Andra Giurgiu / Gérard Lommel

A New Approach to EU Data Protection*

– More Control over Personal Data and Increased Responsibility –

Zusammenfassung

Die Entwicklung neuer Technologien und die bedeutende Rolle des Internets im heutigen Alltag haben den Datenschutz vor neue Herausforderungen gestellt. Darüber hinaus wirkt sich die uneinheitliche Umsetzung der Richtlinie 94/46/EG, die den rechtlichen Rahmen für den Datenschutz in Europa bildet, negativ auf den europäischen Binnenmarkt aus. Vor diesem Hintergrund ist es Ziel des Vorschlags der Europäischen Kommission für eine neue Datenschutz-Grundverordnung, den Rechtsrahmen zu harmonisieren und ein erhöhtes Datenschutzniveau der Bürger zu schaffen. Obwohl sich die Europäische Kommission, das Parlament und der Rat in vielen Punkten noch nicht einig sind, ist eine klare Änderung der Perspektive zu erkennen. Unternehmen sollen selbst tätig werden und eine verantwortliche Haltung zum Datenschutz übernehmen. Die Rechenschaftspflicht der für die Verarbeitung Verantwortlichen wird hiermit in den Vordergrund gestellt. Es gilt nun proaktiv zu handeln, und nicht nur reaktiv. Prinzipien wie Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen spiegeln diesen Ansatz wider. Bürger werden ihrerseits mit am Internetzeitalter angepassten Rechten – wie dem Recht auf Datenübertragbarkeit – ausgestattet, um die Kontrolle über ihre Daten in die eigene Hand nehmen zu können. Die Bedingungen einer gültigen Einwilligung in der Online-Welt werden deutlicher gestaltet und Nutzer und Verbraucher mit erweiterten Rechtsschutzinstrumenten ausgestattet, die die Durchsetzbarkeit des Datenschutzes stärken. Auch wenn vor 2015 kaum mit einer Verabschiedung der Reform zu rechnen ist, verspricht diese neue Herangehensweise die Chance auf einen effizienteren Datenschutz.

Résumé

Le développement des nouvelles technologies et l'importance fondamentale de l'Internet dans la vie quotidienne ont confronté la protection des données à un nouveau défi. En outre, le manque d'une transposition hétérogène de la Directive 94/46/CE, constituant le cadre légal de la protection des données en Europe, a un impact négatif sur le marché intérieur. Dans ce contexte, le projet de règlement relatif à la protection des données personnelles de la Commission européenne vise à harmoniser le cadre législatif et à créer un niveau de protection élevé des données personnelles des citoyens. Même si les opinions de la Commission européenne, du Parlement et du Conseil divergent

* Andra Giurgiu, Research Associate at the Interdisciplinary Centre for Security, Reliability and Trust (SnT) of the University of Luxembourg; Gérard Lommel, Chairman of the National Commission for Data Protection of Luxembourg.

encore sur certains points, une évolution nette de la perspective est à reconnaître. Les entreprises doivent prendre l'initiative et adopter une attitude responsable vis-à-vis de la protection des données. Ainsi, la responsabilisation des personnes chargées du traitement des données personnelles prime. Il est maintenant temps d'agir non pas de manière réactive, mais de façon proactive. Des principes comme la protection des données à travers la technologie ou encore des paramètres par défaut respectant la protection des données expriment cette approche. Les citoyens pour leur part se voient accordés des droits adaptés à l'ère de l'Internet, comme le droit au transfert des données, afin d'être en mesure de prendre le contrôle des données dans leurs propres mains. Les conditions du consentement valable dans un monde «online» sont plus clairement conçues et l'utilisateur, ainsi que le consommateur sont dotés d'instruments légaux renforçant l'imposition de la protection des données. Alors qu'une adoption de la réforme avant 2015 semble peu probable, cette nouvelle approche reflète la chance d'une protection des données plus efficace.

I. European Data Protection put in context

The need for legal protection of individual privacy in the context of automatic data processing became a topic of discussion as early as the 1970 s with the development of the first large-scale computers. As Europe's awareness about privacy with regard to the processing of personal data began to increase, this was followed by the adoption of the first legal instrument to regulate the field. The *Council of Europe* Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108)[1] set the first framework of common standards for European data protection. More than a decade later, Directive 95/46/EC[2] took over, refined and detailed the principles which lay at the heart of Convention 108.

Closely connected to the right to privacy under Article 8 of the European Convention on Human Rights, the right to personal data protection was for a long time entangled with it. Although being also recognized by Article 8 of the Charter of Fundamental Rights of the *European Union*,[3] it was only with the entry into force of the Lisbon Treaty[4] in 2009, which gave binding force to the Charter, that it gained the status of an autonomous fundamental right. Article 16 of the Treaty on the Functioning of the *European Union* (TFEU) also introduced a new legal basis that allows for a comprehensive legislation in the field of data protection to be established.

The development of ICT systems and their increasing capabilities to collect, store and analyze personal data had led to the need for recognizing the full independence and autonomy of the right to the protection of personal data, thus finally separating it from

1 The *Council of Europe* Convention for the protection of individuals with regard to automatic processing of personal data no. 108, 28.1.1981.

2 Directive 95/46/EC of the *European Parliament* and 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 1995, L 281, p. 31-50.

3 Charter of Fundamental Rights of the *European Union*, OJ C 326, 26.10.2009, p. 391–407.

4 Treaty of Lisbon amending the Treaty on *European Union* and the Treaty establishing the *European Community*, signed at Lisbon, OJ C 306, 17.12.2007, p. 1–271.

the right to privacy. But the full recognition of the right to the protection of personal data as a fundamental right of the citizens was also a step forward in the direction of modernizing the European framework in this field. Society as a whole and life as we used to know it have undergone fundamental changes due to extremely rapid technological developments. Placed into this context, the two main objectives of Directive 95/46/EC, namely to establish a high level of protection of the individuals as well as a free flow of information on the internal market, have been seriously undermined by the insufficiently harmonized interpretation and the lack of practical effectiveness of the current set of rules.

In order to enhance the right of the citizens to the protection of their personal data at a time when phenomena such as social networking, cloud computing, profiling and data mining represent the current state of the art, there is an acute need of adapting the outdated legal framework. Not only is Directive 95/46/EC unable to cope with existing challenges but there are already new, emerging threats such as those posed by the development of new technologies like unmanned aircraft systems (drones), second-generation DNA sequencing technologies, human enhancement or second-generation biometrics[5] and additionally everything known as "ambient intelligence" that need to be properly addressed. In a "brave new world" where information systems are ubiquitous, data protection threats need to be properly addressed.

Moreover, in a globalized world the effectiveness of the full economic and strategic value of the European internal market depends, amongst other things, on the free, unhindered flow of information. The existing legal patchwork of various Member States' transposition laws of Directive 95/46/EC impedes this flow of information. Harmonization and more legal certainty and security for the stakeholders are set as the main targets. Apart from that, the EU must be able to act as one on the international level in order to respond to threats such as those recently revealed in the NSA affair.

In 2008, the *Information Commissioner's Office* (ICO) commissioned a review of Directive 95/46/EC. The overall conclusion of the RAND report[6] was that "while the widely applauded principles of the Directive will remain as a useful front-end, they will need to be supported by a harms-based back-end in order to cope with the growing challenge of globalization and international data flows". The link between the concept of personal data and privacy, the measures aimed at providing transparency, the rules and tools for data transfers, the role of the Data Protection authorities (DPAs) in accountability and enforcement as well as the definition of entities involved in data processing were identified as the common weaknesses of the Directive.

With a view to the overall effectiveness of the Directive, it emerged from the consultation performed in preparation of the elaboration of the *Commission's* proposal as well as from the Article 29 Working Party's document on the Future of Privacy,[7] that

5 R. Finn et al., *Seven types of privacy*, in S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age*, Springer, Dordrecht, 2013, pp.3-33.

6 N. Robinson et al., *Review of the European Data Protection Directive*, RAND Europe, 2009, available at http://www.rand.org/pubs/technical_reports/TR710.html, last viewed 28 February 2014.

7 Article 29 Data Protection Working Party, The Future of Privacy: Joint contribution to the Consultation of the *European Commission* on the legal framework for the fundamental right to protection of personal data, WP 168 of 01 December 2009.

harmonization and a wider scope of application, empowering the data subject, increased responsibility of data controllers, strengthening the role of DPAs as well as better data transfers should be the primary goals of the future legal instrument meant to replace the current Directive.

II. The current state of play

It was against this background that the *Commission* released, in January 2012, a new Data Protection Reform Package, consisting of a General Data Protection Regulation (the Regulation)[8] and a Police and Criminal Justice Data Protection Directive.[9] The two legal instruments are supposed to replace, on the one hand, Directive 95/46/EC and on the other hand, Framework Decision 2008/977/JHA.[10] Considering the ampleness of the topic, the present article will focus solely on the main changes brought by the Regulation, leaving aside the aspects covered by the draft Directive regarding data protection in the context of police and judicial cooperation in criminal matters.

Due to its ambitious objective of setting a new and future proof framework for European data protection, the legislative procedure of adopting the draft Regulation has been rather laborious. The *European Parliament* voted on a compromise text in October 2013, thus settling a long list of controversial points, while bringing some significant amendments to the draft Regulation. Although many had hoped for the proposed Regulation to pass during the current parliamentary term, this goal seems impossible to achieve. Moreover, two years after its presentation, no convergence of contradictory positions regarding some of its most essential elements has been reached in the Council, which is working on its negotiating position.

The present article will attempt a critical analysis of the main aspects that are to define the future for European data protection as regards the strengthening of citizens' rights and the increased responsibility of the controllers. In doing so, it will take into consideration the *Commission's* draft proposal as well as some of the main amendments of the *Parliament* and of the *Council*.

8 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), 25.1.2012, COM(2012) 11 final.

9 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, 25.1.2012, COM(2012) 10 final.

10 *Council* Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters OJ L 350, 30.12.2008, p. 60–71.

III. A stronger and more efficient framework: comprehensiveness, harmonization and scope enlargement

The need for a comprehensive approach to data protection had been stressed by various stakeholders, including the *European Commission*.[11] The decision of adopting two separate legal instruments, a general Regulation and a Directive for criminal matters has been therefore met with regret by Europe's data protection advocates seeking a more consistent approach. A very good observation is made by *Paul De Hert* and *Vagelis Papakonstantinou*, who note that the *Commission's* decision to amend Directive 95/46/EC and Framework Decision 2008/977/JHA builds upon an elusive distinction between general and commercial data processing and security-related personal data processing. They consider this distinction to be a "schematic and artificial" one, as there would be almost no difference in scope between the two legal instruments.[12]

Regulating the protection of personal data processed in the framework of police and judicial cooperation in criminal matters through a distinct legal instrument is prone to criticism. Law enforcement access to personal data takes place in a rather opaque manner. Unlawful access of citizens' personal data by police and law enforcement has become everything but a rare case. Since the release of the package, the main focus of debate has been on the General Data Protection Regulation while little attention was paid to the Directive despite such problems. Moreover, considering the fact that one of the main reasons for setting a new framework was the legal fragmentation of the implementation of Directive 95/46/EC and its partially inconsistent application, it is rather regrettable that the Police Directive might share the same uncertain fate.

Another point of criticism expressed by experts and MPs is the non-inclusion of Regulation 45/2001[13] in the current package. Data processing by European institutions and bodies needs to take place in a consistent manner, ensuring a high level of protection of European citizens. Regulation 45/2001 is equally outdated and unfit to cope with some of the challenges of the information age. It will definitely undergo revision so as to be aligned with the rest of the legal instruments regulating European data protection, but the question is, when this will happen and how to proceed in the meantime in case of inconsistencies and legal disparities.

In order to improve the legal harmonization, the *Commission* judiciously opted for a replacement of the current Directive 95/46/EC with a Regulation, having direct effect without any need of transposition. The aim was to contribute to an easier flow of information within the internal market as well as to achieve a greater legal certainty and

11 See 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, Brussels, 4.11.2010, COM(2010) 609 final.

12 P. De Hert, V. Papakonstantinou*, The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals*, in Computer Law & Security Review no. 28/ 2012, pp. 130-142.

13 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, OJ L 8, 12.1.2001, p. 1.

security. Avoiding the inconsistencies of the different transposition laws would increase the protection of the citizens and improve the stage for the various economic actors.

With the aim of increasing the protection of European citizens, the *Commission* also proposed an enlargement of the territorial scope of application of European data protection rules. Thus, the Regulation would also apply to controllers not established in the Union if they offer goods or services or they monitor the behavior of data subjects residing in the *Union*.[14] On this point the *Commission*, the *Parliament* as well as the *Council* seem to be in agreement.

Although it is regrettable that the opportunity to achieve more comprehensiveness though one single legal instrument instead of three has not been seized, the package still appears to be a huge step forward in regulating and modernizing data protection. A single set of rules directly applicable throughout the *Union* instead of diverging transposition laws of Directive 95/46/EC will most certainly boost growth and innovation on the internal market while eliminating inefficient administrative burdens and simplifying compliance for businesses through unified legal rules and a one-stop-shop access to the supervisory authorities. Whether the *Commission's* proposal will achieve its aim of increasing the level of protection for the citizens remains questionable. As previously shown, the border between the processing of personal data for commercial purposes and the processing taking place in the framework of police and judicial cooperation in criminal matters is rather thin. Lowering the present standard in one field will most certainly affect the overall level of citizens' protection in *Europe*.

IV. Empowering the data subjects

1. To consent or not to consent – Is there any real choice?

Being able to express a meaningful consent to the processing of one's personal data is of the essence of informational self-determination.[15] Nowadays however we see a division of Europeans into two sociological groups according to their attitude towards privacy and data protection. One the one hand, there are the "digital natives", belonging to the young generation aged between 15-24 as well as students, who are freely giving away their data, for example on social platforms like Facebook, without many concerns as regards privacy, arguing they have nothing to hide or fear. On the other hand, "digital initiates" are very much concerned over the protection of their personal data. As such they are reading privacy policies, setting tight privacy settings and sharing as little information as possible.[16]

When defining modernized standards for data protection in the digital age, both categories need to be taken into account. For the first group a better protection starts by

14 Art. 2 para. 2 COM (2012) 11 final.

15 The right of the individuals to decide for themselves on the disclosure and use of personal data has been proclaimed by the *German Constitutional Court* as early as 1983 within its famous Census Decision of 15 December.

16 *Special Eurobarometer 359,* Attitudes on Data Protection and Electronic Identity in the *European Union*, published in June 2011, pp. 207-208, available at http://ec.europa.eu/public_opinion/index_en.htm, last viewed 02 March 2014.

raising awareness and setting a minimum standard of protection. This is for example the aim of new principles like privacy by design and privacy by default. For the individuals falling into the second category however, who a are still subject to harmful actions such as data mining and profiling although being proactive, the standards need to be set as high as possible. It is between these margins that the new piece of legislation attempts to define data subjects' protection.

In order to empower the data subject to a more meaningful expression of his will, the *Commission* introduced the need for an "explicit"[17] consent as a valid legal ground for lawful processing. It aimed at putting an end to the discussions around opt-in and opt-out models underlining that consent shall be given explicitly, by a statement or a clear affirmative action, so as to clearly indicate the data subject's wishes. Moreover, the Regulation states that, when "given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter".[18] But the effectiveness of such a provision may prove to be rather questionable in the context of the Internet and of the new technologies.

According to a Special Eurobarometer from 2011, 74% of Europeans regard the disclosure of personal information as an increasing part of modern life. Moreover, the survey also shows that 58% consider that there is no alternative other than disclosing of personal information if they want to obtain products or services.[19]

Against this background, the new provision of the Regulation according to which "consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller"[20] is very interesting. Such a situation may occur for example when the data subject is in a position of dependence from the controller. In such a case consent cannot be deemed as freely given.[21] This additional provision has not met the approval of the *European Parliament* and is prone to be suppressed taking the compromise amendments into consideration.

On the Internet, most of the commonly used online services are provided under standard terms of use, for which the consumer doesn't have any negotiating powers. *Yves Poullet* makes a very pertinent observation when talking about the privatization of cyberspace where big corporations are the ones establishing the rules of the game.[22] The same author notes that on the Internet "it is very difficult to refuse consent and that doing so is considered to be "somehow abnormal'" pushing thus the user to generally consent.[23]

So how much of a choice do we really have when the offer is: take it or leave it? One could argue, of course, that we are not forced to use specific products and services, such

17 Art. 4 para. 8 COM (2012) 11 final.
18 Art. 7 para. 2 COM (2012) 11 final.
19 Special Eurobarometer 359, p. 22.
20 Art. 7 para. 4 COM (2012) 11 final.
21 One possible example provided by the Regulation is that of data processing within the employment context. See Recital 34 COM (2012) 11 final.
22 Y. Poullet, *Data protection legislation: What is at stake for our society and democracy?*, in Computer Law & Security Review no. 25/ 2009, p. 211-226.
23 *Ibidem*, p. 224.

as those offered by Google for example. There are also other alternatives and thus a choice. But if finding a viable alternative becomes a time consuming endeavor, can we still speak of real choices anymore? Moreover, the most renowned facilities and services have acquired such a "must have" status, that social pressure and communication habits of our friends and partners would exclude us from a significant part of our digital relationships if not willing to subscribe to those most commonly used services.

In the end, it is the European legislators who hold the actual negotiating powers in their efforts to strike a balance between the interests of the citizens and the welfare of economic operators. *Europe* as a whole is consenting through legal instruments such as the proposed Regulation to certain practices it deems as admissible while banning others. The consent of the individual plays a rather small role defined within this framework and these limits.

2. Right of access and data portability

The proposed Regulation seeks to enhance control over one's data also through wider access and the ability to take the data with oneself. While the right of access is already known under Directive 95/46/EC, the right to data portability is one of the novelties introduced by the Regulation.

The right of access is to be regarded in connection with the principle of transparency. In order to be able to verify the lawfulness of the processing and the accuracy of the data, the subject needs to be able to know whether personal data about him is being processed by the controller or not and if yes, to have access to it. He should also receive information about the purposes of the processing, the recipients of the data in the case of transmissions, the logic and the consequences of that processing, for cases such as profiling.[24]

The right to data portability is however a totally new right, which appears necessary considering the numerous personal services now offered online. It prevents customer "lock-in" to a certain service and permits a shift to other similar services, thus enhancing the competitiveness on the internal market. This would allow the customer to "take his data" for example from Facebook and import it to another platform. The utility of such a right is easily recognizable considering that 71% of European Internet users deem it important for them to be able to transfer personal information when they decide to change providers or to stop using a service.[25]

According to the new Regulation there are two sides to data portability.[26] The first involves the right to obtain from the controller a copy of the processed data in an electronic and structured format, commonly used which also allows for further use. The second gives data subjects the right to transmit that data from one automated processing system to another, in cases where he provided the data and the processing is based on consent or a contract.[27] This idea might give rise to the broader discussion with regard

24 Art. 15 COM (2012) 11 final.
25 Special Eurobarometer 359, p. 160.
26 Art. 18 para. 1, 2 COM (2012) 11 final.
27 L. Costa, Y. Poullet, *Privacy and the regulation of 2012*, in Computer Law and Security Review no. 28/2012, p. 254-262.

to system interoperability, which does not yet exist in EU law and is more related to consumer protection and unfair competition than to the legal issues of data protection.[28] Following this line of thought, the *European Parliament* is however encouraging data controllers to develop interoperable formats in order to enable such portability.[29]

The *Council* has expressed a need to make clear that "the right to data portability shall be without prejudice to intellectual property rights in relation to the processing of the data in the automated processing systems". It also stressed the fact that portability shall apply only when processing is based on the consent of the data subject. It is not applicable in the cases when the processing operations are justified by the controller's legal obligation, by the vital interests of the data subject, by the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or by his legitimate interests.

While the *Commission* and the *Council* seem to share a preference for regulating the right to data portability through a separate provision,[30] *Parliament* opted for a merger of the rights to access and to data portability into one single provision, however without bringing any changes in substance.[31]

3. Right to be forgotten

One of the most controversial rights of the Regulation is the new right to be forgotten. Built on the existing right to deletion mentioned in article 12 b of Directive 95/46/EC, it is meant to address the fact that information, once published on the Internet, mostly remains to some extent electronically accessible even after having disappeared from the website where it was initially published. This new right for the digital age has generated extensive discussions, as it was said to constitute a justification of the claim to deletion of personal information from the Internet.

Under Directive 95/46/EC, data subjects have the right to rectification, erasure and blocking in case of processing operations, which do not comply with its provisions, "in particular because of the incomplete or inaccurate nature of the data".[32] Such a lack of compliance can also result from violations of the general rules on the lawfulness of the processing, including the infringement of the principles relating to data quality, of the criteria for legitimate data processing or of the conditions for processing special categories of data.

In article 17 of the Regulation the *Commission* proposes a "Right to be forgotten and the right to erasure". Whereas the first paragraph is a specification of the right to erasure under Directive 95/46/EC, the second one speaks of an obligation of the controller, if he has made the data public, "to take all reasonable steps, including technical measures,

28 P. De Hert, V. Papakonstantinou, *op. cit*., p. 138.
29 Recital 51 a *Parliament* amendments of COM (2012) 11 final.
30 According to Recital 55 COM (2012) 11 final "To further strengthen the control over their own data and their right of access, data subjects should have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain a copy of the data concerning them also in commonly used electronic format.
31 See article 15, as amended, entitled „Right to access and to obtain data for the data subject".
32 Art. 12 Directive 95/46/EC.

in relation to data for the publication of which the controller is responsible, to inform third parties which are processing the data, that a data subject requests them to erase any links to, or copy or replication of that personal data".

In reality and somehow in contradiction with the title of article 17, this key provision does not actually contain a right to be forgotten[33] but merely an obligation to inform third parties about the request of putting an end to any reproduction and about the request of erasure expressed by the data subject. It contains therefore an obligation of endeavor rather than an obligation of result, which would not lead to the actual deletion of the data. The *Commission* must have realized the infeasibility of an obligation of the controller to ensure the complete erasure of any public reference to some specific personal data. The more realistic nature of the proposed obligation of endeavor was also noted by the EDPS in its opinion on the reform package.[34]

Parliament however reopens the floor for discussions by amending this text so as to grant data subjects the right to "obtain from third parties the erasure of any links to, or copy or replication of the data".

4. Profiling

Directive 95/46/EC imposes a general right to object to "automated individual decisions" based solely on automated processing which produce legal effects or significantly affect a person by evaluating personal aspects such as the creditworthiness,[35] unless foreseen by a contract the data subject is a part of or by a legal provision, in both cases subject to appropriate safeguards put in place. The *Commission's* Regulation maintains this approach but enlarges the scope, from the protection with regard to automated decisions, to the protection in relation to profiling.[36]

The corresponding provision of the Proposal should however be understood as focusing not on the profiling operations themselves but on regulating measures, which are based solely on automated processing. The creation and use of profiles as such seem not to be specifically addressed. This appears to be more realistic than putting a specific type of data collection and processing technique under severe restrictions.

The *European Parliament's* response is to introduce a first definition of "profiling" in its compromise set of amendments. According to the legal definition "profiling means any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyze or predict in particular that natural

33 It is actually the draft version for the Regulation of November 2011 which contains such a true right to be forgotten, as follows: "Where the controller […] has made the data public, it shall in particular ensure the erasure of any public Internet link to, copy of, or replication of the personal data relating to the data subject contained in any publicly available communication service which allows or facilitates the search of or access to this personal data".

34 European Data Protection Supervisor, Opinion on the data protection reform package, Brussels, 7.03.2012, p. 24, point 127. Cf. generally on the right also contribution by *Spiecker gen. Döhmann*, Steuerung im Datenschutzrecht: Ein Recht auf Vergessen wider Vollzugsdefizite und Typisierung?, KritV 2014, in this special issue.

35 Art 15 para. 1 Directive 95/46/EC.

36 Art. 20 COM (2012) 11 final.

person's performance at work, economic situation, location, health, personal preferences, reliability or behavior".

After clearly determining what profiling means, the *Parliament* then delineates two types of regimes. In principle, profiling shall be permitted under the Regulation, under the reservation of a general right to object. The second, special regime refers to "profiling which leads to measures producing legal effects concerning the data subject or does similarly significantly affect the interests, rights or freedoms of the concerned data subject", which shall be prohibited unless certain conditions are fulfilled.

Meanwhile, the *Council* seems to support the idea of a general right to object to decision-making based on automated processing through profiling. It thereby follows the spirit of the *Commission's* proposal excluding a ban on the use of profiles as such, considering that such analytical methodology is an important part of the economic activities in the digital age.[37]

On the eve of a huge development in predictive analytics based on sophisticated profiling techniques, *Europe* is well inspired to adopt a "risk based approach" in regulating new prospective analytical tools and methods and to focus on the preservation of individual freedoms and rights and not on general prescriptive bans and rules which might rapidly prove to become inapplicable in practice.

5. *Improving redress mechanisms*

Empowering citizens is not just about granting them more rights but also about the existence of the ways, procedures and tools allowing them to enforce such rights and to make them effective. Some facts and figures easily reveal a general lack of awareness of data protection rights as well as the barriers to enforcement.

According to the special Eurobarometer,[38] 63% of Europeans have not even heard of a national Data Protection Authority responsible for helping them protect their rights. When it comes down to court proceedings, the lengths of such proceedings, the costs and the lack of legal experts in the field are considered to be significant barriers when seeking legal remedies against data protection violations.[39] One of the many reasons for this lack of knowledge is, as one lawyer from *Germany* puts it, "that perhaps violations of privacy rights entail non-quantifiable damage or only a quite small and uncertain quantifiable damage. This means that the incentive to use resources on that, I would say,

37 See the Note of the Presidency to the *Council* of the European Union no. ST 6762 2014 INIT of 24 February 2014, on the 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) [First reading], pp 6-7 available at http://register.consilium.europa.eu/content/out?lang=EN&typ=ENTRY&i=ADV&DOC_ID=ST%206762%202014%20INIT, last viewed 6 March 2014.

38 Special Eurobarometer 359, p. 174.

39 European Agency for Fundamental Rights, Access to data protection remedies in EU member states, report of 14 January 2014, p. 37, available at http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states, last viewed 25 February 2014.

to follow up such materially quite minor-seeming breaches of data protection like a spam e-mail or something similar, is extremely modest".[40]

There are many cases when a violation of data protection rules affects not only one single individual but many others in a similar situation. The introduction of a collective redress mechanism by the new Regulation represents the adequate answer to such concerns. This mechanism allows for any body, organization or association, which aims to protect data subjects' rights and interests concerning the protection of their personal data, to lodge a complaint with the supervisory authority of any member state on behalf of one or more data subjects.[41] Apart from the administrative side of collective redress against a supervisory authority, judicial remedies allow for class actions against the supervisory authority, the controller or the processor.[42]

The power of the supervisory authority to impose administrative sanctions, especially in the form of fines, as high as 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover,[43] coupled with the collective redress mechanism, may serve as a serious deterrence for data protection infringements in the future.

V. Increased responsibility of data controllers

1. The principle of accountability

The fact alone of empowering citizens and giving them more and stronger rights would not be enough in order to achieve the goal of increased effectiveness and less bureaucracy in the modernized EU Data Protection Framework in the absence of an enhanced responsibility of data controllers and processors. Time-consuming formal administrative procedures like the obligation to notify, as known under Directive 95/46/EC, have been replaced by putting more responsibility on the data controllers. Companies themselves should act responsibly for ensuring compliance with the new Regulation. We can thus identify a shift from a reactive to a proactive attitude towards data protection compliance. The newly introduced principle of accountability means that the controller should himself adopt adequate policies and implement appropriate measures to ensure and be able to demonstrate compliance in the processing of personal data.[44]

Defining accountability is by no means an easy task. In its basic meaning, accountability would signify "the existence of a relationship whereby one entity has the ability to call upon another entity and demand an explanation and/or justification for its conduct."[45] The Article 29 Working Party sees the emphasis in "showing how responsibility

40 *Ibidem*, p.50.
41 Art. 73 para. 2 COM (2012) 11 final.
42 Art. 74, 75, 76 para. 1 COM (2012) 11 final.
43 Art. 79 para. 6 COM (2012) 11 final.
44 Art. 22 COM (2012) 11 final.
45 J. Ahladeff et al., *op. cit*., p. 26, available at http://www.gini-sa.eu/index.php?option=com_content&view=article&id=54:scientific-papers&catid=37:publicationspresentations-&Itemid=10, last viewed 15 March 2014.

is exercised and making this verifiable".[46] In its paper on "The Future of Privacy" it pointed out to the two sides of accountability. It identified the obligation of the controllers to ensure the observation of the legal substantive principles and rules as well as the need to have the internal mechanisms to demonstrate such compliance.[47]

Whereas in its proposed Regulation the *Commission* gives concrete examples of measures through which to ensure accountability,[48] the *Parliament* prefers not to specify any of the measures expected from data controllers. Instead it lays out general guidelines according to which the measures that are to be determined would have to be taken into account "the state of the art, the nature of personal data processing, the context, scope and purposes of the processing, the risks for the rights and freedoms of the data subjects and the type of the organization". There is a need for the flexibility of the principle of accountability. Thus the suitability of measures has to be decided on a case-by-case basis, tailored to the concrete situation. The risk of the data processing and the nature of the data are two main factors that help determine the types of measures to be adopted by controllers.[49]

Essential elements of accountability are considered to be: organizational commitment and the adoption of internal policies consistent with external criteria; mechanisms to put privacy policies into effect, including tools, training, and education; systems for internal ongoing oversight and assurance reviews, and external verification; transparency and mechanisms for individual participation; and means for remediation and external enforcement.[50]

From the above we can easily conclude that accountability has many facets, not just the legal one. If the legal department of an organization may be the one responsible for drafting the privacy policies, the technology department may care for the implementation and maintenance of the appropriate equipment, while human resources may provide the training and education with regard to data protection. As a follow-up, internal audit and compliance may be then charged with verifying the practical implementation. Companies will have to implement measures on all mentioned levels in order to be able to ensure accountability and this seems to require also a proactive involvement of the top management.

46 Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability, WP 173, 13 July 2010, p. 9.

47 Article 29 Data Protection Working Party, The Future of Privacy…, p. 3.

48 According to art 22 para. 2 COM (2012) 11 final:
"The measures provided for in paragraph 1 shall in particular include:
(a) keeping the documentation pursuant to Article 28;
(b) implementing the data security requirements laid down in Article 30;
(c) performing a data protection impact assessment pursuant to Article 33;
(d) complying with the requirements for prior authorization or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);
(e) designating a data protection officer pursuant to Article 35(1).".

49 Article 29 Data Protection Working Party, Opinion 3/2010…, p. 13.

50 J. Ahladeff et al., *op. cit.,* p. 14.

2. *Responsibility through enhanced security*

Data security is of fundamental importance within the proposed Regulation, especially with a view to the many challenges brought by the extensive use of new technologies that allow for wide-scale data processing. Both the controller and the processor are bound by the obligation to implement appropriate measures so as to assure the security of the processing.[51] Such measures are of technical and organizational nature and they correspond to the risks of the processing and the nature of the personal data to be protected. Parliament expressly refers to the need of taking into account the results of the data protection impact assessment when deciding on such measures.

A new provision of the Regulation based on article 4 paragraph 3 of the e-Privacy Directive[52] introduces an obligation to notify personal data breaches. A personal data breach is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed".[53] Such breaches need to be notified to the supervisory authority[54] and also communicated to the data subjects, when they are likely to adversely affect the protection of the personal data or privacy.[55] Identity theft or fraud, physical harm, significant humiliation or damage to reputation, are seen as possible results that could trigger the obligation to communicate the data breach to the data subject.[56]

The obligation of the controller to document such breaches, as well as that to communicate them to the data subject affected, are further means of complying with the principle of accountability and the principle of transparency as set by the proposed Regulation.

3. *Increased security through technology: the new principles of data protection by design and data protection by default*

Considering that nowadays storing information has become cheaper than deleting it, there are hardly any incentives to do so. Safeguarding fundamental data protection principles such as data minimization and purpose limitation in the age of "big data" as many like to call it has become a significant challenge. The law itself does not suffice anymore in order to cope with that. Challenges brought by technology are to be solved with the help thereof. The proposed Regulation accordingly introduces two new principles, data protection by design and data protection by default, meant to help meet such challenges.

The principle of data protection by design goes back to privacy by design, a principle developed in the 1990 s by Ontario's Information and Privacy Commissioner *Ann Cavoukian*. According to it "privacy by design refers to the philosophy and approach of

51 Art. 30 COM (2012) 11 final.
52 Directive 2002/58/EC of the *European Parliament* and of the *Council* of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31.7.2002, p. 37–47.
53 Art. 4 para. 9 COM (2012) 11 final.
54 Art. 31 COM (2012) 11 final.
55 Art. 32 COM (2012) 11 final.
56 Recital 67 COM (2012) 11 final.

embedding privacy into the design specifications of various technologies".[57] Moreover privacy by design has to take into account the entire lifecycle management of the data.

Data protection by design requires the controller to implement appropriate technical and organizational measures and procedures to comply with the Regulation and ensure the protection of the rights of the data subjects. Such measures are to be considered both at the time when the means of the processing are determined and at the time of the processing itself.[58]

Parliament extended this obligation to processors and also amended the article by adding a paragraph so as to stress the fact that data protection by design should take into account the entire lifecycle management of the data "from collection to processing to deletion, systematically focusing on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data". Furthermore it made data protection by design a prerequisite for public procurement tenders.

The principle of privacy by design is a rather vague one, especially since the proposed Regulation is intended to be technology neutral. Further specifications of this principle can be found in recital 61, as amended by *Parliament*, which states: "The principle of data protection by design requires data protection to be embedded within the entire life cycle of the technology, from the very early design stage, right through to its ultimate deployment, use and final disposal. This should also include the responsibility for the products and services used by the controller or processor." Discussions are however still open. The change of the terms from "privacy by design" to "data protection by design" gave rise to the question as to whether data protection by design should be regarded as a specialization of the principle of privacy by design[59] and to the possible implications of such a shift.

Data protection by default relies on the data minimization principle[60] and on the purpose limitation principle. Thus, only those personal data should be processed which are necessary for each specific purpose of the processing. Also, data should not be collected or retained beyond the minimum necessary for that purpose, as regards the amount of data and its storage time.[61]

According to *Parliament*: "The principle of data protection by default requires privacy settings on services and products which should by default comply with the general principles of data protection, such as data minimization and purpose limitation". Data protection by default is a safeguard for everyone's privacy. It would allow for a minimum standard of protection even if the subject itself does not show any privacy concerns.

But there are many questions left unanswered regarding these two principles. One of them is whether, for example, data protection by design should apply only to controllers and processors or also to technology designers and producers. The Article 29 Working Party argued in favor of data protection by design being binding also for those who design and produce the technology.[62] Moreover, according to a decision of the *German*

57 A. Cavoukian, *Privacy by design*, Ontario, Canada, 2009, p. 3.
58 Art. 23 para. 1 COM (2012) 11 final.
59 L. Costa, Y. Poullet, *op. cit*., p. 260.
60 *Idem.*
61 Art. 23 para. 2 COM (2012) 11 final.
62 Article 29 Data Protection Working Party, The Future of Privacy:..., p. 3.

Constitutional Court, ICT should be designed and constructed in a way so as to avoid or minimize the amount of personal data that is processed. The *German Court* thus created a constitutional right to the confidentiality and integrity of information technology systems.[63]

4. The Data Protection Officer as an additional safeguard for responsibility

The controller's obligation of appointing a data protection officer (DPO)[64] as a measure contributing to the principle of accountability, underlines the shift from a prescriptive piece of legislation that puts a lot of burdens on enterprises, to one which allows for their creative freedom as regards the way they chose to ensure compliance.

The appointment of a DPO is compulsory in any case where the processing is carried out by a public authority or body.

In addition, the size of an enterprise can also trigger the obligation of having a DPO if the processing is carried out by an enterprise employing 250 persons or more. The amendment brought by *Parliament* widens the scope of this controversial provision by referring to a legal person instead of an enterprise and by adding a further trigger, when such processing relates to more than 500 data subjects in any consecutive 12-month period.

Moreover, a DPO needs to be appointed when the core activities of the processor or the controller consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.

Parliament amended this article by also adding one more situation when the appointment of a DPO is mandatory, namely, when the core activities consist of processing special categories of data, location data or data on children in large scale filing systems. An explanatory provision is added to recital 75 according to which archived data, which is restricted and thus not subject to normal access and processing and which can no longer be changed, should not be taken into consideration when establishing whether data about a large number of data subjects is processed.

The proposed Regulation puts a strong accent on the self-responsibility of data controllers which is generally attributed to the management of an organization, even if a DPO is appointed.[65]

VI. Conclusion

Already in 2010, the Article 29 Working Party identified a so-called "data-deluge effect"[66] according to which the amount of personal data that exists, that is processed and further transferred, continues to grow. This phenomenon was said to be favored by the growth of information and communication systems and by the increasing capability for

63 *German Consitutional Court* (BVerfG), judgement of 27 February 2008, 1 BvR 370/07 und 1 BvR 595/07.

64 Art. 35 COM (2012) 11 final.

65 Recital 75 COM (2012) 11 final, as amended by the EU *Parliament*.

66 Article 29 Data Protection Working Party, Opinion 3/2010 ..., p. 4.

individuals to use and interact with technologies. The Working Party therefore identified the strong need for data controllers to implement real and effective internal mechanisms to safeguard the protection of the information of individuals.[67]

Nowadays, the density and precision of our daily trails is very difficult to even grasp. Multiple converging causes have led to such a deluge of data. Endless technological possibilities combined with globalization and the sociological changes in the way people communicate and interact make the signals that we send out in the online world to be almost uninterrupted.

Against this background, the question is whether the Regulation is indeed able to address these challenges to privacy and data protection by empowering the citizens and making the controllers more responsible. Are the new rights and obligations properly redefined in order to cope with online reality? And what is the added value of the proposed Regulation as opposed to Directive 95/46/EC?

The main innovation identified is the trend to replace, to a large extent, the formalistic and excessively prescriptive approach of the Directive with a more balanced one, which builds on the shared responsibility of the key actors. There is a shift towards cultivating a data protection responsibility by allowing enterprises the freedom of choosing the means best tailored to them in order to achieve compliance. *Christopher Kuner* speaks of a "revolution in European data protection law by seeking to shift its focus away from paper-based, bureaucratic requirements and toward compliance in practice, harmonization of the law, and individual empowerment".[68]

The Regulation lays down solely the essential principles, thus avoiding becoming too detailed or too prescriptive.[69] It puts a strong emphasis on placing the controller in a position where he needs to take responsibility for his actions. At the same time it equips the data subjects with the proper tools to take control over their data and enforce their rights on- and off-line. It seeks not to put breaks to innovation and progress. On the contrary, burdensome paperwork and supervision are being replaced with self-regulatory incentives. Accountability and transparency go hand in hand so as to achieve better compliance.

One single set of rules applicable in the same way, the desire to fill gaps by enlarging the scope so as to cover companies not established in the EU, increased responsibility of controllers and more power over their data for citizens are the main positive developments of the proposed Regulation.

It may also put an end to the fragmentation of the means and powers presently recognized for the DPAs by their national laws. The focus is set on giving DPAs stronger and clearer roles and enhancing their active cooperation through the consistency mechanism. In combination with the one-stop-shop, which introduces a single point of contact for enterprises, these changes are most likely to facilitate personal data processing within the EU thus enhancing the internal market dimension.

---

67 *Idem*.

68 Ch. Kuner, *The European Commission's Proposed Data Protection Regulation*: *A Copernican Revolution in European Data Protection Law*, Privacy & Security Law Report, The Bureau of National Affairs, Inc., 6.12.2012, p. 1.

69 The new European Data Protection Board, which is set to replace the current Article 29 Working Party, shall elaborate further guidance and the *European Commission* shall contribute to a harmonized interpretation through delegated acts, if necessary.

Today, data protection must go beyond the national and even the European level and be aligned with global principles. The Regulation also addresses this need for a convergence of European data protection rules towards a more universal, more unified set of rules.

However, given the fact that data protection has become a field for legal as well as technology experts, there is a high risk that the average citizen will be overcome by a feeling of numbness and helplessness when it comes down to the protection of this personal data. Between the naivety of those who maintain that they have nothing to hide and the resignation of others who think that nothing can be done anymore, perhaps the Regulation will create a new horizon.