the supervisory authority "neither seek nor take instruction from anybody", that they "refrain from any action incompatible with their function" and, after their term of office, they shall behave "with integrity and discretion as regards the acceptance of appointments and benefits"[61].

Further on, Article 47 paragraph 7 of the Draft Regulation refers to the financial dimension of the independence[62], stating that the authority is "subject to financial control which shall not affect its independence" and that Member States shall ensure separate annual budgets for the functioning of the authorities. Unfortunately, the draft European norm does not address the question of what types of financial control affect or do not affect an authority's independence. In addition, regarding the Member States' obligation under the Draft Regulation to provide the supervisory authority with the adequate human, technical and financial resources, Working Party 191 considers that an assessment should be made in order to determine how many resources does a data protection authority actually need in order to function properly[63].

In the case of Romania, the RDPA has its own budget, which is included in the state budget [64] adopted by Parliament. Theoretically, the provisions of Law no. 102/2005 safeguard the financial independence of the RDPA, since the authority, while consulting with the Government, adopt its own budget and forward it to the Government, to be included in the national budget. The Ministry of Public Finance is entitled to modify the draft budget and, if the RDPA's President does not agree with the changes, he/she can bring objections before the Parliament.

The appointment [65] of an authority's member is an important part of its independence, as stated by the Court of Justice of the European Union in the case of Austria, mentioned above. However, Article 48 of the Draft Regulation provides that members of the NDPA will be appointed either by the Parliament of by the

[60] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, published in the Official Journal of the European Communities, 12.1.2001, L8/2.

[61] *See also* Article 44 of Regulation (EC) no. 45/2001.

[62] Also reinforced by Recital 94 of the Draft Regulation.

[63] Article 29 Working Party, Opinion 01/2012 on the data protection reform proposals, WP 191, pg. 17.

[64] Financial provisions are regarding the authority are stated in Law no. 102/2005 on the Establishment, Organization and Functioning of the National Supervisory Authority for Personal Data Processing, in Article 17.

[65] Recital 95 of the Draft Regulation also states that: *The general conditions for the members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members should be either appointed by the parliament or the government of the Member State, and include rules on the personal qualification of the members and the position of those members.*

Government of the Member State. This provision appears to be in contradiction with the Court's judgment, where the Austrian authority was found not to be independent, especially because its managing member was, at the same time, a federal officer who was under the supervision of a hierarchical superior from the Federal Chancellery. However, it should be considered that the Court did not rule against the procedure of appointing the members of the Austrian DPA (which is done by the Federal President of the Republic, after receiving a proposal from the government), but against the hierarchical relationship between the managing member and the Federal supervisor. In the context of such provisions, the significance of the act of appointment should be carefully examined, in order to safeguard the independence of the authority. Does the appointed member continue his/her relationship with the appointing authority (e. g. supervision, reporting, informing)? Does this relationship violate the principle of independence? What criteria should a potential member meet in order to be appointed - are they just related to the experience of the person, or do they also concern being member of a political party or being supported by one? Such questions might be considered when drafting national laws that shall apply Article 48 on the general conditions for the members of the supervisory authority. In addition, Working Party 191 commented on the draft provisions, expressing its view that the members of the NDPAs could also be appointed by other independent bodies.[66]

As opposed to other NDPAs[67], the Romanian authority is not a collegiate body and does not exercise power as an administrative court. The RDPA is run by a President, assisted by a Vice President, both appointed by Senate for a mandate of 5 years that can be renewed only once. Among other criteria for eligibility, candidates must be politically independent. However, the entire procedure of appointment implies that the candidates are proposed by the Permanent Office of the Senate, based on the recommendations set forth by Parliamentary Groups of both Chambers of Parliament. Consequently, although the President or Vice-President of the RDPA might not be politically engaged during their mandate, they were appointed based on the support received from the group of MPs, which does not necessarily rule out a *de facto* influence stemming from a political party.

Apart from the aforementioned reforms, out attention was also drawn towards the new Co-operation and Consistency [68] provisions set up in the Draft Regulation, especially the *mutual assistance* and the *joint operations of supervisory authorities*. These mechanisms conform to the reality that personal data moves across borders, thus stronger cooperation between data protection authorities is needed in order to reduce the risks of personal information disclosures and take effective measures when such disclosure has taken place[69]. This type of cooperation occurs when a data subject's rights have been violated in more than one Member State, and it consists of information requests and supervisory measures solicited by one authority to another. The NDPA must conform to the request of assistance within one month; otherwise, the

[66] Opinion 01/2012 on the data protection reform proposals, WP 191, pg. 17.
[67] For example, the Austrian or Danish authorities.
[68] Chapter VII, Articles 55-72.
[69] Recital 91 of the Draft Regulation.

requesting authority shall be competent to take provisional measures themselves on the territory of the non-responsive NDPA and submit the matter to the European Data Protection Board[70].

Such a cooperation mechanism represents an important step forward to a better protection of data subject's rights, if the violation occurs in several member states. However, there are certain issues that should be further taken into consideration by both the European legislators, when adopting the final text of the Regulation, and the Romanian legislators, when framing laws that ensure the correct and effective application of the Regulation. For example, the one month deadline for answering the assistance request might not be enough, considering the complexity of arising violation cases and the resources available to the requested NDPA. Furthermore, the EDPS shows its concern towards using the co-operation mechanism without impeding on national sovereignty[71], and Working Party 191 stresses the need to consider financial and human resources as an important factor for the proper functioning of the cooperation mechanism[72].

Considering the new technological developments that have drawn the European legislators towards reforming the data protection framework, it would be impossible to envisage an effective national data protection authority that does not have the proper expertise in the field of information technology (IT). It is our belief that in a context that requires interdisciplinary and cooperation between legal and technology experts, the NDPAs should benefit from legal and financial measures that encourage them to set up special departments or teams of IT experts. Otherwise, it would be difficult to fully exercise investigative powers in cases where the technology used for data disclosure remains beyond the understanding of the NDPA. In this sense, the Romanian Data Protection Authority does not feature an IT department in its organizational structure[73], and information regarding the number of IT experts available in the institution is not disclosed to the public. Consequently, we consider it desirable that, in the light of the data protection reform, the Romanian DPA should be provided with adequate budgetary resources and should set up a department of IT experts, in order to strengthen its role in applying the Draft Regulation.

4. Conclusion

In conclusion, if the Draft Regulation is adopted, data controllers will have to put in place mechanisms that will ensure the effective use of rights and give timely and motivated responses to requests concerning the data subject's access to data, rectification, erasure and the exercise of the right to object[74].Moreover, controllers

[70]As envisioned by the Draft Regulation in Recital 110, the European Data Protection Board would replace the Article 29 Working Party and would be formed by a head of a supervisory authority of each Member State and of the European Data Protection Supervisor.

[71] Opinion of the EDPS, 7 March 2012, pg. 243.

[72] Idem Opinion 01/2012 on the data protection reform proposals, WP 191, pg. 19.

[73] *See* the Annex of the Regulation on the organization and functioning of the National Supervisory Authority for Personal Data Processing of 2 November 2005, subsequently modified by Decision no 5/2011.

[74] Recital 47 of the Draft Regulation.

should be able to demonstrate compliance with the provisions of the text and implement the measures enlisted by the Draft Regulation in order to be able to prove it. Undoubtedly, there is a series of open questions regarding the correct implementation and performance of such verification mechanisms and audit trails which call upon the Commission's delegated acts to disperse the uncertainties in this matter.

At the same time, Romania needs to make the necessary efforts in order to accommodate this possible new Regulation and to put in place a series of complementary processes which will assure the correct implementation and efficient application of its provisions. This includes modifying existing legislation or setting up new laws that empower the Romanian Data Protection Authority to fully exercise its roles granted by the Draft Regulation, in complete independence, as well as allocating the necessary budgetary resources to ensure that its functioning shall be effective.