Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals

Paul De Hert [a,b], *Vagelis Papakonstantinou* [a,c]

[a] *Free University of Brussels (VUB-LSTS), Belgium*
[b] *Tilburg University (Tilt), Netherlands*
[c] *International Hellenic University, Greece*

Keywords:
EU Data Protection Directive
EU General Data Protection Regulation
Individual consent
DPIAs
The right to be forgotten
Data portability
Personal data breach notifications

ABSTRACT

The recent release by the European Commission of the first drafts for the amendment of the EU data protection regulatory framework is the culmination of a consulting and preparation process that lasted more than two years. At the same time, it opens up a law-making process that is intended to take at least as much time. The Commission has undertaken the herculean task to amend the whole EU data protection edifice, through the introduction of a General Data Protection Regulation, intended to replace the EU Data Protection Directive 95/46/EC, and a Police and Criminal Justice Data Protection Directive, intended to replace the Framework Decision 2008/977/JHA. This paper shall focus at the replacement of the EU Data Protection Directive by the draft General Data Protection Regulation. Due to the fact that the draft Regulation is a long (and ambitious) text, a selection has been made, with the aim of highlighting its treatment of basic data protection principles and elements, in order to identify merits and shortcomings for the general data protection purposes.

1. Introduction – setting the scene

The recent release by the European Commission of the first drafts for the amendment of the EU data protection regulatory framework is the culmination of a consulting and preparation process that lasted more than two years. At the same time, it opens up a law-making process that is intended to take at least as much time. This time sacrifice is not unjustified.[1] The stakes are high, because the Commission intends to replace nothing less than the entire EU data protection edifice. This herculean task shall be carried out by two instruments released simultaneously: the General Data Protection Regulation[2], intended to replace the EU Data Protection Directive 95/46/EC[3] and the Police and Criminal Justice Data Protection Directive[4] intended

[1] Or, for the same purposes, uncommon; the EU Data Protection Directive itself took more than five years in the making.
[2] See European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25.01.2012, COM(2012) 11 final.
[3] 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 pp.0031–0050.
[4] See European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 25.01.2012, COM(2012) 10 final, (named, as per its previously leaked version, the "Police and Criminal Justice Data Protection Directive")."

0267-3649/$ – see front matter
doi:10.1016/j.clsr.2012.01.011

to replace the Framework Decision 2008/977/JHA.[5] The latter has a short history and its replacement is perhaps more of a semantic rather than of substantial value. The replacement of the Directive, however, is an important and far-reaching development; once finalized, the new instrument is expected to affect the way Europeans work and live together.

This paper shall only focus at the replacement of the EU Data Protection Directive (the "Directive") by the draft General Data Protection Regulation, as recently released by the Commission (the "Regulation"). The EU Data Protection Directive is the basic EU data protection instrument. It incorporates the regulatory model and guiding principles that over the years have come to denote the EU data protection approach. Notwithstanding the by now extinct EU Pillar system that restricted its scope, in practice it is to its provisions that all intra-EU data protection regulatory texts,[6] and several other texts of various legal statuses released at national or international level,[7] refer to directly or indirectly. In practice, the Directive has by now become the international data protection metric against which data protection adequacy is measured.

The basic elements and principles of the Directive have a history of more than forty years, long preceding its introduction. In fact, they have remained the same since the introduction of the first data protection act, in the German federal state of Hesse in 1970. Subsequently they were incorporated in all data protection acts at Member State level, until their adoption, and formalization, in the text of the Directive in 1995.

The essence of EU data protection edifice remains straightforward. A certain type of personal data processing is identified and separated from all other intrusions into private life. A specialized legal system is subsequently applied to it, complete with custom-made definitions and actors. A set of principles describe how the processing is to take place and a special processing-specific set of rights is afforded to individuals. Finally, a dedicated enforcement mechanism monitors the application of all of the above.

The above legal system, although devised in the 1960s and 1970s, has fared relatively well until today, despite the grave changes that affected both its structural elements (processing technologies and actors) and the legal and political environment within which it had to operate.

As far as the technology of personal data processing is concerned, the above legal system was designed at an age when the number of computing equipment and processing operations was expected to be finite, traceable and identifiable.[8] This approach is best illustrated in the requirement for notification and its underlying idea that personal data processing operations may be counted and organized in a centrally kept national registry. In addition, distinguishing among processing actors has by now become an increasingly difficult task to accomplish: rather than the 1970s perception of an identifiable and single-jurisdiction data controller, at best assisted by an equally identifiable data processor, nowadays the norm is for multiple, multitasking, "cloud-residing" or "outsourced" processing actors, with complex task and liabilities partitioning among them.

On the other hand, Member State implementations at times varied considerably. Although the Directive was introduced exactly in order to address national law differences back in the late 1980s, that impeded the free flow of data in the Internal Market, it appears that it ultimately did not achieve the desired harmonisation effect.[9]

The Lisbon Treaty, once ratified, abolished the Pillar system, and Art. 16 of the TFEU formally turned the right to data protection into a separate fundamental right, distinct from the right to privacy. The opportunity thus finally came for a rework on the EU data protection model in order to address shortcomings of the past and make better use of the newly acquired legal status.

The amendment process of the Directive began as early as in 2009. After a public consultation, the Commission released a relevant Communication in late 2010.[10] Subsequently, all major participants in the process (the Council,[11] the Parliament,[12] the EDPS[13] and the Art. 29 Working Party[14]) published

[5] Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters.

[6] For instance, the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (the ePrivacy Directive), or even the Framework Decision 2008/977/JHA (on the latter, see Paul de Hert and Vagelis Papakonstantinou, "The Data Protection Framework Decision of 27 November 2008) regarding police and judicial co-operation in criminal matters - A modest achievement however not the improvement some have hoped for," *Computer Law & Security Review* 25 (2009): 406. Reference to the Directive's model and principles may also be found in the Schengen, Eurojust, and Europol regulations or in the Eurodac system, as well as, in the PNR exchange agreements between the EU and third countries (USA, Australia, Canada).

[7] See for instance the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, together with its Additional Protocol.

[8] See also the EDPS Opinion, 2, Tene O, Privacy: The new generations, *International Data Privacy Law*, 2011, Vol. 1 No. 1, pp.15–27.

[9] See the Explanatory Memorandum in the Regulation draft, par. 3.2.

[10] As initiated by the European Commission in late 2010; See, European Commission, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, *A comprehensive approach on personal data protection in the European Union*, COM(2010) 609 final, 4.11.2010 (the "Commission Communication").

[11] See Council conclusions on the Communication from the Commission to the European Parliament and the Council – A comprehensive approach on personal data protection in the European Union, 3071st Justice and Home Affairs Council meeting Brussels, 24 and 25 February 2011 (the "Council Conclusions").

[12] See European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Working Document (1 and 2) on a comprehensive approach on personal data protection in the European Union, 15.03.2011 (the "EP Working Document").

[13] See Opinion of 14 January 2011 on the Communication from the Commission on "A comprehensive approach on personal data protection in the European Union" (the "EDPS Opinion").

[14] See Letter from the Article 29 Working Party addressed to Vice-President Reding regarding the Article 29 WP's reaction to the Commission Communication "A comprehensive approach to personal data protection in the EU", 14.01.2011 (the "Art. 29 Working Party Letter").

their views, both on the Commission Communication and with regard to their own standpoint on the possible amendments for the Directive. Altogether, this documentation creates the institutional and theoretical environment that led to the draft Regulation examined in this paper.

The draft Regulation is admittedly a long (and ambitious) text, that cannot be elaborated in full within the limits of this paper. Necessarily, a selection has been made in the analysis that follows, on the basis of highlighting the draft Regulation's treatment of those basic principles and elements that underlie the whole EU data protection edifice – even in this case, however, the approach shall be of a broader, strategic, nature rather than an actual wording assessment, in order to identify merits and shortcomings for the general data protection purposes.[15]

2. A Regulation for general processing; a Directive for police and justice processing

The release of a Regulation, rather than a new Directive, to replace the EU Data Protection Directive probably took the data protection community by surprise – apart perhaps from the EDPS.[16] However, this ought not be an unexpected development: the Commission in its Communication highlighted emphatically the difficulties for EU data protection that were caused by the lack of harmonisation among Member States.[17] Admittedly, these difficulties mostly concern data controllers, who under the Directive have to face a complex environment of legal uncertainty even for data transfers among Member States.[18] The fragmentation among Member State legislations, however, could also hurt individuals while protecting their data processed within the EU. It was to this end that a Regulation, rather than a new Directive, is suggested by the Commission, as a more suitable instrument to resolve harmonisation problems among EU Member States.[19]

The Commission's choice for a Regulation to replace Directive 95/46/EC contrasts with its choice for a Directive to replace the 2008/977/JHA Framework Decision. We believe this approach does not bring the same beneficial effect as far as their scope of protection is concerned. The Commission had two law-making options at hand while amending the EU data protection framework[20]: either to replace both the Directive and the Framework Decision with a single, comprehensive data protection instrument, or to amend each one of them appropriately within the post-Lisbon Treaty environment. Its decision to follow the second solution may be clear and realistic, but it essentially builds upon an increasingly elusive distinction: that between general and commercial data processing, on the one hand, and security-related personal data processing, on the other.

This distinction, that is maintained in the reform,[21] has proven over the years to be schematic and artificial. Today, datasets that are created by private data controllers for their own purposes may be accessed at some future point by law enforcement agencies. The opposite is not inconceivable too.[22] Case law provides very little assistance to this end.[23] The distinction in scope between the two instruments is therefore extremely difficult, if not impossible, to make. By insisting on two separate instruments for each type of processing, the Commission risks to prolong ambiguity in the field each time law enforcement agencies and the private sector interact.

3. Personal data and sensitive personal data (Art. 4 and 9 of the Regulation)

The question, what constitutes "*personal data*", is evidently critical while establishing whether data protection legislation is applicable. In order for a certain processing operation to be regulated by the Directive (or the draft Regulation, for the

[15] Admittedly, adopting a data subject's point of view; business implications(particularly cost considerations for small businesses) shall not be considered in this paper.

[16] The EDPS suggested the release of a Regulation particularly in order to achieve harmonisation among Member States (see EDPS Opinion, p.15).

[17] See Commission Communication, 2.2.

[18] See Commission Communication, ibid, and draft Regulation, 2.

[19] "*A Regulation is considered to be the most appropriate legal instrument to define the framework for the protection of personal data in the Union. The direct applicability of a Regulation in accordance with Article 288 TFEU will reduce legal fragmentation and provide greater legal certainty by introducing a harmonised set of core rules, improving the protection of fundamental rights of individuals and contributing to the functioning of the Internal Market*" (Draft Regulation, 3.1.).

[20] On this issue see, for instance, of the Commission Communication par. 2.3, the Council Conclusions ("*the notion of a comprehensive approach to data protection does not necessarily exclude specific rules for data protection for police and judicial cooperation in criminal matters within this comprehensive protection scheme and encourages the Commission to propose a new legal framework taking due account of the specificities of this area; certain limitations have to be set regarding the rights of individuals in the specific context in a harmonised and balanced way, when necessary and proportionate and taking into account the legitimate goals pursued by law enforcement authorities in combating crime and maintaining public security*", 4), the EDPS Opinion par. 3.1, as well as, European Parliament's Committee on Civil Liberties, Justice and Home Affairs, *Towards a New EU Legal Framework for Data Protection and Privacy*, November 2011, chapter 4.2.3.

[21] In practice, the draft Regulation in its Article 2.2 excludes from its scope national security processing as well as processing "*for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties*" – the latter to be regulated by the Police and Criminal Justice Data Protection Directive. In this way, the draft Regulation does little to extend the scope of the Data Protection Directive that it intends to replace. The Directive's scope excludes "*processing operations concerning public security, defense, state security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law*" (Art. 3.2).

[22] See, for instance, Article 14 of the Framework Decision.

[23] For instance, Passenger Name Records (PNR) processing was found security-related, despite of the fact that data are collected by airline carriers for commercial purposes (see, for instance, Vagelis Papakonstantinou and Paul de Hert, "The PNR Agreement and Transatlantic anti-Terrorism co-Operation: no Firm Human Rights Framework on either Side of the Atlantic," *Common Market Law Review* 46 (2009): 885–919.). On the other hand, the retention of telecommunications data, equally collected by telecommunications providers for commercial purposes, has been judged as commercial processing (as established by the ECJ in its Case C-301/06, Ireland v. Parliament and Council).

same purposes) it needs to indeed relate to personal information.[24] The wording of the draft Regulation repeats that of the Directive: "'*personal data*' *means any information relating to a data subject*".[25] Further guidance is provided in its Recitals, whereby specific mention is made to location data and internet-related data such as IP addresses or cookies' identifiers.[26] All of the above are to expressly constitute "*personal data*" within the meaning of the draft Regulation. In this way, the Commission provides much-needed clarity as to how exactly personal data may "*relate*" to an individual within the contemporary processing environment.[27] IP addresses, RFID tags or behavioural advertising profiles are all noted examples of identifiable individuals despite the lack of an apparent connection. By referring explicitly to the above cases, the Commission seems to agree with the, admittedly extensive, Article 29 Party approach on this matter, as expressed as early as in 2007.[28]

The Directive's distinction between common and "*special categories of*" (sensitive) personal data is maintained in the draft Regulation. It is actually there that reasons for concern may be traced. As is also the case in the Directive, "*personal data*" are subsequently distinguished into common and sensitive, whereby more relaxed conditions apply to the processing of the former, while the processing of the latter is in principle prohibited, only to be allowed exceptionally. Sensitive personal data pertain to such aspects of private life as religion, political and philosophical beliefs, sex life or criminal records, but of course the listing is restrictive – no new categories of data have been added to it over the last fifteen years. This proved problematic in two ways: first, the listing did not expressly include new but important data as genetic information.[29] Also, processing-intensive methods have blurred the above distinction: for instance, by processing meal preferences or surnames of passengers one may incur information as to their religion, nationality or health, and therefore derive what is, in effect, sensitive data from the processing of, otherwise, common personal data.

The Commission chose to address only the first of the above issues in its draft Regulation. In particular, a number of category-specific personal data definitions are provided under its definitions: "*genetic data*", "*biometric data*", and "*data concerning health*". These are all[30] included under the draft Regulation's Article 9 that caters for sensitive data. Notwithstanding the merits of their wording, these additions are expected to add clarity to the field and also to demonstrate the Commission's decisiveness to bring the relevant processing under data protection regulations.

Reasons for concern therefore are mostly focused on sensitive data that are derived from the processing of common personal data. Such information may be inferred by using new, intensive data-processing techniques. The Commission needs to acknowledge such processing and to explicitly place it under the draft Regulation's Article 9 scope. In addition, the Commission could clarify what happens in cases of databases including both types of data.

A final point, perhaps of semantic value, pertains to the Commission's decision to include three new health-related definitions in the draft Regulation: genetic data, biometric data and data concerning health. This choice risks appearing inexplicable – after all, "*genetic data*" is *prima facie* clearer than "*religion or beliefs*". By doing so, the draft Regulation appears perhaps health-sector nuanced, while this is not part of its role (specialized legislation, as in the electronic communications field would be preferable).

4. The actors: "*controllers*", "*processors*" and "*subjects*" (Art. 4 of the Regulation)

The traditional scheme of personal data processing, whereby a single entity ("*data controller*") decides to process the personal information of "*data subjects*" and it proceeds to execute such processing either at its own premises and with its own means, or by contracting it to third parties ("*data processors*") is more or less maintained in the text of the draft Regulation. Amendments address concerns mostly related to the internet environment – however, by insisting on a largely outdated distinction between data controllers and data processors the Commission risks leaving out the Regulation's scope important processing actors. The Commission did not affect the "*data controller*" and "*data processor*" definitions included in the Directive in its draft Regulation,[31] but rather chose to strengthen controlling instances by placing certain additional obligations upon data processors[32] as well and acknowledging the existence of "*joint controllers*".[33]

On the other hand, the definition of "*data subjects*" is particularly strengthened, taking account of the online environment, genetic data, as well as, perhaps most importantly, of the fact that the identification required by law need not be performed only by the data controller but also by whichever other natural or legal person has access to the data.[34]

In this way, however, the Commission appears to uphold in its draft Regulation the aforementioned traditional personal data processing scheme, whereby roles are expected to be distinguishable and data processors are expected to be passive and of an executionary only function. Nevertheless, what may have constituted a plausible and indeed standard processing scheme in the early 1990s or late 1980s is largely

[24] See Art. 3.1 of the Directive and Art. 4 of the draft Regulation.
[25] See Art. 3 of the draft Regulation and Art. 2 of the Directive.
[26] See draft Regulation, Recital 24.
[27] See also the Commission Communication, 2.1.1.
[28] See Art. 29 Working Party, Opinion 4/2007 on the concept of personal data.
[29] See Commission Communication, 2.1.6, Council Conclusions, 8.
[30] Admittedly, "*biometric data*" is not, hopefully an unintended omission by the Commission that needs to be corrected in future versions of the draft Regulation.
[31] Only the "*conditions*" of the processing were added as a distinguishing characteristic for data controllers (See Art. 4 of the draft Regulation and Art. 2 of the Directive).
[32] See in particular Art. 29 of the draft Regulation.
[33] See Art. 24 of the draft Regulation.
[34] See Art. 4(1) of the draft Regulation in comparison with Art. 2(a) of the Directive.

outdated by now.[35] Data controllers retain of course their central role as to the processing of personal data, but they may come in various types and formats. For instance, Web 2.0 service providers only provide the platform upon which personal data processing is performed and it is not always evident that they are themselves involved in such processing. The same applies to cloud computing, whereby the role of service (platform) providers, and whether they may be considered data controllers or not, still remains unclear.

In addition, the distinction between data controllers and data processors, that was perhaps clear at the time the Directive was introduced, is increasingly disputed in the contemporary complex business environment. By now data processors may be recipients of outsourced work while being located anywhere in the world or third parties that execute the processing and act upon its findings on behalf of their employers, the data controllers.[36] The distinction between the two data processing actors is becoming increasingly blurred in an interconnected world of ubiquitous computing.[37] In view of the above, perhaps the preferable way forward would be for the Commission to boldly abolish the notion of "*data processors*" from its Regulation altogether, and vest the data controller title, rights and obligations upon anyone processing personal information, regardless of its means, conditions or purposes.

5. Reforming the Directive's fair information principles: important additions (Art. 5 and 6 of the Regulation)

So-called *Fair Information Principles* constitute one of the bases of the EU data protection model, in that they apply to all processing of personal data. Once it is established that a certain personal data processing operation falls within the scope of the regulating instrument (Directive or Regulation) and that a lawful basis for such processing may be identified, then such processing ought to first and foremost observe the requirements of the Fair Information Principles. The Fair Information Principles of the Directive are maintained in the text of the draft Regulation (for instance, the fair and lawful processing of personal information, the data quality principle or the purpose specification principle, all in Article 5). Important new additions to this list, included in the same Article 5, "*are in particular the transparency principle, the clarification of the data minimisation principle and the establishment of a comprehensive responsibility and liability of the controller*".[38]

Both the principle of transparency and thus of accountability that are introduced here constitute substantial reinforcement of the individual rights protection.[39] The principle of transparency of the processing creates a personal data processing environment of trust and enables any interested party to enforce effectively data protection rights and obligations, given that personal data processing is mostly conducted behind closed doors. The principle of accountability for data controllers in the personal data processing context is by no means a new idea in the field.[40] Discussions date as back as 2009, when the Art. 29 Data Protection Working Party first included such a principle among its list of recommendations.[41] This idea was further elaborated and formulated into concrete suggestions in 2010.[42] In broad terms, a principle of accountability would place upon data controllers the burden of implementing within their organisations specific measures in order to ensure that data protection requirements are met. Such measures could include anything from the introduction of a Data Protection Officer to implementing Data Protection Impact Assessments or employing a Privacy by Design system architecture.[43] Despite its obvious advantages for data controllers, from the individual's point of view a principle of accountability would enable it to efficiently protect its right to data protection in front of (or even, against) the competent authorities. Let us now turn to two critical points in the new regime.

First there is the change to the purpose limitation principle. In the past, not all Fair Information Principles have been received with the same enthusiasm by data controllers. This has been particularly the case with the purpose specification principle. According to Article 6 of the Directive, "*personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes*". The limitation of such "*further processing*" has frequently raised substantial objections from the personal data processing industry, which is evidently interested in exploiting databases of personal information as much as possible (using techniques such as data mining, data matching or profiling) in

[35] Only recently, in its opinion 1/2010, did the Art. 29 Working Party attempt to define "data controllers" and "data processors" in the text of the Directive, whereby it concluded that "*The Working Party recognises the difficulties in applying the definitions of the Directive in a complex environment, where many scenarios can be foreseen involving controllers and processors, alone or jointly, with different degrees of autonomy and responsibility*".

[36] For instance, in the SWIFT case, whereby the headquarters are in Belgium but the company also operates two operating centers in The Netherlands and in the USA and also several sales offices elsewhere in Europe, the data protection authorities faced substantial trouble while attempting to identify the data controller and separate it from data processors and other participants in the processing. See the relevant Article 29 Working Group SWIFT Opinion (WP 128, 22.11.2006) and also Moerel L, Back to basics: When does EU data protection law apply? *International Data Privacy Law*, 2011, Vol.1 No.2, p.106ff.

[37] See also the Commission Communication, 2.2.4.

[38] See draft Regulation Explanation, par. 3.4.2.

[39] See also draft Regulation, Recital 30.

[40] See also D. Bigo, S. Carrera, Gl. González Fuster, E. Guild, P. De Hert, J. Jeandesboz & V. Papakonstantinous, *Towards a New EU Legal Framework for Data Protection and Privacy: Challenges, Principles and the Role of the European Parliament*, Commissioned by Policy Department C on Citizens' Rights and Constitutional Affairs of the Directorate General for Internal Policies of the European Parliament, Brussels, European Parliament, 2011, p.22ff.; De Hert, P. 'From the Principle of Accountability to System Responsibility. Key Concepts in Data Protection Law and Human Rights Law discussions', in Zombor, F. (ed.), *International Data Protection Conference 2011*, Hungary, Hungarian Official Journal Publisher, 2011, 88–120. See further: B. Van Alsenoy Allocating responsibility among controllers, processors and "everything in between": the definition of actors and roles in Directive 95/46/EC [2012] 28 CLSR 25 at p. 40.

[41] In its Future of Privacy (WP168) document, of December 2009.

[42] In its Opinion 3/2010.

[43] See also the Commission Communication, 2.2.4, Art. 29 Working Party Letter, c.

order to extract useful information on potential clients, business relationships etc.[44]

This request from data controllers seems to be accommodated in the text of the draft Regulation that allows, in its Article 6, "*further processing*" for a purpose that "*is not compatible with the one for which the personal data have been collected*". One immediately feels the compromise here between rights protection and business interests. The processing of personal information for purposes unforeseeable at the time of data collection, to which evidently no consent has been given by the individuals concerned, undermines the principle of purpose specification. The "*compatibility*" criterion in the draft Regulation is of little assistance, because in practice data controllers shall decide alone what is "*compatible*" and what is not, and it shall be up to individuals to take actions to challenge that decision. Until today, routine data protection practice has used broad and general wording ('marketing purposes', 'security purposes' etc.) in order to maximize the processing options in spite of the unequivocal wording of the purpose specification principle – if its application is further relaxed by a "*further processing*" addition, it risks becoming irrelevant in practice.

Second there is the failure to underline the connection between Article 5 and 6 of the Regulation, repeating the failure in the past to make clear that connection between articles 6 and 7 of the Directive. These two Articles in the Directive, each occupying a whole Section, both prescribe the conditions under which personal data processing becomes lawful in the EU: Article 6 of the Directive (now Article 4 of the Regulation) pertains to the "*principles relating to data quality*" and Article 5 of the Directive (now Article 6 of the Regulation) to the "*criteria for making data processing legitimate*". No clear guidance was given in the text of the Directive regarding the relationship between them. Only in the Directive's Recitals where some assistance to this end is provided.[45] Only there the message was voiced that Articles 6 and 7 ought to be read conjunctively; both the data quality conditions and the processing legitimacy grounds should concur in order for a specific processing to be lawful.[46] The Directive's lack of a clear and straightforward connection between Articles 6 and 7 allowed data processors to adopt at times an opportunistic approach, whereby they choose either to apply only Article 7 or Article 6 in order to justify the legitimacy of their processing. One can only deplore that the Commission did not seize the opportunity to clarify its position on the matter. The draft Regulation sets that "*Personal data must be: (a) processed lawfully, fairly and in a transparent manner* […]"(Article 5.1, on the *Principles relating to personal data processing*) and that "*Processing of personal data shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent* […]" (Article 6.1 on the *Lawfulness of processing*). This combined reading of its Articles 5 and 6, without any assistance in its Recitals, as was the case with the Directive, is the only indication included in the draft Regulation that the two Articles should apply conjunctively in order for a processing operation to be lawful.[47] Admittedly, this is a far from straightforward way that the Commission chose to address an issue that has caused much controversy in the text of the Directive. This could lead to substantial application difficulties, that the Commission could avoid by better clarifying this matter in the future versions of the draft Regulation.

6. Individual consent: clearer and more straightforward means (Art. 7 of the Regulation)

The requirement for individual consent holds a central role in the EU data protection model, at least as far as the Directive and its related processing is concerned.[48] It constitutes one of the legal bases in order for processing of personal data to be permitted. Consent allows an individual to make sure that his or her data is processed only in the manner that was specified during their collection when consent was obtained.

The Commission substantially reinforced the individual consent requirement in its draft Regulation. Its definition has been enhanced by means of requiring "*explicit*" consent,[49] in order to "*avoid confusing parallelism with 'unambiguous' consent and in order to have one single and consistent definition of consent, ensuring the awareness of the data subject that, and to what, he or she gives consent*".[50] Further than that, Article 7 of the draft Regulation sets several conditions for a valid and lawful individual consent to be granted: negotiating imbalances and dependencies are taken into account; consent collection must be distinguishable; consent may be withdrawn at any time; children may consent only through their parents or

[44] "*Further processing*" is also explicitly acknowledged in the text of the Framework Decision (in its Article 3.2).

[45] Recital 30, when read together with 29, stating that "*in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or* […]", thus adding up, rather than selectively applying, between the two Articles.

[46] This observation is of paramount importance to personal data protection. Any processing operation cannot be based on only one of these Articles: A processing operation adhering to all the "*principles relating to data quality*" laid down in Article 6 may be found unlawful if it is not based on individual consent or the other legal bases laid down in Article 7 of the Directive. Or, a processing operation that is indeed based on individual consent or on any other of the legal bases of Article 7 of the Directive may be found unlawful if it is not conducted according to all the Article 6 - principles. Application here is conjunctive and not selective.

[47] In other words, that both the Fair Information Principles and the conditions for the processing should concur on any given personal data processing in order for it to be permitted by the draft Regulation.

[48] This requirement is more relaxed when it comes to Justice and Home Affairs personal data processing (where, for the time being, the 2008/977/JHA Framework Decision applies). See critically: D. Bigo, S. Carrera, Gl. González Fuster, E. Guild, P. De Hert, J. Jeandesboz & V. Papakonstantinous, *Towards a New EU Legal Framework for Data Protection and Privacy: Challenges, Principles and the Role of the European Parliament*, Commissioned by Policy Department C on Citizens' Rights and Constitutional Affairs of the Directorate General for Internal Policies of the European Parliament, Brussels, European Parliament, 2011, p. 110–113.

[49] Draft Regulation, Art. 4(8).

[50] See draft Regulation, Explanation, 3.4.1.

custodians. In addition, only opt in ("*ticking a box*") and not opt out ("*silence or inactivity*") consent collection schemes are by now lawful.[51] In all cases, the relevant burden of proof lies with the data controller.[52]

In this way the Commission attempts to address difficulties created by the contemporary processing environment. In the online world, privacy policies are used extensively in order to satisfy the necessary informational requirements needed to allow for '*informed consent*'. However, in reality such 'privacy policies' are tailored specifically to meet legal requirements' and often are not formulated in a way so as to be easy to understand for individual users.[53] To make matters more complicated, different Member States seem to have put in place different requirements for such privacy policies, ranging from a general requirement of written consent to the acceptance of implicit consent. This leads to harmonisation difficulties. Sometimes commercial organisations will create privacy policies with the rules of the most demanding Member States in mind. In other cases some organisations might avoid operating in these more demanding environments.

The difficulties of warranting a free, specific and informed individual consent, as required by Article 2 of the Directive, have been extensively identified in the Commission Communication preceding the release of the draft Regulation,[54] whereby it is stated that requirements on consent should be clarified so as to make it easier to know what is required in order to allow individuals to be able to make a truly informed consent.[55] The approach of the draft Regulation, as evidenced in its wording, is to establish a powerful system for the protection of individual consent while processing personal data. Nevertheless, because the draft Regulation introduces, in its Article 7, valid and justified but apparently quite demanding requirements towards data processors, it remains to be seen which ones will ultimately survive the law-making process; any compromise however in the draft Regulation's Article 7 would be a compromise of the overall level of data protection afforded to individuals.

7. Updating the Directive's individual rights (Art. 11-20 of the Regulation) and introducing the right to be forgotten (Art. 17 of the Regulation)

In addition to tying the processor to fair information principles and to certain legal grounds or "*criteria for making data processing legitimate*", the EU data protection model affords to individuals a set of data protection-specific rights, without which their protection of their personal information would have been impossible. Individuals are handicapped in the data processing process, in that processing does not take place in the open but rather behind closed doors. They are thus mostly unaware when and how their data are being processed. To this end, since the first national data protection acts were released, a set of special rights has been introduced to their aid, which was subsequently adopted in the text of the Directive: the right to be informed that their data are being collected, the right to access the data stored and to learn about details of the processing operation and the right to object, in case of unlawful processing.

Substantial work towards the strengthening of the position of individuals has apparently been undertaken by the Commission in the text of the draft Regulation. Apart from maintaining the individual rights of information, access and objection to their personal information processing,[56] the draft Regulation has added a data controller obligation to transparency and to establishment of appropriate procedures that will assist data subjects,[57] it has increased the amount of information provided to individuals with regard to both rights to information and access, and, perhaps more importantly, expressly regulates profiling (building upon the Directive's "*automated individual decisions*").

In this way the Commission attempts to address difficulties caused by information technology and data processing advances, particularly in the Web 2.0 environment. Apart from discussions on the introduction of internet-specific individual rights, other identified difficulties refer to, for instance, the continued requirement of a fee for the exercise of the individual right of access,[58] or, with regard to the right to information, the employment of standard-developed sets of data protection notifications that would enhance individual protection.

It is hard to identify difficulties regarding the provisions under Chapter III of the draft Regulation, not only due to their volume (altogether, ten long articles, including the two newcomers in the field: the 'right to be forgotten' and the 'right to data portability') but also due to the fact that its organisation is at times difficult to follow.[59] However, the aim of strengthening as much as possible the position of individuals is evident. It remains therefore to be seen, provided of course that the current version is maintained during the law-making stages, whether the elaborate treatment of the draft Regulation shall serve the data protection purposes better than the, relatively brief, wording of the Directive.

With regard to the, much-discussed, right to be forgotten, it should be noted that privacy experts have long elaborated

[51] See draft Regulation, Recital 25.
[52] See draft Regulation Art 7 and Recital 32.
[53] See Robinson, N., Graux, H., Botterman, Maarten. and Valeri Lorenzo 'Review of the European Data Protection Directive' RAND Europe 2009.
[54] Under 2.1.5, where it is stated that requirements on consent should be clarified so as to make it easier to know what is required in order to allow individuals to be able to make a truly informed consent.
[55] The Commission also suggested that reforms in this area should take into consideration the principle of transparency. In this context, online behavioural advertising was noted, where "*both the proliferation of actors involved in the provision of advertising and the technological complexity of the practice make it difficult for an individual to know and understand if personal data are being collected, by whom, and for what purpose*" (Commission Communication, 2.1.5.).
[56] In Articles 14, 15 and 19 respectively.
[57] In Articles 11 and 12.
[58] See Commission Communication, 2.1.3.
[59] Or explain, see for instance Article 13 and Articles 16 and 17.

upon the merits of its introduction.[60] A number of Member States experimented with such a right to be forgotten, providing useful experience to the process.[61] The matter was vividly debated during the period that preceded the release of the draft Regulation. The Commission had announced in its Communication its intention to clarify the content of the 'right to be forgotten'. It defined it as "*the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes*".[62] The Article 29 Working Party has clarified that "*the added value of such a right would be over and above the existing rights, such as the right to have data deleted or the right to object*".[63] The Council, in its Conclusions, encouraged the Commission to explore the introduction of a right to be forgotten, "*as an innovative legal instrument, insofar as the exercise of such right is enabled by new technologies*".[64] The European Data Protection Supervisor (EDPS) expressed a unique view on the 'right to be forgotten': He envisaged it as connected to 'data portability' and has described it "*an obligation for the data controller to delete information as soon as it is no longer necessary for the purpose of the processing*".[65] In his view, it "*would ensure that the information automatically disappears after a certain period of time, even if the data subject does not take action or is not even aware the data was ever stored*".[66]

The Commission indeed included a right to be forgotten in its draft Regulation (in Article 17). It combined it with the individual right to erasure and blocking. The Commission seeks to strike a balance between on the one hand the right to be forgotten and, on the other, freedom of expression and "*historical, statistical and scientific research purposes*" – a task by no means straightforward (if not practically unattainable).[67] Given the controversy on this new right,[68] as well as technical and legal conditions of implementation that maybe make its continued existence impossible,[69] it is yet very early for a proper assessment of the Commission's efforts. Regardless of their outcome, however, the fact remains that even the opening up of the discussion on an individual 'right to be forgotten' on the internet is particularly important for individuals, who are effectively forced to enter massively and untrained online business models that, despite their worth in billions, practically only trade in personal information.

8. The right to system interoperability "*data portability*" (Art. 18 of the Regulation)

The second new addition to the individual rights list in the text of the draft Regulation refers to an individual right to data portability (in Article 18). This too, as is the case with the right to be forgotten, is an internet-specific right. In particular, it grants individuals the right to obtain a copy of their profiles uploaded onto internet platforms in a suitable format for further processing and use by themselves, and for such profile not to contain technical or other impediments to it being subsequently uploaded onto the internet platform of another service provider (essentially, a competitor to the former).

In this way the Commission makes an important contribution to the broader discussion on a right to system interoperability. A general right to system interoperability is nowhere to be found in EU law. Only occasionally a requirement for automated data processing systems to be able to

[60] See also Mayer-Schonberger V, *Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press, 2009. Originally, the term was usually employed to refer to measures such as the deletion of criminal records in order to allow convicted persons to 'make a new start' in life. In the data protection context, the expression is used in relation to the concretisation and adaptation of the rights of the data subject, and in particular the right to delete personal data and the right to object to personal data processing in the online world. Particularly the advent of social networking websites has accentuated the problem, because by now, through extensive 'tagging' and other mass personal data uploading in hundreds of millions of individual profiles, the amount of information collected on any individual has increased exponentially. All this information is readily available, through the effective use of internet search engines. See also Tene O, Privacy: The new generations, *International Data Privacy Law*, 2011, Vol. 1 No. 1, p. 21.

[61] In France, a public debate on the "*droit à l'oubli*" was formally launched in 2009 and first resulted in the adoption of a Charter in which search engines and collaborative sites agree to adopt a series of measures ensuring the implementation of the principles of purpose limitation, consent, right to information, right to access, right to rectification and opposition, as foreseen in French data protection law, in relation with data voluntarily published online by the data subjects (see Secrétariat d'Etat à la Prospective et au Développement de l'économie numérique (2010), *Charte du droit à l'oubli dans les sites collaborateurs et les moteurs de recherche*, Paris. On public support for these issues, see Bigot, Régis and Patricia Croutte (2010), La diffusion des technologies de l'information et de la communication dans la société française, N°269, Centre de Recherche pour l'Etude et l'Observation des Conditions de Vie (CRÉDOC), Paris, p. 131). In Spain, the '*derecho al olvido*' has been discussed especially in relation with the possibility to impose mechanisms that would ensure the rapid and easy deletion of personal data from social networks and search engines' results, possibly including mechanisms that prevent indexation of personal data. The Agencia Española de Protección de Datos (AEPD) has been litigating against Google in this area, and the European Court of Justice is expected to define search engines' obligations derived from EU law through a preliminary ruling requested by the Audiencia Nacional.

[62] See Commission Communication, 2.1.3.

[63] See Art. 29 Working Party Letter, i.

[64] See Council Conclusions, p. 6.

[65] See EDPS Opinion, p. 18 and also Hijmans H, ibid.

[66] *Idem*.

[67] In addition, on the effectiveness (and advisability) of the Commission intervention onto the online environment, in particular when affecting business models still under development, a brief mention is made below under the "right to data portability" analysis; both rights appears to develop an equally intrusive effect on the data controllers concerned.

[68] See Hijmans H, ibid. See, also Koops, E-J, "Forgetting Footprints, Shunning Shadows. A Critical Analysis Of The 'Right To Be Forgotten' In Big Data Practice," *SCRIPTed* 8, no. 3 (December 2011).

[69] See also The Register, *Google exec questions Reding's 'Right to be forgotten' pledge – Says certain aspects of article 17 are 'unworkable'*, 26.01.2012.

seamlessly co-operate among them is met, either in regulatory texts[70] or through actions of the Commission.[71] For most cases, however, a clear interoperability requirement is not directly applicable, leaving thus valuable space to, mostly, e-commerce operators to attempt to 'lock' consumers to their systems. This is more or less the case today with social networks websites. Despite their prevalence and transformation by now into a social phenomenon, their operators have chosen for their systems not to co-operate among them. This means in practice that personal data uploaded onto an internet platform are not easily moved to another (competitive) application. Individuals are therefore restricted in their options, in the sense that the time and effort (if not money) required for such a data transfer makes it impractical.[72]

Despite of the fact that the right to system interoperability is primarily a consumer protection and unfair competition rather than a data protection legal issue,[73] the Commission established during the preparatory stages that led to the draft Regulation that individuals ought to be facilitated while moving their personal information on the internet from one platform to another.[74] It is to this end that Article 18 is included in its draft Regulation. Its application is expected to warrant increased control over uses of personal data over the internet.

Here too, as in the case of the 'right to be forgotten', it is very early to properly assess the Commission's efforts to protect individuals, provided of course that both rights make it through the law-making process in their current wording. However, one thing that has become quite clear by now through the introduction of these two rights is that the Commission seems to be particularly engaged with social networking websites and, indeed, the current internet state of play. As such, this may prove a risky law-making option: legislating in a constantly evolving field risks making the law seem outdated and irrelevant. New regulations, that could perhaps be interpreted as favouring one over another competing internet platforms, could also decidedly affect (or even distort) a process in the making that could ultimately change the internet as we know it[75] – admittedly, not a task of data protection legislators.

9. National data protection authorities (Art. 46-56 of the Regulation)

Member State Data Protection Authorities (DPAs) are intended to constitute "*the main instrument of data protection enforcement*" within their respective jurisdictions.[76] This means that DPAs are responsible for warranting effective implementation of their respective national data protection acts within their jurisdiction. There are several means to achieve this: investigative powers, powers of intervention and the power to engage in legal proceedings.[77]

The Commission in its draft Regulation, given also that reliance on Member State data protection acts is no longer possible, goes into significant detail over the role expected to be held by DPAs ("*supervisory authorities*"), devoting two Chapters (Chapter VI and most of VII) to this end. The new provisions, particularly those of Chapter VI, are largely based on these of the Directive but also make significant new additions, such as the explicit obligation for DPAs to "*co-operate with each other and the Commission*",[78] an elaborate description of the independence requirements,[79] or, perhaps most importantly, introducing the notion of a "*lead authority*" in cross-border cases, in an attempt to provide to data controllers a 'one-stop-shop'.[80] Chapter VII, on "*co-operation and consistency*" seeks to establish appropriate procedures that will hopefully warrant cross-border efficient implementation of data protection provisions within the EU under, most of the time, the watchful eye of the Commission (and the European Data Protection Board).

These amendments to the approach implemented by the Directive is hoped to resolve shortcomings of the enforcement mechanism in effect today. Perhaps due to their mission to constitute an integral but essentially new layer of public administration within their respective jurisdictions, DPAs have customarily suffered from lack of uniform (or, even, optimal) status. The differences among the legal systems in which each one of them is established, as well as political, financial, historical and other factors may have also contributed to this end. Whatever the reasons, the fact remains that DPAs, although common in name and legal basis (the Directive), when closely examined reveal substantially different approaches, that could ultimately affect the application of data protection at Member State level. In addition, the inevitable 'locality' of DPAs brings forward obvious difficulties for individual data protection within the modern data processing environment. Within a Web 2.0 reality, whereby social networking websites and internet-based processing of personal information is the norm, Member State DPAs seem to remain helplessly bound to national borders. Although this is also an issue of the applicable law, a lot would be gained if Member State DPAs engaged in institutional co-operation among them.

[70] For instance, as in the Computer Programs Directive; see also Miller J/Hoffman D, Sponsoring trust in tomorrow's technology: towards a global digital infrastructure policy, *International Data Privacy Law*, 2011, Vol.1 No.2, p.85.

[71] As may be evidenced in the treatment of the first versions of Apple's iPods and iTunes interoperability problems.

[72] See also The Economist, Data Protectionism – Serfing the Web, 11.11.2010.

[73] See also EP Working Document 2, p. 3.

[74] See also Commission Communication, 2.1.3. The EDPS considers data portability and the right to be forgotten as "*connected concepts put forward by the Commission to strengthen data subjects' rights*" (EDPS Opinion, 83 and 89), and also suggests that they be "*limited to the electronic environment*" (91).

[75] See Fortune magazine, *Facebook vs. Google: The battle for the future of the Web*, November 21, 2011.

[76] See the Commission Communication, 2.5.

[77] See Art. 28 of the Directive.

[78] Art. 46.1 of the draft Regulation.

[79] Articles 47 and 48 of the draft Regulation, see also Explanation, par. 3.4.6.1.

[80] See Art. 51 of the draft Regulation and Explanation, par. 3.4.6.2.

From a preliminary point of view it appears that the Commission has identified the needs for increased cross-border co-operation and possibly uniform rule application and has taken positive measures to this end. Whether or not they suffice, or, even, whether or not they are well-described in the text of the draft Regulation shall most likely be proven in practice. However, note should be taken of the fact that the draft Regulation does not preclude the existence of more than one supervisory authority within a single Member State. On the contrary, it acknowledges such case and merely asks that a "*single contact point*" be established.[81] At first sight, this option hardly assists the data protection purposes. Given the draft Police and Criminal Justice Data Protection Directive as well as the intra-EU PNR Directive (and, potentially other regulatory instruments within the same subject-matter), this could lead to a multitude of supervisory authorities at various Member States of no definite hierarchy among them. Harmonisation problems could come as a result, while at the same time individuals may find themselves lost among several local authorities of overlapping competences, rather than a single DPA that is the case today.

Finally, because co-operation and consistency appear to be pursued by the Commission, perhaps it would be useful if institutions that have already a history of several decades contributing to this cause, such as the International Conference of Data Protection and Privacy Commissioners, were recognized by mention in the draft Regulation Recitals.

10. The abolition of the obligation to notify (Art. 28 of the Regulation)

The notification system established in Articles 18 and 19 of the Directive originates in the 1960s and 1970s, when the first national data protection acts emerged. At that time it was conceived that processing operations would be limited in number and volume, and thus possible to be listed in central, national registers. Such registers would assist individuals, who only had to consult them, while protecting their rights. These assumptions have been completely overturned by now. Computing is on its way to becoming ubiquitous. Searches in national registers, regardless whether online, provide limited assistance to individuals seeking redress: in practice, if they do not know who the data controller is the relevant registry will be of no use to them. And, even if they do know the data controller, still the registry will add very little to their knowledge. The Commission Communication prior to the release of the draft Regulation identified that "*there is general consensus amongst data controllers that the current general obligation to notify all data processing operations to the Data Protection Authorities is a rather cumbersome obligation which does not provide, in itself, any real added value for the protection of individuals' personal data*".[82] To this end, it suggested that a simplified, possibly uniform EU-wide registration form be introduced. The EDPS from its part suggested a shift from the Directive system to a system more focused on processing risks.[83]

[81] See Art. 46.2 of the draft Regulation.

[82] In 2.2.2.

[83] See EDPS Opinion, 62.

There is no mention of the notification requirement in the text of the draft Regulation. Instead, data controllers are instructed to maintain themselves documentation of the processing operations under their responsibility.[84] In addition, a series of requirements (such as the personal data breaches notifications or the impact assessments, examined in the following sections) are intended to replace with contemporary, and hopefully effective, mechanisms what has long constituted a major anachronism in the EU data protection model.

11. A generalized use of "*personal data breach notifications*"? (Art. 31-32 of the Regulation)

The latest (third, within less than altogether fifteen years in effect) version of the ePrivacy Directive introduced a mandatory personal data breach notification obligation for data controllers in the electronic communications sector.[85] This addition to the ePrivacy Directive was one of the most disputed issues during its amendment process.[86] Despite of the fact that public opinion in several EU Member States was astonished to hear, mostly from journalists and not from the perpetrators themselves, about spectacular losses or compromises of their personal information,[87] some data controllers concerned strongly objected the introduction of a mandatory notification obligation. Such notifications would incur substantial cost, not to mention the bad publicity, for the organisations responsible.[88] These objections, raised by powerful organisations, were not to be taken lightly – after all, they help explain the layered obligations placed upon data controllers (that are primarily addressed towards their respective DPAs and only under certain conditions directly towards each individual concerned), as well as, the limitation

[84] See Art. 28 of the draft Regulation.

[85] Art. 4.3 "*in the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority*". Data controllers, however, should also take care that "*when the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay*". See also Barcelo R/Traung P, The Emerging European Union Security Breach Legal Framework: The 2002/58 E-Privacy Directive and Beyond, p. 89.

[86] See *Barcelo R/Traung P*, The Emerging European Union Security Breach Legal Framework: The 2002/58 E-Privacy Directive and Beyond, in Gutwirth S/Poullet Y/De Hert P (eds.), Data Protection in a Profiled World, Springer, 2010, pp. 77ff.

[87] See, for instance, *UK's families put on fraud alert*, BBC News, 20 November 2007, *Previous cases of missing data*, BBC News, 25 May 2009.

[88] However, it has been noted that "fear of reputational sanction may lead, notwithstanding the legal mandate, to excessive secrecy about security breaches involving sensitive customer information", Schwartz P/Janger E, *Anonymous Disclosure of Security Breaches*, in Securing Privacy in the Internet Age, 221 Stanford Law Press, Anupam Chandler, Lauren Gelman & Margaret Jane Radin, eds. (2008), p.224. See also Schwartz P/Janger E, Notification of Data Security Breaches, 105 Michigan Law Review 913 (2007).

of this obligation to telecommunications providers only (and not the internet in general).[89]

In its draft Regulation the Commission chose to elevate the personal data breach notifications onto a general data controller obligation within the EU data protection model (in Articles 31 and 32). The definition of a personal data breach is essentially the same as that of the ePrivacy Directive: "'*personal data breach*' *means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4). Also, the approach is similar to the ePrivacy Directive: layered, in that it primarily forces data controllers to alert the supervisory authorities and only "*when the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject*" ought they to alert individuals too. Perhaps the Commission in this way hopes to alleviate data controller concerns, by asking for an already accepted, and tested, model to be used.

The Commission's intended generalized use of personal data breach notifications is a choice strongly supported by data protection proponents in the past.[90] On the other hand, exactly as was the case with the ePrivacy Directive, opposition is expected to be strong by data controllers. Nevertheless, both reality (with its more than frequent and important data losses) and the request of affording an increased level of protection to individuals make such an obligation an important addition to the text of the draft Regulation.

12. The role of 'soft law': Data Protection Impact Assessments (Art. 33 of the Regulation)

A Data Protection Impact Assessment[91] (DPIA) may be defined as a systematic process for evaluating the potential effects on privacy and data protection of a project, initiative, proposed system or scheme and finding ways to mitigate or avoid any adverse effects.[92] It is fair to say that PIA originates from the positive experience of environmental, regulatory and social impact assessments, commenced in 1960s. The idea grew up and developed in a number of common law countries (e.g. USA, UK,[93] Australia) in the mid-1990s.

The concept of the DPIA attracted attention in the EU only recently. In January 2010 the Commission published a report on new privacy challenges[94] where it overviewed DPIA polices around the world and analysed briefly the pros and cons of DPIAs. This report stated, among others, that "*it is much easier to produce privacy-friendly systems if data protection issues are considered early in their design stage*".[95] The European Parliament, in its resolution in May 2010 on Passenger Name Records (PNR), stated that "*any new legislative instrument must be preceded by a Privacy Impact Assessment and a proportionality test*".[96] A need to better assume responsibilities of public authorities and industry by means of PIA was also explicitly addressed by the Commissioner Reding in July 2010.[97] Also, the Art. 29 Working Party in February 2011 endorsed a DPIA for RFID (Radio Frequency Identification) applications.[98]

The Commission Communication prior to the release of the draft Regulation set that, in order to enhance data controllers' responsibility, it would be examined whether "*an obligation for data controllers to carry out a data protection impact assessment in specific cases*" should be included.[99] These situations could include, *inter alia*, processing of sensitive data or "*when the type of processing otherwise involves specific risks, in particular when using specific technologies, mechanisms or procedures, including profiling or video surveillance*".

DPIAs are formally acknowledged in the text of the draft Regulation (in Article 33). Although an exact definition is not provided, they are expected to "*carry out an assessment of the impact of the envisaged processing operations on the protection of personal data*" and to "*contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation*". They are not to find generalized application, but they are to be undertaken only when certain processing operations may

[89] It should be noted that the EDPS finds the balance achieved in the ePrivacy Directive as adequate for the Directive purposes as well (see EDPS Opinion, 77).

[90] See also the Art. 29 Working Party's Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments (WP184), 05.04.2011.

[91] "Privacy Impact Assessment" (PIA) outside the EU.

[92] See Wright D., "Should privacy impact assessments be mandatory?", *Communications of ACM*, July 2011; Wright D. & De Hert, P. (eds.), *Privacy Impact Assessment*, Series: *Law, Governance and Technology Series*, Vol. 6, Dordrecht, Springer, 2012, 523p.

[93] The UK was the first country in Europe to develop a PIA manual in 2007. *Cf.* Information Commissioner's Office, *Privacy Impact Assessment Handbook*, Version 2.0 (2009), http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/files/PIAhandbookV2.pdf.

[94] European Commission, *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments. Final Report*, 20 January 2010, http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf.

[95] Id., p. 50.

[96] European Parliament, Resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0144+0+DOC+XML+V0//EN.

[97] Reding, V., Vice-President of the European Commission responsible for Justice, Fundamental Rights and Citizenship, "Towards a true Single Market of data protection", SPEECH/10/386, Meeting of the Art. 29 Working Party re "Review of the Data protection legal framework", Brussels, 14 July 2010. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/386.

[98] Art. 29 Working Party, *Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications*, WP 180, Brussels, 11 February 2011. This issue dates back to a 2009 Commission's recommendation on DPIA requiring the industry and other stakeholders to develop a DPIA framework for RFID. The first proposal, submitted in March 2010, presented a good starting point, but it did not gain the full support of the Working Party. The revised proposal, submitted in January 2011, eventually got its acceptance.

[99] See Commission Communication, 2.2.4.

cause "*specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes*"; in accordance, a helpful, indicative, list is provided in the draft Regulation, most notably including sensitive ("*special categories of*") personal data.

As such, DPIAs should be examined within the context of the principle of accountability, also combined with the abolition of the notification system. It shall be up to data controllers to decide whether their processing falls within the conditions of the Regulation, unless it is found in the draft Regulation's listing, and conduct a DPIA prior to its execution. The same data controllers shall take steps to make such DPIA "*easily accessible to the public*" – but not to deposit it with the supervisory authority concerned. Only if its findings "*indicate a high degree of specific risks*" are they to consult with the supervisory authorities' prior to executing their processing.[100]

Given the above, one could not avoid thinking that great expectations for data controllers' responsible behaviour are made in this case (also considering that no institutional requirement for an independent undertaking of a DPIA is included in the draft Regulation). In addition, the draft Regulation's approach seems to be insensitive to financial constraints: potentially risky personal data processing is often undertaken by small corporations that may not have the financial means to conduct a proper DPIA. Finally, the draft Regulation does not clarify whether a renewed DPIA will be required whenever changes (substantial? insubstantial?) are made to an already assessed processing operation – what steps need data controllers take in this event? It remains therefore to be seen whether the positive example of environmental and other impact assessments will be repeated in the data protection field as well.

13. A new role for the Article 29 Working Party (that however keeps it away from 'adequacy' establishment) (Art. 64-72 of the Regulation)

The role of the Article 29 Working Party has proven indispensable for EU data protection over the years. It has become the main body for consultation and harmonisation on data protection issues within the EU and has frequently undertaken a privacy watchdog role, identifying difficulties and recommending policies in cutting-edge technologies or newly released business models. Its central role while assessing the data protection level of third countries, in view of data exports from Member States, cannot be overseen. On the other hand, the Article 29 Working Party, despite of its central role, remains more or less a closed office to the public, without a permanent supporting mechanism, to which access (and appointment) is warranted only to its privileged members, the DPAs.

Significant steps towards strengthening the role of the Article 29 Working Party are apparently undertaken by the Commission in its draft Regulation,[101] in line with views expressed during the relevant consultation period.[102] The Article 29 Working Party is to be replaced by a permanent European Data Protection Board. Detailed provisions describe its membership, operation and tasks. Relationships with the Commission and the European Data Protection Supervisor will be hopefully fine-tuned – particularly given that the latter shall host the Board's secretariat.[103]

However, not all changes brought by the draft Regulation seem to be in the Working Party's best interest: perhaps most importantly, it appears that the role it held during the 'adequacy' of protection findings under the Directive regime is no longer vested upon it under the draft Regulation. In addition, the Commission's obligation to inform the Working Party as to its actions, following an opinion or a recommendation, appears to be lighter in the text of the draft Regulation.[104]

The Article 29 Working Party, or European Data Protection Board, holds a central role in the European data protection model. Its output affects, directly or indirectly, all data subjects and data controllers within the EU. It would therefore appear consistent with its role if access to it was granted also to parties of the data processing process (data controllers and data subjects) that may have a vested interest in a unified implementation of data protection rules across the EU.

14. Conclusion: a cause for celebration for human rights

The draft Regulation, because it can no longer rely on national data protection acts, as was the case with the Directive, needs to be judged at several levels. At a higher level, it needs to be assessed with regard to its substance: does it serve its purposes: does it efficiently protect the individual right to data protection in the modern processing environment while also warranting the free movement of personal data: does it achieve its intended harmonizing effect? At a lower level, the draft Regulation needs to be assessed on its self-sufficiency and law-making prowess: does it effectively replace national data protection acts: is it detailed enough and capable of regulating all personal data processing (apart of course from processing falling within the Police and Criminal Justice Data Protection Directive scope) within the EU?

From a preliminary point of view, the draft Regulation seems to score high with respect to the former category of questions but inevitably perhaps less so with the latter.

The Commission in its draft Regulation has taken bold steps for the improvement of the data subjects' position in

[100] See Art. 34.2 of the draft Regulation.
[101] In its Articles 64–72.
[102] See the Commission Communication, 2.5, and also Art. 29 Working Party Letter, f. From his part, the EDPS questioned "*the fact that the Commission (and more specifically the Unit) is at the same time member, secretariat and addressee of the Working Party's opinions*" (143); he also suggested that the way in which himself and the Working Party co-operate could be fine-tuned (152ff.).
[103] See Article 71.1 of the draft Regulation.
[104] Compare Article 30.5 of the Directive and Article 66.4 of the draft Regulation.

contemporary personal data processing conditions. Their rights have been strengthened and data controllers' obligations have increased respectively. Much needed clear and case-specific guidance is by now provided for many categories of processing operations. New enforcement tools have been introduced, replacing others that are by now outdated.

Data controllers, from their part, first and foremost benefit from a choice of legal instrument (a Regulation, rather than a Directive) that will hopefully warrant harmonisation across the EU. In addition, under the auspices of the principle of accountability, their own burden of proof is practically reversed: instead of fulfilling a series of bureaucratic actions in order to evidence their proper execution of legal requirements, under the draft Regulation such execution shall be taken for granted, unless challenged by data subjects or the supervisory authorities.

On the other hand, the Regulation is intended to be directly applicable in the EU, bypassing Member State data protection legislation that seems to have caused uncertainty and lack of harmonisation within the EU. However, in order to do so, it needs to be detailed enough to address each and every case that national law accommodates. Even leaving aside political, financial and other factors of divergence, it also needs to respect the fact that its addressees apply different legal systems. It would therefore seem that the Regulation faces an impossible task. After all, one needs to keep in mind that no precedent currently exists in the EU to-date of the Commission employing a Regulation to regulate such a wide field, particularly in the information society context.

The current version of the General Data Protection Regulation is expected to be the first product of a long line of negotiations. The Lisbon Treaty and the many years that have passed since the Directive was introduced – a generation in fact in terms of personal data processing – make an overhaul of the data protection regulatory framework imperative. Regardless of its merits and shortcomings, the fact remains that the release of the draft Regulation marks the second generation of data protection regulatory instruments at EU level – a far from self-evident fact fifteen years ago, and a definite cause for celebration for human rights.

Professor Paul De Hert (*paul.de.hert@uvt.nl*) (*paul.de.hert@vub.ac.be*) *Free University of Brussels, Belgium (VUB-LSTS) & Tilburg University (Tilt) Netherlands. He is a member of the CLSR Editorial Board.*

Dr. Vagelis Papakonstantinou *(vpapakonstantinou@pkpartners.gr) Free University of Brussels, Belgium (VUB-LSTS) & International Hellenic University, Greece.*