Forgetting about consent. Why the focus should be on "suitable safeguards" in data protection law

Gabriela Zanfir[1]

Working Paper
May 2013

University of Craiova
Faculty of Law and Administrative Sciences

[1] PhD candidate, Faculty of Law and Administrative Sciences, University of Craiova, Romania, e-mail: gabriela.zanfir@gmail.com. This work was supported by the strategic grant POSDRU/CPP107/DMI1.5/S/78421, Project ID 78421 (2010), co-financed by the European Social Fund—Investing in People, within the Sectoral Operational Programme Human Resources Development 2007–2013. The author would like to thank the Tilburg Institute for Law, Technology and Society for providing valuable support for her research during her research visit there.

Abstract

This paper explores the assumption that data processing based on consent is ancillary in the greater context of data protection, being only one of the six lawful bases for data processing. Moreover, the data protection draft regulation proposed by the European Commission in 2012 meets overwhelmingly the concerns regarding consent in data protection expressed on numerous occasions in the past years. Hence, the focus in data protection law should be, instead, on the development of efficient and clear provisions for handling data, which can be deemed as "suitable safeguards", regardless of the bases of their processing. For instance, the rights of the data subject – access, information, erasure etc., purpose requirements and accountability rules are effective in all of the situations of data processing. This article proposes a set of such suitable safeguards which match the content and the purpose of the right to data protection.

Key-words: consent, draft regulation, rights of the data subject, suitable safeguards.

1. Introduction

When one reads the proposal for a data protection regulation (DPR) released by the European Commission in 2012[2], one finds 56 references to the notion of "consent" (including the Preamble). By comparison, Directive 95/46[3] (DPD - Data Protection Directive) contains 12 such references. One explanation for the exponential growth of the regulation of consent is the energy put in the last decade into analyzing if and why consent is pivotal in data protection law in general[4], what does freely given, informed and

[2] European Commission, COM(2012) 11 final, "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)", (Brussels, 25 January 2012).

[3] Directive 95/46 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 November 1995), 31-50.

[4] See Article 29 Working Party, "Opinion 15/2011 on the definition of consent", WP 187; Roger Brownsword, "Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality", in *Reinventing Data Protection?* ed. Serge Gutwirth *et al.* (Heidelberg: Springer, 2009), 83–110; Lee A. Bygrave, Dag W. Schartum, "Consent, Proportionality and Collective Power, in *Reinventing Data Protection?*, ed. Serge Gutwirth *et al.* (Heidelberg: Springer, 2009), 157 – 173; Federico Feretti, "A European Perspective on Data Processing Consent through the Re-conceptualization of European Data Protection's Looking Glass after the Lisbon Treaty: Taking Rights Seriously", *European Review of Private Law* 2 (2012): 473–506; Daniel Le Métayer and Sarah Monteleone, "Automated consent through privacy agents: Legal requirements and technical architecture", *Computer Law & Security Review* Vol. 25, 2 (2009): 136 – 144.

unambiguous consent mean[5] or whether consent is revocable[6], just to give a few examples. Despite of all the attention consent enjoyed from academia and advisory bodies, the truth is that it represents just one of the six legal grounds to process personal data (one of five for sensitive data)[7]. Moreover, as Khitlinger showed, consent plays a limited role in the DPD's treatment of the requirements imposed on data controllers for data quality, fairness of processing or data security[8]. For instance, the controllers have to comply with obligations such as the one to inform the data subject pursuant to Article 10 and Article 11 of the DPD, regardless of the legal basis for the data processing.

Even in data protection's most legitimizing provision as a fundamental right, Article 8 of the Charter of Fundamental Rights of the European Union (the Charter), consent is enshrined as an alternative for the bases of fair processing. Article 8(2) of the Charter states that data must be processed "on the basis of the consent of the person concerned or some other legitimate basis laid down by law".

In addition, a significant part of the future data protection law in the European Union makes no reference whatsoever to consent: the proposal for a Directive regarding data protection in criminal matters[9] (the draft directive), also contained in the data protection reform package issued by the European Commission.

While this paper does not aim to minimize the role of consent in the legal philosophy of the informational self-determination, it proposes a more practical approach to what efficient protection of personal data means. In the end, informational self-determination can be considered as rooting in free will, which can be expressed by consent, withdrawal of consent, action or inaction with regard to the processing of personal data.

The first section of the article analyzes the *status quo* of consent in the Data Protection Directive (2), with references to the improvements brought by the DPR proposal, emphasizing the background value of consent as a legal basis for processing data in the European Union. After embracing the fact that there is more likely for data processing to happen under consent-free conditions than subject to consent, the second section looks at the aims of data protection and explores the ways to accomplish those aims (3). The final section will structure a possible set of "suitable safeguards" to keep the data

---

[5] See generally Neil C. Manson and Onora O'Neill, *Rethinking Informed Consent in Bioethics* (Cambridge University Press, 2007); Edgar A. Whitely, Nadja Kanellopoulou, "Privacy and informed consent in online interactions: Evidence from expert focus groups", International Conference on Information Systems (St. Louis, Missouri, 2010), available online at: http://www.encore-project.info/deliverables.html (Last accessed on October 20, 2012).

[6] See Liam Curren, Jane Kaye, "Revoking consent: a blind spot in data protection law?", *Computer Law and Security Review* 26 (2010), 273 - 283.

[7] Article 29 Working Party, WP 187, *supra* in note 4, p. 34.

[8] Mark F. Kightlinger, "Twilight of the idols? EU internet privacy and the postenlightenment paradigm", *Columbia Journal of European Law* 14 (2007-2008), 21.

[9] COM(2012) 10 final, 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.

processing fair, based on the current European data protection general legal framework, but also on the recent proposals for future data protection legislation: rights of the data subject, purpose requirements and accountability mechanisms (4). The conclusion (5) will show that the focus in giving effect to data protection law should be on stronger rights for the data subject, on clear purpose and time limitation related to it for data processing and on several rights of the data subject and correlative obligations of the controllers and processors, which are applicable regardless of the legal basis for the data processing.

2. The *status quo* of consent in the Data Protection Directive

Pursuant to Article 7 DPD, personal data may be processed only if the data subject has unambiguously given his consent, or processing is necessary for the performance of a contract to which the data subject is party, or processing is necessary for compliance with a legal obligation to which the controller is subject, or processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject. This enumeration means, in fact, that "most instances of processing will be able to be justified under the criteria in paras b-f of the provision"[10], which do not include consent.

The number of "or"-s offered as an alternative for data processing based on consent must be disappointing, *prima facie*, for all the data protection enthusiasts who link informational self-determination primarily to the consent of the individual concerned. They usually stumble upon the first enumerated criteria for lawful processing, a fact that was translated in the doctrine by considering consent "a cornerstone"[11] or "pivotal"[12] for data protection law.

When read carefully, Article 7 DPD reveals itself as allowing the processing of personal data on almost any ground, a door opened gradually from exceptions provided by law to the "legitimate interests pursued by the controller". The only criterion offered for assessing the legitimacy of the interests is a balance between them and the "interests for fundamental rights and freedoms" of the data subject, which is quite an evasive criterion.

[10] Lee A. Bygrave, *Data Protection Law*. *Approaching Its Rationale, Logic and Limits*, (Kluwer Law International, 2002), 66.
[11] See Feretti (n 4) at 484; See Le Métayer, Monteleone (n 4) at 136.
[12] See Manson and O'Neill (n 5) at 112; They are referring to the UK Data Protection Act, which transposes the provisions of the Data Protection Directive, stating that the Act "assigns individual consent a large, indeed pivotal role in controlling the lawful acquisition, possession and use of personal information"; See also Brownsword (n 4) at 109.

The alternative prerequisites are formulated broadly, thereby reducing significantly the extent to which data controllers are hostage to the consent requirement in practice[13].

2.1 The unsettled position of consent

The attributes envisaged for consent in the Data Protection Directive – "freely given", "specific", "informed and unambiguous" were subject to doctrinal debates[14] and to the intervention of the Article 29 Working Party[15].

Even the authors who consider data processing consent a crucial component of data protection law which gives effect to the goal it purports, admit that the way in which it is currently devised in the law and its application provide an insufficient protection for individuals and an inadequate safeguard for the values it aims to protect *vis-à-vis* the realities of marketplace practices and economic interests[16]. Moreover, as Bygrave and Schartum explain, a large range of extra-legal factors undermines the privacy interests that consent mechanisms are supposed to promote or embody, as the degree of choice presupposed by these mechanisms will not often be present for certain services or products, particularly offered by data controllers in a monopoly or near-monopoly position[17].

Taking into account consent is considered to "remain key to inform a properly functioning policy for the enhancement of individual autonomy"[18] and that its concrete mechanisms are, nevertheless, unclear, academics sought solutions to make consent rules work properly. They proposed the insertion of "collective consent"[19] in data protection law, or even "privacy agents"[20] who are to handle other people's consent, besides solutions like removing the psychological barriers to provide consent by providing comprehensive normative disclosure limits, making it explicit that data subjects may always be allowed to refuse consent or withdraw it at a later stage without negative consequences or strings attached[21].

In the DPR proposal, the European Commission clarifies most of the concerns regarding the conditions for valid consent, while distributing it, in a form or another, throughout the whole act as a sign of strengthening the position of the data subject with

[13] See Bygrave (n 10) at 66.
[14] See Le Métayer and Monteleone (n 4) at 139.
[15] See Article 29 Working Party, "Opinion 15/2011 on the definition of consent" (n 4).
[16] See Feretti (n 4) at 505.
[17] See Bygrave and Schartum (n 4) at 160. In line with their idea, Feretti (n 4) at 488, also makes a point from underlying that "the inclusion of data processing consent in the general terms and conditions of sale or services can be a common, yet subtle or elusive, method of obtaining consumer consent notwithstanding whether a transaction occurs online and irrespective of the opt-in/opt-out dichotomy".
[18] See Feretti (n 4) at 500.
[19] See Bygrave and Schartum (n 4) at 170.
[20] See Le Métayer and Monteleone (n 4) at 140-142.
[21] See Feretti (n 4) at 501.

regard to data processing, even if, *de facto*, its role is still an alternative to other forms of lawful processing.

2.2 The reply of the DPR proposal

The proposal for a Data Protection Regulation has been received extremely different by privacy specialists. While some see it as failing to provide either significant legal certainty or simplification, adding administrative burden and leaving a substantial risk of fragmentation[22], others see it as a "cause for celebration for human rights" [23], considering that "once finalized the new instrument is expected to affect the way Europeans work and live together"[24]. Surprisingly, though, both extreme approaches agree on one point: the provisions for consent have been significantly improved.

The skeptics underline that the draft regulation "helpfully removes the unnecessary and confusing distinction between *explicit* consent and other consent (see Articles 8 and 7 of the DPD, respectively)"[25], while the others also consider that the Commission substantially reinforced the individual consent requirement, enhancing its definition by means of requiring explicit consent[26].

Thus, the new definition of consent is considered clarifying, especially if read in conjunction with Recital 25 of the draft regulation[27]. According to Article 4(8) of the DPR proposal, "the data subject's consent means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed".

Consent is again enumerated as one of the six bases for lawful data processing in Article 6(1), point a), of the draft regulation, which proposes an interesting addition by declaring that consent is such a lawful basis if it is given "for one or more specific purposes".

One of the most important innovations of the draft regulation are the clear conditions for consent in Article 7, as it introduces procedural provisions regarding the proof of the data subject's consent – the burden of proof shall be beard by the controller, the explicit option of the data subject to withdraw consent and rules intended to counter-balance the power positions held by some controllers, such as employers. Hence, consent

---

[22] Peter Traung, "The Proposed New EU General Data Protection Regulation", *CRi* 2 (2012): 33.
[23] Paul de Hert and Vagelis Papakonstantinou, "The proposed data protection Regulation replacing Directive 95/46: A sound system for the protection of individuals", *Computer Law & Security Review* 28 (2012): 142.
[24] Id. 131.
[25] See Traung (n 22) at 38.
[26] See de Hert and Papakonstantinou (n 23) at 135.
[27] Recital 25 specifically states that silence or inactivity should not constitute consent and that consent is considered as being explicitly given either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data.

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. All of these improvements regarding the conditions for consent are responses to the critiques of the provisions in the DPD[28]. However, there are already concerns regarding the entering into force of Article 7 as it is currently drafted, exactly because the requirements towards data processors appear to be quite demanding[29].

But what is indeed remarkable regarding consent in the DPR proposal is its widespread echo throughout the whole draft. While the DPD only specifically refers to consent in Article 2 – its definition, Article 7 – lawful processing basis, Article 8 – sensitive data and Article 26 – derogation rules for data transfers to third countries without an adequate level of protection, the draft regulation introduces a panoply of functions for consent individually or for processing pursuant to consent, with regard to the processing of personal data of a child (Article 8), the right to be forgotten (Article 17), the right to data portability (Article 18), measures based on profile (Article 20) and processing for historical, statistical and scientific research papers (Article 83). However, perhaps the most intense effect given to consent in data protection law is the administrative sanction provided by Article 79(6)(a), according to which "the supervisory authority shall impose a fine up to 1.000.000 EUR or, in case of an enterprise up to 2% of its annual worldwide turnover, to anyone who, intentionally or negligently (…) does not comply with the conditions for consent pursuant to Articles 6, 7 and 8".

As a preliminary conclusion, the draft regulation is generous with consent rules. However, consent still represents only one of the six justifications that allow personal data to be processed. In addition, where consent is mentioned in other provisions of the DPR proposal, it also has the nature of an "alternative". Now that the vast majority of concerns regarding consent were met by the draft regulation, it is time for data protection law to find a practical pivotal concept, or cornerstone, which must be directly linked to the object of the right to personal data protection.

2.3 Putting data processing based on consent in context

Profiling has been defined as "the process of discovering correlations between data in databases that can be used to identify and represent a human or nonhuman subject

[28] Even the European Commission criticized the effects in practice produced by the wording of the Data Protection Directive regarding consent, in a 2011 report: "(…) these conditions are currently interpreted differently in Member States, ranging from a general requirement of written consent to the acceptance of implicit consent. Moreover, in the online environment – given the opacity of privacy policies – it is often more difficult for individuals to be aware of their rights and give informed consent. This is even more complicated by the fact that, in some cases, it is not even clear what would constitute freely given, specific and informed consent to data processing, such as in the case of behavioural advertising, where internet browser settings are considered by some, but not by others, to deliver the user's consent". See COM(2010) 609 final, "A Comprehensive Approach of Data Protection in Europe" (4 November 2010), 8-9.

[29] See de Hert and Papakonstantinou (n 23) at 136.

(individual or group) and/or the application of profiles (sets of correlated data) to individuate and represent a subject or to identify a subject as a member of a group or category"[30]. Thus, gathering of data is quintessential for profiling. This procedure is one of the main concerns of privacy advocates nowadays[31]. To meet this concern, the DPR proposal makes a specific reference to "profiling" in Article 20, building on Article 15 DPD, which regulates "automated individuals decisions".

Recital 58 of the Preamble in the DPR proposal explains the conditions under which this special kind of data processing is lawful: "Every natural person should have the right not to be subject to a measure which is based on profiling by means of automated processing. However, such measure should be allowed when expressly authorized by law, carried out in the course of entering or performance of a contract, or when the data subject has given his consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child".

The extrapolation of these rules to data processing in general explains in a few words the philosophy of data protection law: every natural person should have the right not to be subject to processing of personal data, unless such processing has a lawful basis – which can be a legal provision, consent or other specific condition stipulated by data protection law, and unless the processing is subject to "suitable safeguards". This means that irrespective of which is the lawful basis for data processing, it must be clear that the individual has some degree of control, pursuant to his or her right to informational self-determination, upon the processing of personal data and that the processing must comply with specific, explicit safeguards so that the fundamental rights of the individual are observed.

For instance, Kightlinger, one of the most vehement critics of consent in European data protection law, argues that under the DPD, the informed consent is never sufficient to ensure that a website operator (he might as well refer to any other type of controller) may collect and use the person's personally identifiable information[32] lawfully and that, as far as the transfer of personal data to third countries is concerned, the consent of the individual

---

[30] Mirelle Hildebrandt, "Defining Profiling: A New Type of Knowledge?" in *Profiling the European Citizen,* ed. Mirelle Hildebrandt and Serge Gutwirth, (Springer, 2008), 19.

[31] See, for instance, Tal Zarsky, "Responding to the Inevitable Outcomes of Profiling: Recent Lessons from Consumer Financial Markets, and Beyond", in *Data Protection in a Profiled World*, ed. Serge Gutwirth, Yves Poullet and Paul de Hert (Springer, 2010), 53 – 75; Mirelle Hildebrandt, "Profiling and the rule of law", 1 *Identity in the Information Society* 1 (2008): 55 – 70.

[32] In the American legal system, personal data is often regarded as personally identifiable information. However, the Consumers' Privacy Bill of Rights released in 2012 by the White House opts for the expression "personal data"; see in this regard Gabriela Zanfir, "EU and US Data Protection Reforms. A Comparative View" in *7th Edition of The International Conference "The European Integration, Realities and Perspectives" Proceedings* (2012), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2079484 (accessed on February 26, 2012).

plays no role[33]. This happens because the Directive imposes "a panoply of obligations" on operators that have little or nothing to do with a person's consent, including the duty to obtain a license from a DPA, to satisfy the data quality principles, to grant to individuals access to processed data, or to provide information to the individual prior to the processing[34]. He concludes that consent can safely take a "back seat", because it is the job of data protection authorities, not the individual, to protect privacy of personally identifiable information from threats posed by data controllers and possibly from the negative consequences of the individual's own consensual decisions[35].

While it is true that data protection authorities (DPAs) play an important part in making sure that the data protection provisions are complied with, the supposition that only DPAs are in charge is erroneous. The most obvious counterarguments are the legal remedies and liability rules in Articles 22 and 23 DPD which allow actions for damages in national courts "as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive". Hence, the individual also has an important part in making sure that controllers are engaged in lawful processing operations[36]. In addition, the individual has a few "weapons" accorded to him by data protection law: the rights to intervene directly in the process of processing. So, why shouldn't the focus be on "sharpening" those rights?

Another critique of the central position of consent in conceptualizing data protection can be derived from the idea that, especially in the online world, the reliance on consent for the processing of personal data or the carrying out of an action that would otherwise constitute a violation to the privacy of the data subject does not always safeguard protection of his privacy[37]. For instance, it was revealed that, in practice, only a fraction of internet users read the privacy notices that precede the collection of their informed consent[38]. As Brownsword argued, such consents are "reduced to a bureaucratic process, where the collection of informed consent is carried out in a casual way, and where we succumb to the temptation to make use of consent as a lazy justification"[39]. A probable antidote to the "lazy justification" reality would be, as Kosta construed, asking data controllers to justify their actions not only on the basis of the consent of their users, but

[33] See Kightlinger (n 8) at 21.
[34] Id. at. 20.
[35] Id. at 29.
[36] For instance, in a famous case in Romanian courts, an individual received a 10.000 EUR compensation for moral damages, caused by the publication of details regarding his health condition on the website of the Municipality of Sector 1 of Bucharest as a justification for the individual receiving a public transportation free pass; he based his allegations on the provisions of Law No. 677/2001 which transposes into national law the Data Protection Directive; (See Jud. sect. 1 Bucureşti, sentinţa civilă din 16.03.2009, irevocabilă).
[37] Eleni Kosta, "Unraveling consent in European Data Protection legislation. A prospective study on consent in electronic communications", Doctoral Thesis, submitted on June 1, 2011, Faculty of Law, K.U. Leuven, Interdisciplinary Center for Law and ICT, 315.
[38] Brendan Van Alsenoy, Eleni Kosta, and Jos Dumortier, "D6.1 – Legal requirements for privacy-friendly model privacy policies", *The IWT SBO SPION Project*, 31.
[39] Roger Brownsword, "The cult of consent: fixation and fallacy", *King's Law Journal* 15 (2004): 224.

also stroking a balance between the controllers' legitimate interests and "the right of the users"[40].

Last, taking into account also that even when data processing is based on consent problems appear in practice, in the sense that "not only consent may be implied or data processed on the basis of opt-out practices, but it may also be traded for perceived immediate economic advantages, or it may be taken contractually or as part of the general terms and conditions of a contract"[41], and that currently "information is automatically processed to an extent not dreamed of when the need for data protection law was first accepted"[42], the next section will look into the object of the right to the protection of personal data with the purpose of identifying safeguards suitable to comply with this right.

3. The object of the right to the protection of personal data

The right to the protection of personal data has been recognized as such in Article 8 of the Charter after a 30 years history of regulating data protection in Europe[43]. It became clear that, at least in the European Union, this right protects something distinct than private life, as Article 7 of the same Charter expressly protects private life. Having two provisions that share an identical object is illogical. Therefore, what does the right to the protection of personal data protect?

A good way to answer the question is to first categorize the substances of the two rights envisaged. A valuable approach is to see them in terms of "opacity tools" vs. "transparency tools"[44]. Opacity tools protect individuals, their liberty and autonomy against state interference and also against interference from other private actors, this being an accurate description of the legal effects of the right to private life enshrined in Article 7 of the Charter[45]. Transparency tools limit state powers by devising legal means of control of these powers by the citizens, by controlling bodies or organizations and by the other state powers, which is what Article 8 of the Charter does by organizing the channeling, control and restraint of the processing of personal data[46].

Following the same line of reason, Gomes de Andrade showed that the main difference between the right to privacy and the right to data protection is that the first one

[40] Kosta (n 37) at 315.
[41] See Feretti (n 4) at 476.
[42] See Brownsword (n 4) at p. 99.
[43] For the beginning of data protection regulation in Europe, see Frits W. Hondius, *Emerging Data Protection in Europe* (North-Holland Publishing Co. and American Elsevier Publishing Co, 1975). For the generational evolution of data protection laws in Europe, see Viktor Mayer-Schönberger, "Generational Development of Data Protection in Europe", in *Technology and Privacy: The New Landscape*, ed. Philip E. Agre and Marc Rotenberg (The MIT Press, 1998), 219-242.
[44] Serge Gutwirth and Paul de Hert, "Regulating Profiling in a Democratic Constitutional State", in *Profiling the European Citizen,* ed. Mirelle Hildebrandt and Serge Gutwirth, (Springer, 2008) 271 – 303.
[45] Id. at 276-278.
[46] Id. at 276-278.

is substantive and the other one is procedural. "Substantive rights are created to ensure the protection and promotion of interests that the human individual and society consider important to defend and uphold. Procedural rights operate at a different level, setting the rules, methods and conditions through which substantive rights are effectively enforced and protected"[47]. Therefore, even if the enactment of the first data protection rules can be considered a consequence of the affirmation of the right to private life, conceived at the beginning in a narrow understanding, data protection "gradually overflowed this context and assumed a role vis-à-vis all the freedoms enshrined in the European Convention on Human Rights"[48]. Data protection, as such, "does not directly represent any value or interest *per se*, it prescribes the procedures and methods for pursuing the respect of values embodied in other rights – such as the right to privacy, identity, freedom of information, security, freedom of religion, etc."[49] These are the grounds for data protection to be considered "a catch-all term for a series of ideas with regard to the processing of personal data; by applying these ideas, governments try to reconcile fundamental but conflicting values such as privacy, free flow of information, the need for government surveillance, applying taxes, etc"[50].

It was acknowledged in the literature that the objective of the data protection regulation in general is to protect individual citizens against unjustified collection, storage, use and dissemination of their personal details[51]. Hence, data protection is pragmatic: it assumes that private and public actors need to be able to use personal information, as it is often necessary for societal reasons[52].

To answer the question raised earlier, the right to the protection of personal data has as object, just as its name clearly suggests, the protection itself of the personal data being processed, and not private life in general or personal data in particular. As uncommon *a right that protects a protection* sounds, there could be no other way to better express the procedural nature of such a right. It indeed encompasses mechanisms of protection: principles for lawful and fair processing, "interventional" rights of the data subject, data quality rules and accountability rules.

As a preliminary conclusion, the right to data protection, in fact, assumes the inherent nature of processing personal information in the modern society. It is not its purpose *per se* to preclude such processing or to give an absolute right to the individual to

---

[47] Norberto Nuno Gomes de Andrade, "Oblivion, the right to be different from oneself. Reproposing the right to be forgotten", *Revista de Internet, Derecho y Politica* 13 (2012): 125.

[48] Yves Poullet, "Pour une troisième génération de réglementation de protection des données, dans Défis du droit à la protection à la vie privée", coll. *Cahiers du Centre de Recherches Informatique et Droit*, 31 (Bruxelles: Bruylant, 2008), 41.

[49] Norberto Nuno Gomes de Andrade (n 76) at 125.

[50] Paul de Hert and Serge Gutwirth, "Data protection in the case law of Strasbourg and Luxemburg: Constitutionalism in action", in *Reinventing Data Protection?*, ed. Serge Gutwirth *et al.* (Heidelberg: Springer, 2009), 3-44.

[51] Peter Hustinx, *Data protection in the European Union*, Privacy & Informatie 2 (2005), 62.

[52] See de Hert and Gutwirth, (n 50) at 3.

object by means of his or her consent to the processing of personal data. Its object is to provide mechanisms of protection or "suitable safeguards" for individuals with regard to the processing of their data. Section 4 of this paper will have a look into which are the categories of "suitable safeguards" in data protection law, calling for a deeper analysis of their legal background and an enhanced attention to their future development.

4. A new "cornerstone" for data protection law: the suitable safeguards

In order for its protection to be effective, the content of a subjective right, which represents "a prerogative or a bundle of prerogatives"[53] accorded to the subject of the right, must be appropriate for safeguarding the object. The previous section contributed to the identification of the object of the right to the protection of personal data and this section identifies the bundle of prerogatives accorded to the data subject, which are veritable safeguards suited to the protection of personal data – "suitable safeguards".

The most concise and encompassing provision in EU positive law with regard to the protection of personal data is Article 8 of the Charter. Hence, it is sensible to start the search for "suitable safeguards" with this provision, even though most of them were developed since the first enactment of data protection laws in Europe[54]. The second paragraph of Article 8 provides that personal data "must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified".

The first point to be made is that, even though the bases for lawful processing are mentioned in Article 8(2), they should not be included in the category of "suitable safeguards" in the sense analyzed by this paper. They represent more than suitable safeguards, as they allow the processing itself, while the safeguards are the bundle of prerogatives accorded to the data subject so that the procedural object of protecting personal data is protected itself. Therefore, pursuant to paragraph 2 of Article 8, the suitable safeguards must first be looked for in the rights of the data subject, on one hand, and in the principles for fair processing and purpose requirements, on the other hand.

The rights of the data subject are already systemized and structured in a well delimited set of prerogatives, and each of them is important for the realization of data protection.

---

[53] Jean Dabin, *Le Droit Subjectif*, (Paris: Dalloz, 2007), 168.

[54] See generally Adriana C. M. Nugter, *Transborder Flow of Personal Data within the EC* (The Netherlands: Springer, 1990). The volume analyzes some of the first data protection laws in Europe – *Bundesdatenschutzgesetz* (Germany, 1977), *Loi relatif a l'informatique, aux fichiers et aux libertes* (France, 1978), *Data Protection Act* (UK, 1984) and *Wet Persoonsregistraties* (The Netherlands, 1989), all of them containing provisions with regard to the specific rights of the data subjects and correlative obligations of the data processors. Information and access rights were omnipresent, while the first European data protection laws contained some variations of the right to object, the right to erasure and the right to correction.

With regard to the principles of fair processing and purpose requirements, it must be observed that Article 6 DPD – under the "Principles relating to data quality" section, is built around the concept of purpose limitation. The only paragraph of Article 6 DPD which does not expressly mention "purpose" is paragraph 1(a), which is a general provision, merely requiring the data processing to be lawful and fair. Thus, purpose requirements are functional and central for fair processing, and they can be converted in a palpable prerogative.

Article 8(3) of the Charter states that "compliance with these rules shall be subject to control by an independent authority". Thus, it refers to a form of accountability. However, accountability in data protection is more complex than the mere control of the data protection authorities. Such a fundamental provision indicates, nevertheless, that accountability plays an important part in the protection of personal data, beyond the general accountability of the "debtors" of correlative obligations stemming from the rights in the Charter. As such, the Charter itself provides a further incarnation of accountability in general in Article 47, which states that everyone whose rights and freedoms guaranteed by the law of the Union are violated "has the right to an effective remedy before a tribunal". The importance of accountability in data protection is highlighted by its extensive regulation in the DPD, under the chapter of "judicial remedies, liability and sanctions", which is further developed and structured in the DPR proposal.

Taking all these considerations into account, the "suitable safeguards" encompassed by the right to the protection of personal data can be structured as such: the rights of the data subject (4.1), the purpose requirements (4.2) and the mechanisms of accountability (4.3). Each of them will be shortly referred to.

4.1 Rights of the data subject

A core principle of data protection laws in general is that persons should be able to participate in, and have a measure of influence over, the processing of data on them by other individuals or organizations[55]. One of the outcomes of this principle are the consent rules, which were found in the previous sections as being limited with regard to the self-determination of the data subject. However, "the Directive insists on the participation of data subjects even where their consent is not needed"[56], and it does so by enforcing a set of specific rights: the right to be informed (Articles 10 and 11), the right to access the processed data and to receive a copy of them (Article 12(a)), the right to object to data processing (Article 14), the right not to be subject to fully automated decisions based on data processing (Article 15), the right to have the data rectified, erased or blocked (Article

[55] See Bygrave (n 10) at 63.

[56] Spiros Simitis, "Data Protection in the European Union – The Quest for Common Rules", in *Collected Courses of the Academy of European Law,* Vol. VIII-1 (European University Institute: Kluwer Law International, 1997), 130.

12(b))[57], to which the right to a judicial remedy (Article 22) can be added, although it is more strongly connected with the accountability of the controller[58].

It has been noted that the purpose of these rights is "to permit the persons concerned to follow and correct processing"[59]. Thus, the rights of the data subject are prerogatives which allow the individual to control the way in which his or her personal data are processed, regardless of the legal basis of the processing. Nevertheless, except for the right to a judicial remedy, all of these prerogatives are subject to certain limitations[60].

Previous literature shows that "the Commission in its draft Regulation has taken bold steps for the improvement of the data subjects' position in contemporary personal data processing conditions"[61] and that the main achievement to this end is that their rights "have been strengthened and data controllers' obligations have been increased respectively"[62]. Despite of the enhancement of the provisions regarding the rights of the data subject, these particular safeguards need to be further clarified with regard to their scope and their restrictions.

The DPR proposal contains a chapter dedicated to the "Rights of the data subject" (Chapter 3), which further details and enhances the already existing rights and adds the right to be forgotten and the right to data portability in the panoply of data protection rights. However, none of the two are completely new to data protection law, as both have roots in the DPD, within the right to erasure and the right to receive a copy of the processed data respectively. According to the first draft report on the DPR proposal of the Committee on Civil Liberties, Justice and Home Affairs[63] of the European Parliament, Article 18 is proposed for deletion and its content is moved under Article 15 – "the right to access".

The DPR proposal introduces in Article 12 rules regarding the procedures and mechanisms for exercising the rights of the data subject, including means for electronic requests, requiring response to the data subject's request within a defined deadline, and the motivation of refusals[64]. While such specific rules are welcomed, paragraph 3 of this article hampers the efficiency of the rights of the data subject, as it specifically allows the

---

[57] For a comprehensive analysis of these rights enshrined in the DPD and also in Directive 2002/58 on privacy and electronic communications, see Douwe Korff, *Data Protection Laws in the European Union* (Federation of European Direct Marketing and Direct Marketing Association, 2005) at 71 - 144.

[58] For instance, the Romanian law transposing Directive 95/46, Law no. 677/2001 for the protection of persons with regard to the processing of personal data and the free movement of such data, enshrines in art. 18 "The right to a judicial remedy", under Chapter IV – "The rights of the data subject in the context of personal data processing".

[59] See Simitis (n. 56) at 131.

[60] See Articles 13(1), 14(a) and 15(2) DPD.

[61] See de Hert and Papakonstantinou (n 23) at 141-142.

[62] Ibid.

[63] Committee on Civil Liberties, Justice and Home Affairs, "Draft report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation", (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), December 17, 2012.

[64] See para. 3.4.3.1. from the Explanatory Memorandum of the DPR Proposal.

controller to refuse to take action on the request of the data subject, as long as the data subject is informed of the reasons for refusal and on the possibilities for a judicial or administrative remedy.

The rights of the data subject are systemized in the draft Regulation in three categories: 1) information and access (the right of the data subject to be informed - Article 14, and the right of access to data - Article 15), 2) rectification and erasure (the right to rectification- Article 16, the right to be forgotten and to erasure[65] - Article 17, the right to data portability[66] - Article 18) and 3) the right to object and profiling (the general right to object – Article 19, and the right not to be subject to profiling – Article 20).

While the strengthening of the rights of the data subject has been one of the main data protection reform themes, on a closer look their proposed provisions lead to uncertainty and often limit the scope of the rights. For instance, it is true that the right of the data subject to be informed contains, due to the draft regulation, a more consistent set of compulsory details to be provided by the controller to the data subject. However, Article 14(5) provides that this right shall not apply where the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort. Similarly, Article 14(5)(c) limits the scope of the right to be informed by excluding from its application the situation of indirect collection of data where it is expressly laid down by law, without requiring further safeguards.

These specifications considerably soften the "teeth" of the provision, as nowadays the cases in which data are collected from other sources than the data subject are numerous. By contrast, the DPD contained a specific provision which covered the information of the data subject when the data were indirectly collected. While the first limitation is also present in Article 11(2) DPD, it is made clear there that it should apply in particular for processing of data for statistical or research purposes. Perhaps the biggest difference between the current provision and the proposed one is the moment of making the information available to the data subject. While Article 11(1) DPD states that the information must be made available "at the time of undertaking the recording of personal data", Article 14(4)(b) of the DPR proposal provides that the information can also be made "within a reasonable period after the collection". This provision obviously hampers the

[65] For a critique of the provision of a right to be forgotten in the data protection reform package see Jeffrey Rosen, "The Right to Be Forgotten", 64 *Stanford Law Review Online* 88 (2012); See also Jef Ausloos, "The Right to be Forgotten – Worth Remembering?", *Computers Law and Security Review* 28 (2012): 143-152; Bert Jap Koops, "Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right to be Forgotten" in Big Data Practice", *Tilburg Law School Legal Studies Research Paper Series* 8 (2012).

[66] For an introductory study about the right to data portability as it is enshrined in the DPR proposal, see Gabriela Zanfir, "The right to data portability in the context of the EU data protection reform", *International Data Privacy Law*, Vol. 2, No. 3 (2012), 149-163; For a critique of the right to data portability see Peter Swire and Yanni Lagos, "Why the right to data portability likely reduces consumer welfare: Antitrust and Privacy critique", *Maryland Law Review forthcoming*, available online at http://ssrn.com/abstract=2159157, (Last accessed on February 26, 2013).

lawful processing of personal data based on consent, when the data is not collected directly from the data subject[67].

Another problem of the rights provisions in the DPR proposal is the use of subjective, unclear, criteria for assessing their proper application, such as "the essence of the right to the protection of personal data"[68], "structured and commonly used format"[69] or the "reasonable period" previously mentioned.

The European Data Protection Supervisor (EDPS) formally criticized in its Opinion on the data protection reform package the approach taken by the Commission with regard to the restrictions of the rights of the data subject. The EDPS considers that the scope of possible restrictions has been considerably expanded in comparison to what is currently provided in Article 13 DPD, as all the rights of the data subject can now be restricted due to Article 21 DPR proposal, including the right to object and the measures based on profiling[70]. For instance, the EDPS called for restricting the use of the public interest exemption to clearly identified and limited circumstances including criminal offences or economic financial interests[71].

The effectiveness of the rights of the data subject is without a doubt a suitable safeguard for fair data processing, the more so as the proposal of a Directive for data protection in criminal matters also provides for a similar set of rights, adapted to the sensitive area of its general scope. The draft Directive recognizes the rights to information, access, rectification, erasure and restriction of processing[72] and it also makes a reference to profiling measures[73].

4.2 Purpose requirements

Purpose requirements are of paramount importance for processing personal data, as the purpose for processing data is equivalent to a guiding force of the whole "process of processing". Four of the five principles related to data quality enshrined in Article 6 DPD

[67] For instance, such a situation can easily be imagined in the context of database transactions between data brokers. See Natasha Singer, *You For Sale: Mapping, and Sharing, the Consumer Genome*, New York Times (June 16, 2012) available at: http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html?_r=1&pagewanted=all (Last accessed on February 28, 2013).
[68] Article 17(3)(d) of the DPR proposal.
[69] Article 18(1) of the DPR proposal.
[70] Opinion of the European Data Protection Supervisor on the data protection reform package issued on March 7, 2012, para. 160.
[71] Id., para. 159.
[72] Articles 11 to 16 of the proposal for a Directive 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.
[73] Article 9 of the draft Directive.

revolve around the purpose of the processing[74]. In addition, the legal definition of "controller" has as point of reference the purpose of the processing[75].

One of the unanimously recognized data protection principles is the principle of purpose specification. It is considered to be a cluster of three principles: the purposes for which data are collected shall be specified/defined; these purposes shall be lawful/legitimate; and the purposes for which the data are further processed shall not be incompatible with the purposes for which the data are first collected[76]. Moreover, the obligation to connect the processing to a particular purpose predeterminates the selection of the data and confines their use[77].

The data protection reform package confirms the pivotal role of purpose specification and purpose limitation in data protection law. Both the draft regulation and the draft directive provide that personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes"[78].

Other common rules are that the processed data must be adequate, relevant, and not excessive in relation to the purposes for which they are processed and that all the reasonable steps must be taken to ensure that the personal data are inaccurate, having regard to the purpose of the processing[79]. The draft regulation adds a very important condition, a proportionality rule, which circumscribes the material scope of lawful data processing by establishing that personal data shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data[80]. Moreover, the rule of lawful processing pursuant consent in Article 6(1)(a) is directly linked to the "specific purposes" of the data processing.

Another essential requirement related to the processing purpose is that data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed[81].

All of these requirements are currently enshrined in Article 6 DPD, except the express proportionality rule. According to the EDPS, the effectiveness of the purpose limitation principle depends on (1) the interpretation of the notion of 'compatible use' and (2) the possible derogations to the purpose limitation principle, in other words, the

[74] Article 6(1)(b),(c),(d),(e) of the Data Protection Directive.
[75] According to Article 2(d), (d) "'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data".
[76] See Bygrave (n 10) at 61.
[77] See Simitis (n 56) at 129.
[78] Article 5(b) of the draft regulation and Article 4(b) of the draft directive.
[79] Article 5(c),(d) of the draft regulation and Article 4(c),(d) of the draft directive.
[80] Article 5(c) of the draft regulation, second thesis.
[81] Article 5(e) of the draft regulation and Article 4(e) of the draft directive.

possibilities and conditions for incompatible use[82]. Hence, the EDPS calls for additional precision in the proposed Regulation[83].

Another key issue is the interpretation of "specified", "explicit" and "legitimate" purpose, taking into account that the three conditions are cumulative. Interpreting these conditions *stricto sensu* is vital for the efficiency of the purpose requirements. For instance, a general purpose such as "public interest" must not be considered as fulfilling the "explicit" requirement. From this point of view, the position taken by the Commission in recital 44 of the draft proposal is subject to critique, as it specifically allows political parties to "compile data on people's political opinions" for "reasons of public interest", if the "operation of the democratic system requires so" in a Member State. It is difficult to find a valid argument which legitimizes a database of political partisans necessary for the operation of the democratic system.

A criterion for the "explicit" requirement could be that the purpose of the processing should allow the quantitative assessment in time of the data processing[84]. As for the meaning of "legitimate", previous literature underlined that this notion "denotes a criterion of social acceptability, such that personal data should only be processed for purposes that do not run counter to predominant social mores"[85].

4.3 Mechanisms of accountability

The draft regulation introduces expressly a principle of accountability in Article 5(f), stating that personal data must be "processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation". A similar provision is enshrined in the draft directive, in Article 4(f). However, even though such a principle was not expressly recognized in the DPD, certain provisions, such as the ones related to the judicial remedies and the control competences of the data protection authorities, indicated a certain degree of accountability of the controllers. Moreover, Article 6(2) DPD states that "it shall be for the controller to ensure that paragraph 1 is complied with", which can be seen as an approximate definition of accountability, as paragraph 1 contained all the principles relating to data quality.

It has been shown that, in broad terms, a principle of accountability would place upon data controllers the burden of implementing within their organizations specific

[82] EDPS Opinion (n 59), para. 116.
[83] Id., para. 117.
[84] For instance, personal data related to the students of a University are processed with the purpose of keeping track of their academic results; hence, the period of time needed for this processing equals to the period of the students' enrollment. If all or some of their personal data need to be processed for statistical purposes after this period, the legal safeguards for this situation must be observed.
[85] See Bygrave (n 10) at 61.

measures in order to ensure that data protection requirements are met[86]. At the same time, from the data subject's point of view, a principle of accountability would enable her to efficiently protect her right to data protection in front of or even against the competent authorities[87]. Hence, accountability translates into two types of mechanisms.

On the one hand, such mechanisms include anything from the introduction of a Data Protection Officer to implementing Data Protection Impact Assessments or employing a Privacy by Design system architecture[88]. On the other hand, they include rules regarding remedies, liability and sanctions. Articles 22, 23, and 24 of the DPD have been consistently developed both in the draft regulation and the draft directive[89].

The DPR proposal excels in expressly providing procedural rights for the data subject: the right to lodge a complaint with a supervisory authority (Article 73) – which is also extended to any body, organization or association which aims to protect data subjects' rights, the right to a judicial remedy against a supervisory authority – which is provided also for legal persons[90] (Article 74), the right to a judicial remedy against a controller or processor (Article 75), the right to compensation and liability (Article 77), and even common rules for court proceedings[91] (Article 76).

Also, the administrative sanctions provided for in the draft regulation are severe. Article 79 provides that each supervisory authority shall be empowered to impose administrative sanctions, which can amount up to one 1 million euro or, in case of an enterprise, up to 2% of its annual worldwide turnover. As a general rule, pursuant to Article 79(2), the administrative sanction shall be in each individual case "effective, proportionate and dissuasive", a formula which will need further clarification.

This particular safeguard needs attention taking into account at least the fact that the administrative sanctions as provided for in the draft regulation have four thresholds – from a warning in written to the 1 million euro fine, each threshold having its conditions, which amount in the case of the most serious one to 15 different hypotheses (Article 79(6) from (a) to (o)). Thus, accountability of the controller is taken very seriously in the future of data protection law in Europe.

5. Conclusion

[86] See de Hert and Papakonstantinou (n 23) at 134.
[87] Ibid.
[88] Ibid.
[89] See Articles 50 to 55 from the draft directive.
[90] This provision must refer to legal persons in their controller or representative of a controller capacity, as the DPR proposal makes it very clear that its provisions only apply to natural persons.
[91] Since the Treaty of Amsterdam, an explicit base for harmonization of civil procedural law is to be found in Article 65 of the EC Treaty (currently Article 81 TFEU); See Mariolina Eliantonio, "The Future of National Procedural Law in Europe: Harmonisation vs. Judge made Standards in the Field of Administrative Justice", *Electronic Journal of Comparative Law*, vol. 13.3 (2009).

This article explored a conclusion drawn from a "sketch" of the legal philosophy of data protection: every natural person should have the right not to be subject to processing of personal data, unless such processing has a lawful basis – which can be a legal provision, consent or other specific condition stipulated by data protection law, and unless the processing is subject to "suitable safeguards". Thus, it put consent rules into context and highlighted in section 2 that while they are an important part of data protection law, focusing on them is not productive for the achievement of the goal of the right to the protection of personal data, which has a highly procedural object. Instead, the focus should be on a set of rules that apply to all the types of data processing flowing from the six lawful bases recognized by data protection law and also to both spheres recognized in EU for the general data protection rules (the general framework and the *criminal matters* sphere).

Section 3 clarified what the object of the right to the protection of personal data is, in order to identify the suitable safeguards which match the achievement of its goal. It found that this right assumes the inherent nature of processing personal information in the modern society and that it is not its purpose *per se* to preclude such processing or to give an absolute right to the individual to object by means of his or her consent to the processing of personal data. In fact, its object is to provide mechanisms of protection or "suitable safeguards" for individuals with regard to the processing of their personal data: it "protects the protection of personal data". In fact, this paper aimed at correlating the object of the right to the protection of personal data to its content.

The last section identified three types of "suitable safeguards", the bundle of prerogatives that constitute what it was identified as the content of the right to the protection of personal data, that need equal attention from lawmakers and privacy professionals and that need to be further developed and clarified: the rights of the data subject, the purpose requirements and the accountability mechanisms. Each of them enjoys broad improvements in the EU's data protection reform package. However, section 4 showed that they are far from being clear and that they need further systematization and development.

After making a thorough analysis of consent in data protection law in her thesis, one of the conclusions Kosta reached was that "the role of consent in this era is reduced, as the control of the individual over his personal information is overcome by the facilitation of everyday activities in electronic communications and especially the internet, to the extent that the privacy of the individual is not infringed"[92]. If we accept that the role of consent in data protection is reduced, then the right to the protection of personal data needs, both in theory and in practice, to rely on other specific and well defined prerogatives of the data subject so that its purpose is achieved. The proposal of considering a systematization of these prerogatives under the concept of "suitable safeguards" is one possible solution of

[92] Eleni Kosta (n 37) at 318.

this problem, a solution which could also contribute to a functional redress system[93] for data protection in the European Union.

[93] The preliminary results of the EU Fundamental Rights Agency project on "Data protection: Redress Mechanisms and Their Use", presented at the Computers, Privacy and Data Protection Conference in Bruselles, January 23-25, 2013, show that „data protection cases are few and dispersed between a variety of different courts" in the Member States and that „in most jurisdictions data protection does not form an important area for the specialization and development of judicial expertise".