Default entitlements in personal data in the proposed Regulation: Informational self-determination off the table?

This paper will appear in December issue of Computer Law and Security Review,
Please consult the journal for a final version.

Nadezhda Purtova[i]

Abstract

This paper offers to assess the proposed General Data Protection Regulation through the framework of default entitlements in personal data. The notion of default entitlements comes from economic analysis of law and provides new insights into the implications of the data protection reform. While, under the principle of informational self-determination the default entitlements should lie with the individual, the Commission is shown to assign a great deal of default rights to others, including the Information Industry. This article cautions against the possibility of reducing the European system of data protection rooted in the values of individual autonomy and informational self-determination to a mere set of administrative rules channelling the flow of personal data, yet without a clear direction.

Keywords

Default entitlements,
data protection reform,
informational self-determination,
legitimate interest,
consent,
right to be forgotten,
purpose limitation,
Article 8 of the EU Fundamental Rights Charter

---

[i] Department of European and Economic Law, University of Groningen, The Netherlands; Tilburg Institute for Law, Technology, and Society (TILT), The Netherlands.

Default entitlements in personal data in the proposed Regulation: Informational self-determination off the table?

1. Introduction

Throughout the evolution of the data protection legislation and ultimately of the data protection rights, including the most recent stage – the 2012 Proposal for a General Data Protection Regulation,1 rapid changes in information technologies and practices have driven the policy-makers to make choices on what is right and wrong in personal data processing.2 One such choice is the definition of the data protection regime as a tool to ensure individual informational self-determination and individual's control over his data on the one hand, or as an instance of 'fair information practices', i.e. a set of procedural rules channelling, not restricting, personal data flow and accommodating the competing interests of others in collecting, using and otherwise processing these data on the other hand.3 A review of the reform efforts in the subsequent paragraphs suggests that despite the rhetoric of individual control that the European politicians adopted,4 the benefits of the Big Data for European economy seem to have too big of an appeal. This paper argues that the proposed Regulation may be an important turning point in the evolution of European data protection in that it effectively puts the possibility of having informational self-determination as a normative cornerstone of data protection off the table, or, at the minimum, reduces the meaning of informational self-determination to the point of no significance. The proposed Regulation signifies the choice in favour of the Information Industry's default entitlement to collect and further process personal data as a normative foundation and a rationale of data protection in Europe.

Some definitions are needed to make the focus of the argument and the connection between informational self-determination and default entitlements in personal data more explicit.

1.1. Informational self-determination, Fair Information Practices and default

The right balance between the claim to informational self-determination[5] and individual's control over his data on the one hand and the competing interests of others in collecting, using and otherwise processing these data on the other hand has been one of the most vital dilemmas in the policy area of data protection.[6] The debate can also be translated into 'who has the *default entitlement* in personal data': the individual or others, i.e. business and government. When informational self-determination vision of the data protection prevails, the individual by default is given control over disclosure and further processing of personal data: data processing is then conditional on the individual's consent, except when the law accommodates for the interests of others and allows processing on other grounds. When data collection and further processing are

the default rule, such a data protection regime is commonly referred to as Fair Information Practices, shielding the individual from negative effects of processing, channelling rather than restricting it.[7]

To combine the two approaches and the two interests has been a struggle for Europe ever since the negotiations leading to the adoption of the current Directive.[8] The Directive, although drafted under the influence of the German data protection rooted in the values of dignity and informational self-determination, does not use the language of informational self-determination or individual autonomy or indicate them as the values to be achieved. Instead, the Directive's provisions are described as 'largely procedural in focus'.[9] One should look back at its drafting history to understand that the Directive emerged against a backdrop of twenty years of the national data protection laws, each rooted in national legal and normative traditions.[10] The Directive has succeeded in somewhat evening the playing field of rules for data processing within the (then) EC.[11] However, attempts to explicitly anchor the common data protection rules in such strong normative choices as informational self-determination faced fierce resistance and consequently failed.[12] At the same time, the Directive's strong connection to the protection of privacy and other fundamental rights and interests of the individual - expressed *inter alia* in Article 1(1) and Recitals 2, 7, 9, 10 etc. of the Preamble and the ECJ's case-law[13] - allows interpretation and national implementation of the Directive as an instrument implementing the right to informational self-determination.[14]

1.2. Default entitlements

The term 'default entitlements' is a hybrid of two concepts: a legal entitlement understood as 'the fact of having a right to something',[15] and default allocation or assignment of resources, predominantly used in the law and economics literature. While the relevance of speaking about entitlements in the context of data protection as a fundamental right is evident, the significance of the law and economics lingo needs some explanation.

The economists of law often speak of allocation of resources, i.e. distribution of assets used to meet human needs[16] among the market actors, in the context of the efficiency analysis of legal entitlements.[17] The relevance of this analysis for the data protection field is two-fold. First, the exponential commodification of personal data[18] as well as the rhetoric adopted by the European officials,[19] leave little doubt that personal data is a resource of high market value, and European officials want this value to be 'unpacked' to boost the declining economy and to stimulate innovation.[20] Second, the resource allocation analysis is relevant for the European data protection field because the European efforts towards a data protection reform are an appropriate occasion to revisit the matter of efficiency of rights assigned in and regarding personal data.

How entitlements in personal data are being allocated initially, i.e. the default entitlements before the parties negotiate reallocation, is of special importance. In conventional law and economics, under Coase theorem, how resources are initially allocated does not matter, so long as transaction costs, such as costs of negotiations, organising collective effort, etc. are zero. The market participants are thought to be able to always negotiate the most efficient result.[21] Conventional economic analysis of law presumes that resources, such as personal data, 'tend to gravitate toward their most valuable uses.'[22] As a logical extension of this argument, an argument is often made that it should not matter whether the individual has a legal right to decide whether or not to disclose his/her personal data. The Information Industry should be by default allowed to collect all personal data it can access. According to the conventional economic theory, as long as the transaction costs are addressed, those individuals who appreciate their privacy more, will always be able to buy it, e.g. by choosing a privacy-respectful service as a luxury product in the range of similar services.[23]

However, a substantial body of empirical evidence questions the accuracy of this Coasian prediction. Findings in behavioural economics and anthropology of law suggest that the initial assignment of a legal entitlement may affect the outcome of bargaining.[24] Namely, the resource assigned to a market participant by default, even though transaction costs are zero, tends not to change hands and stick with the initial 'owner.'[25] This phenomenon, known as the endowment effect, brings an end to the illusion of the possibility to 'buy more privacy' when personal data of an individual is not by default his/hers to keep secret.

Interestingly, recent empirical studies on perceptions of privacy[26] imply that privacy policies containing 'privacy promises' without the back-up of the individual control rights as a default legal rule do not necessarily create safe havens of privacy and data protection, even when lived by perfectly. To the contrary, privacy assurances in such circumstances serve more as an element of a marketing strategy, and a cue to 'clam up' and feel more at ease revealing personal data to a company in question. Brandimarte et al show that 'people who experience more perceived control over limited aspects of privacy sometimes respond by revealing more information, to the point where they end up more vulnerable as a result of measures ostensibly meant to protect them,'[27] the phenomenon labelled as 'the control paradox'.

1.3. Importance of default entitlements analysis

Thus, the default entitlements in personal data are not simply of relevance but also of major importance for the current European and international data protection discourse. In addition to the points from the behavioural economics analysis highlighted earlier, understanding of the default rules of data protection, and initial allocation of rights in personal data among them, determine the scope of the privacy- and data protection interests of the individual that, possible

limitations aside, in general deserve safeguarding, and therefore pertain to the very essence of the still young right to data protection.[28] This choice is vital as it delineates a terrain where the individual is entitled by default to deny access to his personal data, and others have no claim in it, unless law imposes a respective limitation on the entitlement of the individual. Equally, outside of the scope of the safeguarded privacy and data protection rights others have a default entitlement to do what they please and the individual has no claim.

Finally, understanding the nature of the protected interests is important to determine the legitimate grounds and permissible degree of limitations on the individual's entitlement necessary to accommodate competing interests of others.[29] As assessment of permissibility of such limitations usually is done through some form of balancing,[30] it is crucial to have conceptual and normative clarity as to the interests on both sides of the scales.

1.4. Roadmap of the analysis

The analysis will proceed as follows. First, I will examine if and how the elements of informational self-determination – both on the level of values to be protected and in the form of control rights – are present in the proposed Regulation. The control rights will be considered with a special emphasis on whether or not they occur by default or upon fulfilment of certain conditions. I will then move to examine what rights regarding personal data others appear to be given, either by default or conditionally. This analysis will demonstrate that – were the proposed Regulation adopted in its current state – the scope of default control rights of an individual over his/her personal data would be significantly narrower compared to the situation under the current data protection Directive. Simultaneously, the rights of others in personal data would significantly increase in scope and often be the default rule of data protection, thus effectively removing informational self-determination from the foundations of data protection in the European Union.

2. Elements of informational self-determination in the Proposal

The European data protection regime currently in force is connected to the idea of informational self-determination both on the level of objectives and specific control rights of the data subject.

2.1. Objectives of data protection

In contrast with the data protection Directive currently in force, the Proposal is not connected to the informational self-determination on the level of its objectives. The author has demonstrated elsewhere the significance of Article 8 ECHR privacy jurisprudence for the development of a relatively young and still evolving right to data protection.[31] For the purposes of this article it suffices to restate that the ECHR privacy case-law and legal doctrine have provided a solid basis to root the right to data protection in the values of individual autonomy, development of personality and informational self-determination.[32] To break the link between privacy and data protection in this sense would amount to breaking the normative connection between data protection and informational self-determination.

Unlike the Directive, the proposed Regulation is not anchored in the protection of privacy anymore. While Article 1 of the Directive states that the Member States must "protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data," the objective of the Regulation is to "protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data" (Article 1(2)). Poullet and Costa notice that the word 'privacy' itself is gone from the text of the Regulation, substituted for 'data protection' even in such long-standing terms as 'privacy by design' and 'privacy impact assessment'.[33] Such conceptual separation between privacy and data protection, they argue, threatens protection of liberties since it 'cuts the Data Protection regulation from the innovative and quite protective Strasbourg Court's jurisprudence which repeats that privacy might be considered as the way to achieve the right to self-determination, to dignity and, to that extent, represents and essential condition for all liberties.'[34] The link between EU data protection and privacy has been more that a mere declaration. It has had a tangible effect on the practical outcomes of application of the data protection law. The Court of Justice in Luxemburg has been repeatedly invoking the Directive's objective to ensure privacy - or protection of private life – in its analysis as a benchmark against which data processing has to be evaluated.[35] In *Österreichischer Rundfunk* the Court explicitly stated that the provisions of the Directive have to be interpreted in light of fundamental rights,[36] and in particular, the right to respect for private life in Article 8 ECHR.[37] The Court went on to conclude that if the measure at hand did not comply with Article 8(2) ECHR as to the requirement of proportionality, it was also not in compliance with the Directive.[38] The entry into force of the Lisbon Treaty[39] in 2009 that gave EU its own 'constitutional' right to data protection in Article 8 of the Charter of Fundamental Rights of the European Union[40] did not weaken the link between data protection and privacy in the jurisprudence of the Court of Justice. In *Scheke* case that was ruled on after Lisbon, the Court, although found a reference to Article 8 ECHR unnecessary to assess the interference with the fundamental right to protection of personal data, explained that the right to respect for private life with regard to the processing of personal data is recognised both by Articles 7 (private life) and 8 (data protection) of the Charter, which offer the same meaning and scope of the protection as laid down by the Convention.[41]

Removal of any reference to privacy in the proposed Regulation in favour of the objective 'to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data' (Article 1(2)) may change practical outcomes of the application of the data protection law. To demonstrate, let us consider how the changed objectives of data protection might influence the outcome of balancing interests of data subjects and others in connection to personal data. As follows from the brief overview of the Court of Justice data protection case-law, the objectives of data protection are invoked, among others, for balancing competing interests in personal data, e.g. in the context of proportionality analysis.[42] One instance

of such proportionality analysis is under Article 6(1)(f) of the proposed Regulation which provides that processing of personal data is lawful when

> processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

This provision is a functional equivalent of Article 7(f) of the Directive that currently allows data processing 'for the purposes of the legitimate interests pursued by the controller […], except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1)' (read, 'fundamental rights and freedoms of natural persons and in particular their *right to privacy* with respect to the processing of personal data'). The way in which both provisions have been formulated clearly requires interpretation, namely, the balancing of any legitimate interests, such as conducting a business, with an individual's fundamental rights and freedoms. In case of the Directive those are named in Article 1(1), i.e. privacy and, consequently, informational self-determination and control.[43] The proposed Regulation, instead, calls for balancing of the controller's interests against '*rights and freedoms of the data subject which require protection of personal data'*. Keeping in mind that the Regulation uncouples the objectives of data protection from protection of privacy, the rights and freedoms which require data protection are effectively limited to the right to data protection under Article 8 the EU Fundamental Rights Charter.

However, the right to data protection as provided for in Article 8 of the Charter lacks clarity as to its content and own normative weight needed in order to function as a benchmark against which the legitimate interests of the controller are to be assessed, as well as to be used for any form of balancing or proportionality analysis. If privacy and related autonomy and informational self-determination are not the rationale of the right to data protection – the conclusion that follows from removal of privacy protection from the Regulation's objectives – then what is? Article 8 explains the content of the protected right in a way that leaves a major gap concerning what constitutes the legitimate basis of processing. After stating that 'everyone has the right to the protection of personal data concerning him or her,' it further explains 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. Compliance with these rules shall be subject to control by an independent authority.' Thus, apart from the expressly named rights of access and the right to have data rectified, in determining further exact scope of the right to data protection, Article 8 refers to law that is to further specify what constitutes legitimate data processing. Currently, the data protection Directive is one such law, to be substituted by the proposed Regulation once it is adopted, or any other document that

will come as a result of the reform efforts, and Article 6(1)(f) legitimate interest of a controller is one instance of a legitimate ground of data processing provided for by law.

However, the trouble is that the analysis under Article 6(1)(f) of the proposed Regulation coupled with Article 8 of the Charter is caught up in the logical fallacy of circular reasoning and therefore is flawed. The chain of reasoning involves many individual components, some of which are valid, but nevertheless do not allow to arrive at a logically valid conclusion, as the starting premise is also the end proposition:[44] Submission A ('Data processing under Article 6(1)(f) is lawful') is true when Submission B is true (data processing is 'necessary for the legitimate interests of a controller') and Submission C is true ('the legitimate interest overrides the interests or fundamental rights and freedoms of the data subject'). Submission C is conditioned on the validity of Submission D ('the interests of the data subject require protection of personal data'), whereas what is included in the right to protection of personal data under Article 8 of the Charter is – at least in part – to be determined by law, i.e. among others, by the proposed Regulation (this is Submission E, referring back to Submission A). In short, Article 6 (1)(f) of the proposed Regulation allows data processing for the purposes of pursuing legitimate interests of controllers when the right to data protection under Article 8 of the Charter is respected, and the right to data protection under the Charter is respected, among others, when the proposed Regulation allows data processing. The logical circle is complete.

One may object that the problem of circular reasoning is dealt with in Article 6(5) of the proposed Regulation providing that the Commission via a system of delegated acts will further specify the conditions under which legitimate interests of the controller override the interests of the individual in protection of his/her personal data.[45] I tend to disagree. Whereas the immediate need of the actors involved in data processing to refer to Article 8 of the Charter for guidance on what would necessitate protection of personal data and therefore determine the balance between the controller's and individual's interests will be eliminated, the circular reasoning will remain (possibly, including slightly bigger number of propositions) with the Commission and not data processing actors having to go through the same algorithm of reasoning while developing its context-specific guidelines, starting with Submission A and eventually ending on Submission E, referring back to A. In addition, it is unclear whether Article 6(5) self-delegated Commission power to balance the conflicting interests in personal data will survive the reform process. The scale of the Commission's ambition to participate in lawmaking in the field of data protection in general has been subject to criticism, and is even more suspect in the context of Article 6(1)(f) that has a direct influence on the scope of the right to data protection as one of the European fundamental rights. As Hofmann rightly observes, 'delegated acts are meant to "supplement or amend certain non-essential aspects" of a legislative matter'. [46] Determining the scope of protection is surely not non-essential.

The odd correlation between Article 6(1)(f) of the proposed Regulation and Article 8(2) of the Charter is only one of examples of the identity crisis in which the EU right to data protection finds itself, partially as a result of disconnecting data protection from privacy and, by proxy, informational self-determination.

2.2. Control rights

Next to the departure from the informational self-determination on the level of values, the Regulation also narrows down the scope of the control rights of the data subject compared to the situation under the Directive. The area of default entitlement of the individual in personal data created by the proposed Regulation is becoming narrower in comparison to the system of the Directive, while the scope of the default entitlements of others is growing broader. This part will focus on the individual's control rights and default entitlements.

The principle of individual control – a common denominator in the bulk of the data protection laws in Europe,[47] the purpose of which is to enable an individual to have a degree of freedom to choose how to deal with his or her personal data.

Lee Bygrave explains the control principle as follows:

> A core principle of data protection law 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.[48]

Although the importance of the principle is a matter of a wide consensus,[49] data protection laws rarely contain it in a single provision or refer to it as 'the principle of control.' Instead, it is manifested through abstract value concepts and 'a combination of several categories of rules'.[50] The OECD Guidelines, for example, contain the 'Individual Participation Principle' (paragraph 13),[51] although, as Bygrave points out, 'rules giving effect to it embrace more than what is articulated in that particular paragraph'.[52] German data protection laws likewise revolve around a wider principle of informational self-determination, which was developed in German constitutional jurisprudence,[53] 'meaning the capacity of the individual to determine in principle the disclosure and use of his/her personal data'.[54]

The 1995 Directive sets out a more comprehensive system relating to the rules of individual control. Bygrave offers a classification of the control-enabling rules.[55] There is first a requirement for a general transparency of data processing, which includes a controller's obligation to publicise his data processing activities by giving notification to a supervisory authority of the fact and basic details thereof (Article 18). This notification obligation is also combined with a requirement to make this information available in a public register (Article 21(2)).

The second group of relevant rules is aimed at making people aware of the processing of data pertaining to them. To achieve this, the 1995 Directive prohibits, where other legitimate grounds are absent, the processing of personal data without the consent of data subjects (Articles

7, 8 (2)(a)). It also obliges data controllers to inform data subjects directly about the fact and basic details of the processing of information relating to them (Arts 10-11), whether or not these data subjects utilised a right of access thereto.[56] The right of access is enshrined in Article 12 of the 1995 Directive and enables a data subject to not only have access to data relating directly to him, but also:

> to information about the way in which the data are used, including the purposes of the processing, the recipients and sources of the data, and the 'logic involved in any automated processing of data concerning [the data subject] … at least in the case of the automated decisions referred to in Article 15(1)'.[57]

The third group of rules gives an individual a right to object to the processing of his personal data and demand that it be corrected or deleted if it is invalid, irrelevant, unlawfully retained, etc.[58] Since consent must be freely given, it can also be revoked at any time.[59] The right to object is a product of the ban on data processing without consent.[60] The Directive also specifies individual instances thereof, such as the Article 14(a) right to object to direct marketing and the Article 15(1) right to object to decisions 'based solely on automated processing of data intended to evaluate certain personal aspects related to him [the data subject]'. In addition, there is a right to demand that incomplete or inaccurate data, or data that is not processed in compliance with the Directive's requirements, be rectified, blocked or deleted (Article 12(b)).

The preparatory documents accompanying the Proposal, as well as earlier statements of the Commission officials, identify strengthening individual control over his personal data as a cornerstone of the data protection reform.[61] The Commission promises to 'improve individuals' ability to control their data', among others by introducing new data protection rights: a right to be forgotten in the online environment; and a right to data portability: 'a right to obtain a copy of the stored data from the controller and the freedom to move it from one service provider to another, without hindrance'.[62] However, although the rhetoric of control dominates the discourse around the reform, the scope of some control rights in the Proposal has become narrower than in the Directive to the extent that supports the sense that the Proposal has moved away from the idea of informational self-determination in favour of the interests of others in processing personal data as long as the rules channelling this processing – fair information practices – are respected.

a. Consent

Consent rule is the most outstanding instance of such reassignment of the default entitlements in personal data. Consent requirement is meant to enable an individual to determine whether or not and under what conditions his/her data are disclosed. Therefore, consent lies at the core of the right to informational self-determination and ensures the default entitlement in

personal data on the side of the individual. Although some argue that the requirement of consent is central to the Directive's data protection system,[63] it seems to be losing its significance in the proposed Regulation.

The consent rule as a ground for legitimate data processing has often been criticised for its unreliability due to weaker position of the data subject and the difficulty of managing consent-based data processing. When it comes to the issue of unreliability, the data protection authorities advise against data processing based solely on the grounds of consent in the field of electronic commerce, employment relationships,[64] and data transfers outside the European Union. In addition, many data protection authorities do not recognise consent given by a minor or a child.[65] The reasoning behind such a position is the associated risk of forced or ill-informed consent being obtained in such circumstances and the difficulties caused by the withdrawal thereof.[66] In the context of e-commerce there is an increased risk that a data subject did not fully understand, or did not read, the standard terms and conditions, which can be too long and unclear. In some jurisdictions the application of the consent rule in e-commerce is even more limited by the requirement for written consent, i.e. on paper.[67] Many data protection authorities also rightly see employment relationships as being inherently dependent, meaning that employees cannot meaningfully consent to data processing.[68] Finally, consent under Article 26(1)(a) (transfer to a non-EU country without an adequate level of protection) can rarely be unambiguous and fully informed since, *inter alia*, due to the language barrier and a poor knowledge of data practices and enforcement mechanisms in the jurisdiction in question, the data subject can hardly be expected to possess the know-how to calculate either the potential risks related to the transfer of his data outside the European Union or, often, the irreversibility of a decision to give such consent.[69] Accordingly, the data protection authorities advise against reliance on consent as the sole legal basis for data processing, except where 'it is absolutely necessary'.[70]

In response to the criticism, the proposed Regulation strengthened the individual consent requirement: (a) its definition has been enhanced by an extra requirement that it should be 'explicit' (Article 4(8) of the Proposal); and (b) Article 7 of the Proposal is solely devoted to the conditions of consent.[71] The personal data of a child under the age of 13 is to be processed with the consent of the parents or other legal representatives only (Article 8 of the Proposal). The controller has a burden of proof of the existence and validity of consent (Article 7 and Recital 32).

Interestingly, while the requirements for a valid consent have been strengthened, the consent rule has lost its significance as a ground for lawful data processing under the proposed Regulation since it cannot 'provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller' (Article 7(4)). From the perspective of the informational self-determination as a normative foundation of the European data protection it seems, however, that, metaphorically speaking, the surgeon has amputated the

leg that could have been saved. In other words, the weaknesses of consent can be addressed by alternative means. To name only few, some consumer protection organisations on the stage of consultations emphasized 'a need to raise awareness amongst consumers, and particularly children, about the consent and its implications in terms of their personal data.'[72] An idea of assisted consent and data brokers – professional organizations managing data on behalf of the data subjects – can be examined to deal with the issue of consent given not feely or in context of imbalance of powers between the controller and data subject.[73] Ironically, almost any instance of data processing in the context of the Big Data occurres in the circumstances of power imbalance. Such data processing is executed by corporations that have advantage in expertise and resources.

By making strengthened formal requirements to consent a focus of the reform efforts while making no attempts to create circumstances in which consent could be given *meaningfully*, the Proposal discourages reliance on consent to justify data processing. At the same time, as the analysis in part 3 will show, at least in private sector processing, the use of broadly defined alternative grounds of processing, such as legitimate interests of the controller under Article 6(1)(f), is made easier, both on the stage of data collection and maintaining control over personal data further on.

b. Purpose limitation

Purpose limitation strictly speaking is not a control right but a principle. However, the exercise of control rights is so closely linked to this principle that any analysis of individual control and informational self-determination is not complete without a discussion of purpose limitation. The principle of purpose limitation (Article 6(1)(b) of the Directive) is another instance of the data protection guarantee that, once the Regulation is adopted without relevant changes, will shift from the informational self-determination rationale, i.e. no (further) processing by default, unless an individual agrees or law requires, to the default entitlement to process data. The purpose limitation principle – one of the general principles of data protection - is rooted in the values of informational self-determination and individual control. Article 29 Working Party considers purpose limitation as an unavoidable prerequisite of individual control, as the latter can be meaningfully exercised through consent or the right to object only if the data subject 'fully understands the purposes of processing.'[74] The principle reinforces the default entitlement of the data subject by requiring that the purpose of processing must be specified before or in any case not later than the instance of collection.[75]

The purpose specification should be understood as a limit on how the data controllers can use personal data.[76] Under Article 6(1)(b) of the Directive, personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. The underlying idea is not to let one-time legitimization of a single instance of data processing under Article 7 to become an open floodgate for further unlimited uses of these

data, such as data sharing and open data initiatives regarding public sector data,[77] keeping collected data longer than authorised in case some need for it presents itself later, etc.

The purpose limitation principle has two elements: purpose specification and compatible use.[78] Pursuant to the principle of *purpose specification*, the personal data should be only collected 'specified, explicit and legitimate purposes.' These purposes are 'raison d'être of the processing operations.'[79] If personal data is processed further, the new purpose must be specified.[80]

The *compatibility* principle prohibits further processing 'incompatible' with the original purposes of collection. Member States assess the compatibility of further use differently: some approach compatibility strictly, involving formal comparison of the initially given (often in writing) purpose of collection with the purposes of use. Others allow a degree of flexibility and apply a more accommodating approach. It involves a comparison of the two purposes; the context in which the data have been collected and the reasonable expectations of the data subject as to the further use; the nature of the data and the impact the further processing would have on the data subject; as well as the measures taken by the controller to ensure fair processing and protection of the individual from any undue impact.[81] Thus, although the assessment has to take place on a case-by-case basis, in principle the initial purpose of processing can change, as long as the purpose of collection explicitly or implicitly includes the new purpose,[82] or even when the purpose changes significantly, but appropriate safeguards are provided.[83] The flexible approach to the compatibility requirement can be criticised as an instance of a slippery slope reasoning, undermining the data subject's ability to effectively control the use of his/her personal data and, possibly, too accommodating of the interests of others, e.g. in part referring to the data subject's expectations regarding further use.[84] However, overall the compatibility requirement does endow the data subject with a degree of control and exclude the possibility for the controllers to process personal data by default and at will. Under the proposed Regulation, the situation is radically different.

In its opinion on the purpose limitation principle Article 29 Working Party reinforced the understanding of the current data protection regime as rejecting the default entitlement of the data controller to process. Namely, the Working Party repeatedly emphasized that the requirement of purpose limitation under Article 6(1)(b) and an appropriate legal basis under Article 7 of the Directive are *cumulative requirements*,[85] meaning that mere presence of a legal basis cannot legitimize incompatible use, and even if the further processing is compatible, it has to be based on one of the legal grounds of processing anyway.[86] The proposed Regulation allows the use of legitimate basis of processing to compensate for the lack of compatibility and thereby severely reduces the significance of the compatibility requirement.[87] Although Article 5(b) of the proposed Regulation repeats the Directive's principle of purpose limitation by requiring that data must be 'collected for specified, explicit and legitimate purposes and not further processed in a way

incompatible with those purposes', the fundamental difference between the Directive and the Regulation lies in the consequences of further processing for incompatible aims. While incompatible use under the Directive is unlawful and therefore prohibited, Article 6(4) of the Regulation allows to further process, provided the controller identifies a new legal ground for the processing, except for the 'legitimate interest' of the controller under Article 6(1)(f).[88] Article 29 Working Party interprets this change to mean that 'it would always be possible to remedy the lack of compatibility by simply identifying a new legal ground for the processing,'[89] e.g. by changing provisions of a contract with the data subject, and proposes to delete the respective paragraph.[90]

Article 6(4) exception does not merely 'remove the substance' of the purpose limitation principle,[91] but simultaneously makes the remaining guarantees of individual control such as the consent requirement, right to object and request erasure, pointless, as their exercise is conditioned upon a purpose of processing. This element of the reform may not immediately introduce default entitlement of the controller to process personal data, but is dangerously approaching this point at a speed directly proportionate to the ease of invoking alternative grounds of processing, such as performance of a contract – in private sector, or exercise of official authority – in public sector.

c. Right to be forgotten and erasure, data portability and right to object

The right to be forgotten and data portability are both examples of how the fading significance of the consent requirement reduces the default entitlements of the individual in his/her personal data. In the new data protection framework the two rights mutually interact and, together with the right to object, form a mechanism of enforcement of the individual control and informational self-determination.

Both right to be forgotten and data portability have been connected to and considered as a logical extension of the notion of informational self-determination and the individual's default entitlement to control disclosure and further processing of his/her personal data. In her speech of 30 January 2012 Nelie Kroes, Vice-President of the European Commission responsible for the Digital Agenda, identified individual ownership of personal data as a cornerstone of the proposed general data protection regulation (hereinafter Regulation).[92] Ownership of personal data is a proprietary right in personal data of the widest scope[93] and, according to Kroes, implies that "[personal data] can only be used with good reasons. You can correct it, get a copy in a commonly-used, interoperable format to go on using it elsewhere, or to have it deleted."[94] Some scholars understand the right to be forgotten as strongly associated with the individual's sovereignty over his/her data. Steven Bennet points out that that the introduction of the right to be forgotten in Europe may in fact lead to creation of the property right in personal data.[95]

Next to the purpose limitation discussed earlier, the enjoyment of both rights is ultimately determined by the legal ground used to justify initial processing of personal data that the data subject wants erased or moved. While the data subject has an unconditional right to obtain erasure

of personal data processed on the ground of consent (Article 17(1)(b)), when a contract or a legitimate interest of the controller provide grounds for lawful processing, a data subject can only *object* to the processing (Article 19(1) of the Proposal), which is a weaker right.

The objection should be justified 'on grounds relating to their particular situation […] unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject' (Article 19(1) of the Proposal). The objection has to be upheld (Article 19(3)). This effectively takes the default entitlement in personal data away from the data subject and gives it to the controller. More specifically, (A) when exercising his/her right to object, the individual has the burden to *justify* his/her objection by personal circumstances, which shifts the balance of entitlements in favor of the processing party. Interestingly, one of the previous drafts of the Regulation that leaked earlier did not require justification (Article 17 of the earlier draft). (B) In order to process data the controller has to have a legitimate interest that overrides the interests of the data subject. In light of the earlier analysis of the balancing of these two interests and lack of normative foundation of the data protection right in the new data protection framework, a conclusion follows that under the new Regulation, in case the data subject objects, it would be sufficient for the controller to simply restate the same interest in order to override the objection and continue processing. When the data subject wants to make use of the right to be forgotten and / or object to data processing in connection to Article 18 right to data portability (e.g. have his records erased after he/she obtains a copy or transfers the records to another platform), same mechanisms are in play.

In addition to the difficulties of erasure, the proposed Regulation introduces other discrepancies in the scope of the right to data portability, conditioned on whether or not the data involved are processed on the basis of consent or contract or other grounds. Article 18(1) provides for a general right to data portability applicable to all instances 'where personal data are processed by electronic means and in a structured and commonly used format'. Regardless of the legal basis of processing, the data subject can obtain a copy of processed data 'in an electronic and structured format which is commonly used and allows for further use by the data subject.' Article 18(2) goes on to specify the (significantly wider) scope of data portability in cases when 'the data subject has provided the personal data and the processing is based on consent or on a contract': only when relevant processing is based on consent or contract and the data is provided by the data subject, the data subject is given the right to 'transmit those personal data … retained by an automated processing system, into another one, … without hindrance from the controller from whom the personal data are withdrawn.' Read together, the two paragraphs reveal how limited the scope of control that the right offers is, especially when processing is not based on consent or contract: (A) the general right to data portability does not enable the data subject to 'take his/her data and leave'. It does not do more than provision of a copy for the data subject's own use. Whether or not the copy can be used on a competing platform is left on the provider's

discretion to invoke proprietary rights. Whether or not the data subject can meaningfully 'leave', i.e. have his record erased after obtaining a copy, is a matter of and subject to the challenges of the right to be forgotten and erasure. (B) The only case when the data subject can go on and use the obtained copy on a competing platform without being hindered by the original provider, e.g. by invoking proprietary rights in the record, is when the data have been 'provided by the data subject,' and is processed on the basis of consent or contract. One can legitimately assume that the situations when both requirements are met are going to be rare. First, it has already been established that the use of consent to justify processing is likely to be minimal once the relevant provisions of the Regulation are in force. Second, it is not clear what 'provided by the data subject' should mean. In case it should be interpreted as 'actively given by the data subject', Article 18(2) guarantee will have no relevance for the environment of ubiquitous computing when data are being harvested constantly, often without the data subject knowing, not to mention, actively participating. As a result, the impact of the data portability right both in terms of facilitating competition and system interoperability,[96] and as a tool to achieve informational self-determination, is limited, especially when the data processing is not based on consent or contract. Even more so, from analysis of among others, Article 18(2) of the proposed Regulation it follows that, when drafting the provisions on data portability, the Commission departed from safeguarding the proprietary interests in personal data *the controller* might have, rather than from the presumption of 'everybody owning their own personal data'.[97]

To summarize, the control rights provided for in the proposed Regulation are significantly weaker when the relevant data processing relies on a legal basis other than consent, which most likely will be majority of the cases. This is consistent with a 'shared view' expressed by the industry during consultations that 'too much emphasis on consent will undermine privacy as individuals will become used to always agreeing to a stated purpose without necessarily understanding what is being asked of them'.[98]

3. Accommodating interests of others: Limits on control rights

The analysis so far has shown that the scope of control rights under the proposed Regulation is dangerously reduced to the point that the informational self-determination as a rationale of the proposed data protection regime is severely limited and threatens to become irrelevant. This Part will show another aspect the shift from informational self-determination to default entitlements of the information industry and other actors to process data, namely, the extended degree of accommodation of the interests of others in personal data. The scope of accommodation under the proposed Regulation is notably broader that under the current Directive and suggests that the data processing is a default rule, when individual control and self-

determination would become a privilege. It is apparent from the heavier limitations on control rights.

This paper by no means asserts that an individual should or does under any circumstances have unlimited control over his personal data. Such an absolute control would not be consistent even with far reaching German constitutional jurisprudence on informational self-determination.[99] The right to respect for private life under Article 8 ECHR is not unlimited either. Article 8 (2) ECHR provides that the right to protection of private life (protecting informational self-determination) can be limited, provided the limitation is imposed by law and is necessary in a democratic society for a restricted number of legitimate purposes, such as 'in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.' However, the limitations imposed must be an exception rather than a rule. The further analysis demonstrates that under the proposed Regulation the exercise of informational self-determination will become an exception to the default entitlement to process data.

Even under the regime of informational self-determination as a default rule, the consent rule is not the only condition to legitimize data processing. Since the current rules provide for a number of alternative conditions, such as authorisation by law,[100] the approach defended in this study regards consent as a default rule, unless prescribed otherwise by law or contract.[101] Both 1995 Directive and the proposed Regulation account for the legitimate interests of others in personal data and accommodate interests of others by limiting default entitlement of the individual in his/her personal data. A major difference between the two documents, however, lies in the scale of these limitations. The degree to which the Regulation accommodates the interests of others is so significant that the Regulation's rules of data processing effectively shift the balance away from the informational self-determination and default individual's entitlement in favour of competing (business) interests and *the default entitlement of others to process*. In doing so, the Regulation threatens to distort the 'human rights' understanding of the function of the data protection right as an instrument to secure informational self-determination and autonomy as opposed to a mere set of modalities of data processing. To prove the point, let us compare the limitations of control rights under the Directive and the proposed Regulation.

Roughly the data protection regime under the 1995 Directive contains limitations of the individual control over his personal data in the form of:

- Article 7 and 8 (2) grounds of legitimate data processing alternative to the data subject's consent;[102]
- Exemption from the data subject's information rights under Article 11 (2) where the data have not been obtained from the data subject "in particular for processing for statistical purposes or for the purposes of historical or scientific research, the

provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law";
- Exemption from the obligation of the controller under Article 12 (c) to notify third parties to whom the data have been disclosed of rectification, erasure or blocking of data if "this proves impossible or involves a disproportionate effort";
- Exemptions under Article 9 for the processing of personal data for journalistic purposes or the purpose of artistic or literary expression, necessary to reconcile the right to privacy with freedom of expression; and finally,
- In the form of Article 13 exemptions and restrictions – to be established by the laws of Member States - regarding Articles 6 (1) general principles of data processing, information rights of the data subject under Articles 10 and 11 (1), right of access, rectification, erasure or blocking under Article 12 and Article 21 obligation to publicize data processing operations.

The proposed Regulation has kept all of the limitations under the Directive, introducing some improvements but also slightly shifting the balance between the individual's interests and the interests of others in favour of the latter.

- Article 6(1) and 9 provide for grounds of legitimate data processing alternative to the data subject's consent, largely overlapping with those in the Directive.[103]
- Article 14(5)(b) parallels the Directive's Article 11(2) exemption from the information obligations when the data have not been obtained from the data subject 'if the provision of such information proves impossible or would involve disproportionate effort';
- Article 13 of the Regulation copies the Directive's Article 12(c) exemption from the obligation of the controller to notify third parties of rectification, erasure or blocking of data if "this proves impossible or involves a disproportionate effort";
- Article 80 of the Regulation, similarly to the Directive's exemptions under Article 9, reconciles data protection rights and the processing of personal data for journalistic purposes or the purpose of artistic or literary expression; and finally,
- Similarly to the Directive's Article 13, under Article 21 of the Regulation the Union or Member States may derogate from the general principles of data protection (Article 5, points (a) to (e)), and other information and control rights of the data subject (Articles 11 to 20), and a newly added data breach communication (Article 32) when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard legitimate goals named in the Article, consistent with Article 52(2) of the EU Fundamental Rights Charter and Article 8(2) ECHR.

What makes those limitations very different from the limitations under the Directive is the fact that the Regulation does not rely on privacy and informational self-determination as normative anchors anymore. The application of every limitation named above depends on 'necessity' and some form of balancing of the data subjects' and others' interests against each other. The principle of fair processing implies the prerequisite of proportionality in that, while processing data, the controller is expected to balance his interests and those of the data subject in order to avoid invading them unnecessarily, unreasonably, or excessively.[104] As it has been explained in section 2.1 above, such a balancing exercise invoking not privacy and informational

self-determination, but still unclear and in any case narrower and more technical data protection rights on the side of a data subject against competing claims may produce quite different outcomes, most likely, in favour of the interests of others that those 'others' deem legitimate and of greater importance weight.

To illustrate, in the case of consent and the other preconditions to data processing, whether the consent rule has or does not have a normative priority should not, theoretically, have an impact on the scope of the data processing that is permitted. However, when priorities are not unequivocally set out in favour of privacy, informational self-determination and consent, it enables the interpretation of other, often vague and inclusive, preconditions to the processing of data, as if they have a priority over informational self-determination. For instance, Article 7(f) of the Directive currently allows data processing 'for the purposes of the legitimate interests pursued by the controller […], except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1)'. The way in which this provision has been formulated clearly requires interpretation, namely, the balancing of any legitimate interests, such as conducting a business, with an individual's fundamental rights and freedoms named in Article 1(1), i.e. privacy and, consequently, informational self-determination and control. As Kuner explains, the various Member States conduct this balancing act differently and 'data controllers must examine local law in detail to determine if the exception applies'.[105]

A corresponding Article 6(1)(f) of the Proposal balances those legitimate interests of the controller against "the interests or fundamental rights and freedoms of the data subject '*which require protection of personal data*' [Italic – N.P.]. To briefly restate the argument made in section 2.1, fundamental rights and freedoms that require protection of personal data – contains no normative reference. This criticism is twofold. *First*, the use of 'protection of personal data' as an element guiding the decision-making on whether or not to process data questionable. Indeed, it is not clear what is meant by 'protection of personal data'. If interpreted in light of the other provisions of the proposed Regulation analysed above, the Commission understand data protection as the rules of the game, rather than a deterrent for playing the game - for disclosure and further processing of data. Therefore it cannot be used to guide the decision-making on whether or not to process. *Second*, the 'legitimate interest of the controller' is a standard that is (a) easier to meet than the one adopted by the Directive, since the data protection rights are narrower in scope than privacy and informational self-determination, and (b) vague enough to allow the outcome prejudiced in favour of the business interest, since the content of the data protection rights has not completely formed yet. The 'legitimate interest' ground of processing is even more permitting given that this is the controller who – in the first instance – exercises the balancing. The review of the outcome of balancing by courts and data protection authorities, happens only post factum. One may object that the Commission is to adopt a number of delegated acts to

clarify use of the 'legitimate interest' ground for data processing, and that this will be the Commission who will exercise the balancing under Article 6(1)(f). However, first, this does not eliminate the fact that, as pointed out in section 2.1, the EU right to data protection does not provided necessary guidelines to execute the balancing; and, second, it is unclear whether the Commission will indeed be able to produce the guidelines of sufficient precision, equally helpful in all types of processing situations. As Kuner aptly notes, 'given the complexity of this issue, the permissibility of which can often only be judged based on the facts of a particular case, it is unclear how the Commission can produce guidance that is both authoritative and specific enough to be useful.'[106]

4. Conclusions

This contribution critically examined the proposal for a new General Data Protection Regulation on the matter of how it assigns default entitlements in personal data and goes about the principle of informational self-determination. This paper has demonstrated that although informational self-determination has been acknowledged as a normative core of the European regime of data protection in legal doctrine, national and European case-law, as well as in the recent rhetoric around data protection policy-making, there is a risk that the proposed Regulation, if adopted without changes, will lead away from this normative choice towards default entitlements of others to process data. This is done, *first*, by divorcing the objectives of the Regulation from its roots in privacy. The right to data protection in Article 8 of the Charter lacks both clarity as to its content and its own normative weight needed in order to function as a benchmark for assessment of data processing, e.g. when the legitimate interests of the controller and the rights and interests of the data subject are to be balanced against each other, or in proportionality analysis.

Second, the scope of default control rights that the individual has over his/her personal data is reduced compared to the current regime under the Directive. One of the most important control rights – the consent rule – is losing significance as a ground of lawful processing as the strengthened formal requirements to consent are difficult to comply with. Simultaneously, the standards of other grounds of lawful processing, such as legitimate interest of the controller, are easier to meet and put the data processing actors in a position of more control over the data by limiting the data subject's right to demand erasure or invoke the right to data portability. In addition, the Regulation introduces a new exception to the purpose limitation principle that allows further processing for incompatible purposes, provided one ground of lawful processing is present. This exception makes already weakened guarantees of individual control such as the consent requirement, right to object and request erasure, pointless, as their exercise is conditioned

upon a purpose of processing. The control rights and guarantees are not only weak by themselves, but also have a weakening effect on each other.

Third, the proposed Regulation allows a margin to accommodate interests of others in personal data wider than under the Directive. The application of every limitation under the Regulation depends on 'necessity' and some form of balancing of the data subjects' and others' interests against each other.

The distorted normative core of the revised data protection instrument may have negative effect on the outcomes of balancing of the various interests of others in personal data against the interests of the data subject. Namely, the reference to the protection of the largely process-oriented right to data protection as a goal of the instrument in itself does not have normative weigh to provide a counter-balance to the competing claims to personal data. As a result, it is possible to predict that – if left as it is – the proposed Regulation will shift the balance away from the informational self-determination and default individual's entitlement in favour of competing (business) interests and default entitlement of others. There is a danger that the Proposal will put more emphasize on the development of internal market, rather than on the individual's rights regarding his personal data. This is especially remarkable given that on the stage of assessing the existing data protection framework under the 1995 Directive experts did not find that the value choices of the European data protection regime needed reconsideration.[107]

In addition to the disappointment among some privacy advocates, the reassignment of default entitlements in favour of the data processing actors will have more tangible implications. One of the most significant implications is suggested by the so-called endowment effect, meaning that the resource assigned to a market participant by default tends not to change hands and stick with the initial 'owner.'[108] This phenomenon, in terms of data protection, brings an end to the illusion of the possibility to 'buy more privacy' for those who value it more, e.g. in a form of a luxury product, when personal data of an individual is not by default his/hers.

The reform's approach combining the rhetoric of individual control with measures taking this control away from the data subject risks to distort clarity as to the protected scope of the right to data protection, essential for the data subjects in order to understand and defend their rights, for the controllers in order to comply with their obligations, and for the supervisory authorities in order to control the compliance effectively.

The proposed Regulation has been published more than a year ago and there is still no sight of it being adopted. Many explain such a delay with unprecedented lobbying efforts of the information industry and governments of the third countries resulting in nearly 5000 amendments to the document.[109] Peter Hustinx, the European data protection supervisor, reportedly told journalists that failure to approve the legislation before the end of Parliament's term in 2014 would 'have serious repercussions in terms of economic development' and favour lobbyists.[110] In her 7 March 2013 speech, Viviane Reding, EU Commission's Vice-President, commented on the

progress of the ongoing data protection reform: 'Since the beginning of the negotiations, … [t]hose who want to maintain a high level of protection in Europe have recognised the need to move fast. Those who want to lower the level of protection in Europe have tried to slow the file down.'[111] This paper cautions, that the adoption of the Regulation may not necessarily raise the European privacy playing field. The Regulation seems to be drafted in the spirit of 'unlocking' the full (economic) potential of personal data rather than securing informational self-determination, although the policy talk around the proposal is all about improving individual control. In the global and decades-long debate about what should be the core of the data protection efforts – the value of informational self-determination or the use of data, provided the individual is shielded from harm, the Commission seems to have chosen for the latter. This choice alone would be a bitter but acceptable pill to take for the author of this contribution, as well as for many privacy advocates, be it a result of open public debate. However, the Commission made informational self-determination and control a privilege rather than a default right, and implemented this shift in the proposal while still maintaining the rhetoric of individual control and even individual ownership of personal data. This article cautions against the adoption of the proposed Regulation for the sake of changing the status quo alone, as the proposal bears the possibility of reducing the European system of data protection rooted in the values of individual autonomy and informational self-determination to a mere set of administrative rules channelling the flow of personal data, yet without a clear direction.

Dr Nadezhda Purtova, LLM, MSc

Postdoctoral researcher at Tilburg Institute for Law, Technology, and Society (TILT), The Netherlands

n.n.purtova@uvt.nl

Address:
Tilburg Institute for Law, Technology, and Society
Tilburg University
P.O. Box 90153
5000 LE Tilburg
The Netherlands

Bibliography

Books

Bennet 1992
Colin J. Bennett, *Regulating Privacy – Data Protection and Public Policy in Europe and the United States* (New York: Cornell University Press, 1992)

Bygrave 2002
Lee A. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (The Hague; New York : Kluwer Law International, 2002)

Gauch 2003
Hugh G. Gauch, *Scientific Method in Practice* (Cambridge University Press, 2003)

Heisenberg 2005
Dorothee Heisenberg. *Negotiating Privacy: The European Union, the United States, and Personal Data Protection* (Lynne Rienner Pub, 2005)

Kuner 2007
Christopher Kuner, European *Data Protection Law: Corporate Compliance and Regulation*, (2nd edition, Oxford University Press, 2007)

McConnell, Brue & Flynn 2011
C.R McConnell., S.L. Brue, and S.M. Flynn, *Economics: principles, problems, and policies* (19th ed. New York: McGraw-Hill/Irwin, 2011)

Nugter 1990
A.C.M. Nugter, *Transborder flow of personal data within the EC. Boston*, (Kluwer Law and Taxation Publishers, 1990)

Posner 1998
Richard A. Posner, *Economic analysis of law* (Aspen Law & Business, 5th ed. 1998)

Purtova 2012
Nadezhda Purtova, *Property Rights in Personal Data: a European Perspective* (Alphen aan den Rijn: Kluwer Law International (2012)

Robison et al. 2009
Neil Robinson et al., *Review of the European Data Protection Directive: Technical Report Prepared for the Information Commissioner's Office* (Santa Monica: RAND, 2009).

Solove 2006
Daniel J. Solove, Marc Rotenberg & Paul M. Schwartz, *Information Privacy Law* (New York: Aspen Publishers 2006)

Book chapters

Bygrave 2009
Lee A. Bygrave & Dag Wiese Schartum, 'Consent, Proportionality and Collective Power', in Serge Gutwirth et al. (eds), *Reinventing Data Protection?* (Berlin: Springer, 2009)

Cate 2006
F. Cate, 'The Failure of Fair Information Practice Principles', in J.K. Winn (eds) *Consumer Protection in the Age of the Information Economy* (Aldershot/Burlington, VT: Ashgate, 2006)

Gutwirth 2009

Paulde Hert & Serge Gutwirth. 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalization in Action', in Serge Gutwirth et al. (eds), *Reinventing Data Protection?* (Berlin: Springer, 2009)

Rouvroy & Poullet 2009
Antoinette Rouvroy & Yves Poullet, 'The Right to Information Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy', in Serge Gutwirth et al.(eds) *Reinventing Data Protection?* (Berlin: Springer, 2009)

Lynskey 2013
O. Lynskey, 'From market-making tool to fundamental right: the role of the Court of Justice in data protection's identity crisis' in S. Gutwirth et al. (eds), *European Data Protection: Coming of* Age (Berlin: Springer, 2013)

Mayer-Schőnberger 1997
Viktor Mayer-Schőnberger, 'Data Protection in Europe', in P.E. Agre & Marc Rotenberg (eds), *Technology and Privacy: The New Landscape, (Cambridge, Massachusets, London: The MIT Press, 1997)*

Articles

Bagger Tranberg 2011
Charlotte Bagger Tranberg, 'Proportionality and data protection in the case law of the European Court of Justice' (2011) *International Data Privacy Law* 1:4, 239-248

Von Benda-Bekkmann 1995
F. von Benda-Bekkmann, 'Anthropological Approaches to Property Law and Economics' (1995) *European Journal of Law and Economics* 2, 309-306

Bennet 2012
Steven C. Bennet, 'Right to Be Forgotten: Reconciling EU and US Perspectives' (2012), 30 *Berkeley J. Int'l L.* 161, fn 17

Bohme & Koble 2007
Rainer Bohme and Sven Koble, 'On the Viability of Privacy-Enhancing Technologies in a Self-Regulated Business-to-Consumer Market: Will Privacy Remain a Luxury Good?' (2007) Revised version of the paper presented at the Workshop on the Economics of Information Security (WEIS), Carnegie Mellon University, June 2007

Brandimarte, Acquisti & Loewestein 2010
L. Brandimarte, A. Acquisti and G. Loewenstein, 'Misplaced Confidences: Privacy and the Control Paradox' (2010) Ninth Annual Workshop on the Economics of Information Security (WEIS) June 7-8 2010 Harvard University, Cambridge, MA

Brandimarte, Acquisti & Loewestein 2012
L. Brandimarte, A. Acquisti and G. Loewenstein, 'Misplaced Confidences: Privacy and the Control Paradox' (2012) *Social Psychological and Personality Science* 4:3, 340-347

Burkert 1988
Herbert Burkert, 'The Law of Information Technology' (1988) *DuD,* 384–385

Coase 1960
R.H. Coase, 'The Problem of Social Cost' (1960) *J. L. & EcoN* 3, 1–44

Costa & Poullet 2012
Luiz Costa and Yves Poullet, ' Privacy and the Regulation of 2012' (2012) *Computer Law & Security Review* 28, 255

De Hert & Papakonstantinou 2012

Paul De Hert & Vagelis Papakonstantinou, 'The proposed data protection Regulation replacing Directive 95/46/EC: A Sound system for the protection of individuals' (2012) *Computer Law & Security Review* 28, 130-142

Hofmann 2009
Herwig Hofmann, 'Legislation, Delegation and Implementation under the Treaty of Lisbon: Typology Meets Reality' (2009) *European Law Journal* 15:4, 482–505

Jolls, Sunstein & Thaler 1998
Christine Jolls, Cass R. Sunstein and Richard Thaler, 'A Behavioral Approach to Law and Economics' (1998) *Stanford Law Review* 50, 1471-1550

Kahneman, Knetsch & Thaler 1990
Daniel Kahneman, Jack L. Knetsch and Richard H. Thaler, 'Experimental Tests of the Endowment Effect and the Coase Theorem' (1990) *J. POL. EcoN* 98:6, 1325-1327

Koops 2011
Bert-Jaap Koops, 'Forgetting footprints, shunning shadows: A critical analysis of the "right to be forgotten" in big data practice' (2011) *SCRIPTed,* 8:3, 229-256

Kuner 2012
Christopher Kuner, 'The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law,' (2012) *Privacy & Security Law Report*, 11 PVLR 06, 6

Poullet 2009
Yves Poullet, 'Data Protection Legislation: What Is at Stake for Our Society and Democracy?' (2009) *Computer Law & Security Review* 25:3, 211-226

Purtova 2010
Nadezhda Purtova, 'Private law solutions in European data protection: Relationship to privacy, and waiver of data protection rights' (2010) *Netherlands Quarterly of Human Rights* 28 :2, 179-198

Schwartz 2004
Paul M. Schwartz, 'Property, Privacy, and Personal Data'(2004) *Harv. L. Rev.* 117, no. 7

On-line articles and blogs

Davis 2013
Simon Davis, 'Analysis: Why the EU data protection crisis is more perilous than you imagined' (online blog *Privacy Surgeon,* published on 31 May 2013) http://www.privacysurgeon.org/blog/incision/analysis-why-the-eu-data-protection-crisis-is-more-perilous-than-you-imagined/, accessed on 28 August 2013

Wieneke 2008
David Wieneke, 'Is Linkedin for Sale? Does That Mean Your Personal Information Is Too?' (Online Law Blog: How Trademark, copyright, privacy and politics shape the Web, 18 June 2008) http://usefularts.us/2008/06/18/is-linkedin-for-sale-does-that-mean-your-personal-inforamtion-is-too/, accessed 28 August 2013

Speeches

Neelie Kroes, (2012) 'EU Data protection reform and Cloud Computing' SPEECH/12/40, given at "Fuelling the European Economy" event, Microsoft Executive Briefing Centre, Brussels, 30 January 2012, available online at http://europa.eu/rapid/press-release_SPEECH-12-40_en.htm?locale=EN)

Neelie Kroes, (2013) "The Economic and social benefits of big data." Speech given on 23 May 2013 at Webcast Conference on Big Data, Brussels, available online at http://europa.eu/rapid/press-release_SPEECH-13-450_en.htm

V. Reding, (2013) "The EU's Data Protection reform: Decision-Time is Now", Speech delivered on 7 March 2013 at 2nd Annual Cloud Computing Conference, Brussels, available online at http://europa.eu/rapid/press-release_SPEECH-13-197_en.htm

Notes

[1] COM(2012)11 final (hereinafter referred to as 'the proposed Regulation')

[2] For more detail on evolution of data protection see, e.g. Bennett 1992 and Mayer-Schőnberger 1997).

[3] E.g. Nugter describes the division of the two considerations already on the stage of drafting the data protection directive: "[T]he primary concern of the Commission seemed rather to be more the protection of a European data processing industry, than the safeguarding of individual rights. The European Parliament's primary concern, by contrast, has been the protection of the individual. […] In fact, these different attitudes characterize the many reports, proposals and studies that were to come in the following years" (Nugter 1990 quoted in Heisenberg 2005).

[4] Among others, Commissioner Kroes commenting on the Proposal: "Our proposal starts from everybody owning their own personal data." (Kroes 2012).

[5] The right to informational self-determination has been developed by the German Constitutional Court in 1983, in its famous Census decision (Bundesverfassungsgericht [BVerfG Federal ConstitutionalCourt], Case No. 1 BvR 209/83, 15 Dec. 1983, 65 BVERFGE 1 (Ger.). The Court declared the Census Act of the Federal Parliament unconstitutional based on the provisions of Article 1 (human dignity) and Article 2 (right to free development of personality) and ruled that "basic right warrants [...] the capacity of the individual to determine in principle the disclosure and use of his/her personal data," and further "the authority of the individual to decide himself, on the basis of the idea of self-determination, when and within what limits information about his private life should be communicated to others" (translated in Rouvroy & Poullet 2009 at 45). European and international legal scholarship has adopted this language to define the right to informational self-determination (e.g. De Hert & Gutwirth 2009 at 14, Schwartz 2004). Note, however, that Rouvroy and Poullet treat control over one's personal data as insufficient for achievement of the ideal of informational self-determination (p. 52)).

[6] E.g. Nugter describes the division of the two considerations already on the stage of drafting the data protection directive: "[T]he primary concern of the Commission seemed rather to be more the propotion of a European data processing industry, than the safeguarding of individual rights. The European Parliament's primary concern, by contrast, has been the protection of the individual. […] In fact, these different attitudes characterize the many reports, proposals and studies that were to come in the following years" (Nugter 1990 at 29, quoted in Heisenberg 2005 at 53-54).

[7] e.g. Cate 2006

[8] n. 5

[9] Bygrave 2002 at 84 quoting Burkert 1988, pp. 384–385, and further: 'The predominance of procedural concerns appears symptomatic of legislators' uncertainty about the nature of the interests to be protected, together with a desire for regulatory flexibility in the face of technological complexity and change'.

[10] Some explain this 'identity crisis' of the European data protection by the seemingly contradictory objectives of the Data Protection Directive – market integration and protection of fundamental rights. For a comprehensive analysis of jurisprudence of the Court of Justice reconciling the two see Lynskey 2013 at 59; see Purtova 2012 arguing that the aim of creating internal market means eliminating obstacles for free movement of data rather then a tribute to the laissez-faire doctrine.

[11] Yet, residual differences of national implementation have been one of the driving forces behind the Commission's choice for Regulation as an instrument of the data protection reform (European Commission. 2012. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century", COM/2012/09 final).

[12] For instance, the UK rejected the German proposals for a default consent requirement for data processing as too strict. For an overview of the various competing national and industrial group interests on the stage of drafting of the Directive see Heisenberg 2005 at 51 et seq.

[13] E.g. in Österreischer Rundfunk (Joint cases C-465/00, C-138/01, and C-139/01 [2003] ECR I-6041) concerning the conflict between data protection rights and a public interest in efficient use of public funds, the Court found that if the national Austrian law requiring publication of the officials' salaries is not compatible with Article 8 ECHR, it is also incompatible with the Directive (para. 91).

[14] The author has developed an argument in favour of such interpretation elsewhere (see Purtova 2012).
[15] "Entitlement" in Oxford Online Dictionary at <http://oxforddictionaries.com/definition/english/entitlement?q=entitlement>
[16] McConnell, Brue, & Flynn 2011
[17] Together referred to as 'economic analysis of entitlements'.
[18] See, for instance, Wieneke 2008, reporting that "Bain Capital has bought a 53 million stake in the social networking site LinkedIn. This would bring the total valuation for LinkedIn to just above $1 billion."
[19] Kroes advocates for 'unlocking' personal data and get maximum value from 'big data' to boost European economy ('knowledge is the engine of our economy. And data is its fuel'; 'I want to support a strong European data industry', indicating social network data intelligence company as an example; etc. (Kroes 2013)).
[20] Kroes 2013.
[21] Coase 1960.
[22] Posner 1998 at 11
[23] e.g. Bohme & Koble 2008.
[24] For a detailed overview and analysis of behavioural economics criticism of conventional (neoclassical) economics, including the endowment effect, see Jolls, Sunstein & Thaler 1997-1998; for a perspective of anthropology of law see Benda-Bekkmann, von 1995.
[25] e.g. Kahneman, Knetsch, & Thaler 1990.
[26] A recent study showed that 'mere control over publication of private information affects individuals' privacy concerns and their propensity to disclose sensitive information even when the objective risks associated with such disclosures do not change or, in fact, worsen.' (Brandimarte, Acquisti, & Loewenstein 2010).
[27] Brandimarte, Acquisti, & Loewenstein 2010 (italics added – NP).
[28] Although the right to data protection has firmly entered the European policy and academic discourse, as well as EU constitutional texts in Article 8 of the EU Charter of fundamental rights, the exact contours of this right are still being debated. During the 2012 data protection reform efforts, e.g. it is still debated whether such new elements as a right to be forgotten and data portability should be part of the modern data protection regime (see Koops 2011; arguments concerning the classification of the right to data portability as a data protection right - UK Ministry of Justice, Call for Evidence on the Proposed EU Data Protection Legislative Framework: Summary of responses, published on 28 June 2012 available online at https://consult.justice.gov.uk/digital-communications/data-protection-proposals-cfe (last accessed on 30 July 2012) on whether the right to data portability is a data protection right or a consumer protection measure).
[29] These choices are consistent with the two-step analysis under Article 8 ECHR: first, to establish whether an interest interfered with lies within the scope of the right, and subsequently to determine whether the limitation of the right is legitimate.
[30] E.g. balancing between the right to private life and 'interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others' under Art.8(2) ECHR; weighing 'legitimate interests pursued by the controller' against 'the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)' (referring to 'the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data') under Art.7(f) 1995 Directive, etc.
[31] Purtova 2012
[32] see also de Hert & Gutwirth 2009 at 15.
[33] Costa & Poullet 2012 at 255.
[34] Ibid.
[35] Case C-101/01 Bodil Lindqvist [2003] ECR I-12971, para. 86: "In that context, fundamental rights have a particular importance, as demonstrated by the case in the main proceedings, in which, in essence, Mrs Lindqvist's freedom of expression in her work preparing people for Communion and her freedom to carry out activities contributing to religious life have to be weighed against the protection of the private life of the individuals about whom Mrs Lindqvist has placed data on her internet site." Case C-73/07 Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy [2008] ECR I 9831, para. 52, and others.
[36] E.g. Joined Cases C-465/00, C-138/01, and C-139/01 Osterreichischer Rundfunk [2003] ECR I-6041, para. 68.
[37] Ibid. para. 70

[38] Ibid. para. 72, 91.
[39] Consolidated versions of the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU) [2010] OJ C83/1.
[40] Charter of Fundamental Rights of the European Union [2010] OJ C83/ 389
[41] Joined cases C-92/09 and C93/09, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen, [2010] ('[A]ccording to Article 52(3) of the Charter, 'in so far as it contains rights which correspond to rights guaranteed by the Convention, the meaning and scope of those rights are to be the same as those laid down by the Convention.') … In those circumstances, it must be considered that the right to respect for private life with regard to the processing of personal data, recognised by Articles 7 and 8 of the Charter, concerns any information relating to an identified or identifiable individual (see, in particular, European Court of Human Rights, Amann v. Switzerland [GC], no. 27798/95, § 65, ECHR 2000-II, and Rotaru v. Romania [GC], no. 28341/95, § 43, ECHR 2000-V) and the limitations which may lawfully be imposed on the right to the protection of personal data correspond to those tolerated in relation to Article 8 of the Convention.' paras. 51-52).
[42] On proportionality in data protection case-law of the Court of Justice see Bagger Tranberg 2011.
[43] see also Kuner 2007 at 76 (As Kuner explains, the various Member States conduct this balancing act differently and 'data controllers must examine local law in detail to determine if the exception applies').
[44] See '"Whatever is less dense than water will float, because whatever is less dense than water will float" sounds stupid, but "Whatever is less dense than water will float, because such objects won't sink in water" might pass.' Bringing an example of circular reasoning (Gauch 2003 at 184.)
[45] Article 6(5) of the proposed Regulation reads: 'The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.'
[46] Hofmann 2009 at 491, on Article 290 of the Treaty on the Functioning of the European Union.
[47] Bygrave 2002 at 87
[48] Bygrave 2002.
[49] Paragraph 27 Explanatory Memorandum to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data available at <www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#memorandum>.
[50] Bygrave 2002 at 63.
[51] Paragraph 13 of the OECD Guidelines reads as follows:
An individual should have the right:
a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
[52] Bygrave 2002 at 63
[53] See Poullet 2009.
[54] de Hert & Gutwirth 2009 at 14.
[55] Bygrave 2002, pp. 63–66.
[56] Ibid. at 64.
[57] Ibid. at 65.
[58] Ibid. at 65.
[59] Kuner 2007 at 212, para. 4.105.
[60] Bygrave 2002 at 65.
[61] e.g. "The aim of the new legislative acts proposed by the Commission is to strengthen rights, to give people efficient and operational means to make sure they are fully informed about what happens to their personal data and to enable them to exercise their rights more effectively. To strengthen the right of individuals to data protection, the Commission is proposing new rules which will: Improve individuals' ability to control their data […]" ((COM/2012/09 final) Communication from the Commission to the European Parliament, the Council, the European Economuc and Social Committee and the Committee of the Regions "Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century"); Neelie Kroes commented on the proposed reform: "Our proposal starts from everybody owning their own personal data. It can only be used with good reasons. You can correct it, get a copy in a commonly-used, interoperable format to go on using it elsewhere, or to have it deleted" (Kroes 2012).

[62] ((COM/2012/09 final) Communication from the Commission to the European Parliament, the Council, the European Economuc and Social Committee and the Committee of the Regions "Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century"). Costa and Poullet 2012 and De Hert & Papakonstantinou 2012 consider these and other data protection innovations in more detail.

[63] 'In a small number of jurisdictions, the consent requirement has been given priority over the other preconditions such that a data controller must ordinarily obtain the data subject's consent to the processing unless this would be impracticable. [fn. 18: the case, e.g., in Estonia and, to a lesser extent, Belgium and Greece. […] In Belgium, consent is given priority only with respect to processing of sensitive personal data.] It is doubtful that the Directive, as originally conceived, mandates such prioritisation. However, the Directive does not disallow it.' Bygrave further argues that ECtHR jurisprudence may develop to push data protection *towards prioritising consent (*Bygrave & Wiese Schartum 2009).

[64] 'The Article 29 Working group has taken the view that where as a necessary and unavoidable consequence of the employment relationship an employer has to process personal data, it is misleading if it seeks to legitimize this processing through consent. Reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment.' (Article 29 Working Party, 'Opinion 8/2001 on the processing of personal data in the employment context' (WP 48, 13 September 2001), 3).

[65] Kuner 2007 at 211.

[66] Ibid. at 68

[67] Ibid. at 68–69 ('Some member state laws also restrict the possibility to give consent electronically. For instance, under the German Federal Data protection Act, consent to the processing of personal data must be given "in writing", meaning pen on paper, unless consent is to be given in the course of using "teleservices" under the Teleservices Data protection Act, in which case consent may be given electronically under certain conditions.')

[68] Article 29 Working Party, 'Opinion 8/2001 on the processing of personal data in the employment context' (WP 48, 13 September 2001), 3, stating '[t]he Article 29 Working group has taken the view that where as a necessary and unavoidable consequence of the employment relationship an employer has to process personal data it is misleading if it seeks to legitimize this processing through consent. Reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment' (cited in iybid., pp. 211–212). See also Nikon v. Onof, decision No. 4164 (2 October 2001), in which the French Cour de Cassation did not allow the reading of an employee's email messages, even with the employee's consent (cited in Kuner 2007 at 212, fn. 214).

[69] Working Document: Article 26(1) at 11 reads: 'the Working Party suggests that consent is unlikely to provide an adequate long-term framework for data controllers in cases of repeated or even structural transfers for the processing in question.' (Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995.)

[70] Kuner 2007 (e.g. WO, 'Working document of the surveillance of electronic communications in the workplace' (WP 55, 29 May 2002)).

[71] Article 7 (Conditions of consent):
1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.
2. If the data subject's consent is to be 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.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.
4. 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."

[72] SEC(2012) 72 final, Commission Staff Working Paper "Impact Assessment" at 76

[73] Bygrave & Wiese Schartum 2009.

[74] Article 29 Working Party. 2013. Opinion 03/2013 on purpose limitation, adopted on 2 April 2013 00569/13/EN WP 203, at14

[75] WP 203 at 15

[76] WP 203 at 11

[77] for the purpose specification assessment of the EU open data initiatives see Article 29 Working Party. 2013. Opinion 06/2013 on open data and public sector information ('PSI') reuse, adopted on 5 June 2013, 1021/00/EN WP 207

[78] WP 203 at 11
[79] WP 203, pp. 11-12
[80] WP 203 at 12
[81] WP 203, pp. 25-26
[82] WP 203, pp. 22-23
[83] such as freely given and informed consent for using privately taken photos on a commercial website for promotional purposes in Example 7, WP 203 at 60.
[84] Compare criticism of the reasonable expectations of privacy test in the US information privacy law: as Solove, Rotenberg, and Schwartz point out, there is a fundamental flaw or paradox at the core of the reasonable expectation of privacy test: 'legal protection is triggered by people's expectations of privacy, but those expectations are, to a notable extent, shaped by the extent of the legal protection of privacy' (Solove, Rotenberg & Schwartz 2006 at 251).
[85] WP 203 at 11, 12, 27, 33 etc. This interpretation is based on the language of Article 8 of the EU Charter of Fundamental Rights naming the requirements separately (WP 203 at 11).
[86] WP 203 at 33.
[87] WP 203 at 11.
[88] Article 6(4) of the proposed Regulation reads: 'Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.'
[89] WP 203 at 36
[90] WP 203 at 37
[91] WP 203 at 36
[92] "Our proposal starts from everybody owning their own personal data. It can only be used with good reasons. You can correct it, get a copy in a commonly-used, interoperable format to go on using it elsewhere, or to have it deleted." Speech of Nelie Kroes given in January 2012 (Kroes 2012).
[93] Purtova 2011 at 85
[94] Kroes 2012
[95] Bennet 2012, fn 17 and literature cited there.
[96] De Hert & Papakonstantinou 2012

[97] Kroes 2012.

[98] SEC(2012) 72 final, Commission Staff Working Paper "Impact Assessment" at 76
[99] The German Constitutional Court states that '[t]he individual does not have a right in the sense of an absolute, unlimited 'mastery' over 'his' data; he is rather a personality that develops within a social community and is dependent upon communication.' Bundesverfassungsgericht [BVerfG – Federal Constitutional Court], Case No. 1 BvR 209/83, 15 Dec. 1983, 65 BVERFGE 1, para. 44, quoted in Buitelaar at 22
[100] See, e.g., the conditions of legitimate processing in Articles 7 and 8 of the 1995 Directive.
[101] Although the human rights nature of data protection implies that there is a limit to what an individual can agree to (see Purtova 2010).
[102] Namely, if (b) the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract; or
(c) compliance with a legal obligation of the controller; or
(d) to protect the vital interests of the data subject; or
(e) the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
(f) the legitimate interests pursued by the controller or by the third party or parties, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1) (**for the general categories of personal data**); and
(b) carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law; or
(c) the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or
(e) data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims (**for the special categories of personal data**).

[103] The conditions of lawful processing remained largely the same except a newly added Article 8 requirement of the Regulation that the personal data of a child under the age of 13 is to be processed with the consent of the parents or other legal representatives only, and special regime of processing of health data and data processed for scientific, statistical and research purposes (in Articles 81 and 83 of the Regulation).

[104] See, e.g. Bygrave & Wiese Schartum 2009 at 163.

[105] Kuner 2007 at 76.

[106] Kuner 2012.

[107] e.g. Robinson et al. 2009.

[108] e.g. Kahneman, Knetsch & Thaler 1990.

[109] Davis 2013.

[110] "New data protection rules at risk, EU watchdog warns", 30 May 2013, available online at http://www.euractiv.com/infosociety/eu-watchdog-warns-lobbyists-parl-news-528128, last accessed on 18 July, 2013

[111] Reding 2013.