This is a draft version. Final version published in International Data Privacy Law, 2014-3.

Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation

Currently under discussion is the European Commission's proposal for a General Data Protection Regulation, which will replace the Data Protection Directive from 1995 over time. The Regulation proposes to introduce a number of specific obligations and rights in order to protect the interests of the citizen and consumer and provides far-reaching powers for governmental agencies to enforce these rules. However, not only is this directly against the original purpose of and ratio behind data protection rules, moreover, an increased emphasis on consumer interests and rights to control personal data seems an inadequate tool for solving the current problems involved with Big Data.

With the Charter of Fundamental Rights of the European Union from 2000, coming into force in 2009, in which the right to data protection is contained in a provision (article 8) separated from the right to privacy (article 7), and the plans to adopt a European Union wide General Data Protection Regulation, the still young right to data protection seems to have reached the point of maturity. Its origins lie partially in the data protection rules of northern European countries arising in several countries in the seventies of the last century and the Council of Europe's Resolutions on data processing[1] and partially in the U.S. and the realization of the so called Fair Information Practices (FIPs), which were developed because the right to privacy was thought unfit for the 'modern' challenges posed by large automated data processing.[2] The increased use of large data bases by (primarily) governmental organisations raised a number of problems for the traditional conception of the right to privacy, which is aimed at protecting the private interests of the citizen, among others, by giving him a right to control over private and sensitive data.[3] First, data processing often does not regard private or sensitive data, but public and non-sensitive data such as car ownership, postal codes, number of children, etc.[4] 'Dictionary definitions of privacy uniformly speak in terms of seclusion, secrecy, and withdrawal from public view. They all denote a quality that is

[1] U Dammann, O Mallmann & S Simitis (eds.), Data protection legislation: an international documentation: Engl.-German: eine internationale Dokumentation = Die Gesetzgebung zum Datenschutz (1st edn, 1977). FW Hondius, Emerging data protection in Europe (1st edn, 1975). Organisation for Economic Co-operation and Development, Policy issues in data protection and privacy: concepts and perspectives: proceedings of the OECD seminar, 24th to 26th June 1974 (1st edn, 1976). H Burkert, Freedom of information and data protection (1st edn, 1983).

[2] See among others: Privacy Protection Study Commission, Personal privacy in an Information Society (1st edn, 1977). Federal Trade Commission, Privacy online: A report to congress (1st edn, 1998).

[3] See also: The Privacy Act of 1974 5 U.S.C. § 552a. See further: H Burkert, Freedom of information and data protection (1st edn, 1983).

[4] See for the distinction between 'private' and 'personal' data: R Wacks, Personal Information: Privacy and the Law (1st edn, 1989) 21-25. See for the distinction between 'private' and 'public' among others: S Strömholm, Right of Privacy and Rights of the Personality (1st edn, 1967) 65-75.

not inherent in most record-keeping systems', one of the U.S. governmental reports from 1973 established.[5]

Secondly, and related to that, the traditional privacy definitions emphasized the right 'of the data subject as having a unilateral role in deciding the nature and extent of his self-disclosure. None accommodates the observation that records of personal data usually reflect and mediate relationships in which both individuals and institutions have an interest, and are usually made for purposes that are shared by institutions and individuals.'[6] Because data processing often does not regard private and sensitive data, the right to control by the data subject was felt undesirable, because governments need such general data to develop, among others, adequate social and economic policies, and unreasonable, because in contrast to private and privacy sensitive data, data subjects have no or substantially less direct and personal interest in controlling (partially) public and general information. Consequently, instead of grating a right to control, the focus of these principles was on the fairness and reasonableness of the data processing, for example by specifying that data should not be collected and processed when this was not necessary for or proportionate to the goal pursued and by laying down that the data should be correct and kept up to data, so as to guarantee that the profile of a person or a group of people was accurate.[7]

This first concern (that data processing often regards non-sensitive or public data) has remained an identifying element of data protection instruments and the definition of personal data has even been further stretched to cope with the increased possibilities of identification.[8] The Council of Europe (CoE) adopted two Resolutions for data processing in 1973 and 1974, one for the public and one for the private sector, which defined 'personal information' simply as information relating to individuals (physical persons).[9] Here, the individual and subjective element in the definition of personal data is still prominent. Already in 1981, however, in the subsequent Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted by the Council of Europe, 'personal data' was defined as any information relating to an identified or identifiable individual.[10] The explanatory report stressed that an 'identifiable person', an element which was new to this definition, meant a person who can be easily identified; it did not cover identification of persons by means of very sophisticated methods.[11] Still, data which were not yet linked to an individual, but could be with relative ease, fell under the scope of the definition.

In the Data Protection Directive of the European Union (EU) of 1995,[12] which remains until now the most important instrument for data protection in Europe, this concept was widened even further. In the original proposal of the Commission, the concept of 'depersonalisation' was contained, which signified modifying personal data in such a way that

[5] Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers and the Rights of Citizens (1st edn, 1973).
[6] Records, Computers and the Rights of Citizens (1973).
[7] See further: AF Westin & MA Baker, Databanks in a Free Society: Computers, Record-keeping and privacy (1st edn, 1972).
[8] Likewise, the impossibility to own and to privatize information may have had an influence: FW Hondius, Emerging data Protection in Europe (1st edn, 1975) 103-105.
[9] Council of Europe. Committee of Ministers, Resolution (73) 22 On the Protection of the privacy of individuals vis-à-vis electronic data banks in the private sector. (Adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies). Council of Europe. Committee of Ministers, Resolution (74) 29 On the Protection of the privacy of individuals vis-à-vis electronic data banks in the public sector. (Adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies).
[10] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, article 2 sub a.
[11] <http://conventions.coe.int/Treaty/EN/Reports/HTML/108.htm>.
[12] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

the information they contain can no longer be associated with a specific individual or an individual capable of being determined except at the price of an excessive effort in terms of staff, expenditure and time.[13] The Directive would not be applicable to those data. However, the advisory report of the Economic and Social Committee suggested deleting the reference to an 'excessive effort', 'for a processing task requiring an excessive effort today may require no effort at all next year.'[14] The European Parliament proposed to further limit this concept and in the final proposal it was deleted altogether,[15] although a special position has been reserved for personal data processed for statistical purposes.[16] At the same time, at the suggestion of the Parliament,[17] the definition of personal data was enlarged by specifying that 'an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.'[18]

It not only introduces a very wide, and non-exhaustive, list of possible identifying factors, the possibility of 'indirect' identifiable data was also inserted.[19] The Article 29 Data Protection Working Party (Working Party), the advisory body installed by the Data Protection Directive, has clarified that this suggests that even 'ancillary information, such as "the man wearing a black suit" may identify someone out of the passers-by standing at a traffic light. So, the question of whether the individual to whom the information relates is identified or not depends on the circumstances of the case.'[20] Finally, this trend of a widening scope may also be witnessed[21] in the proposal for a General Data Protection Regulation, which will replace the Data Protection Directive over time, in which personal data is defined in a slightly broader manner. The reason for this, as is acknowledged by the Working Party and is increasingly emphasized by scholars, is that potentially all data could be personal data. Data which at one moment in time may contain no information about a specific person whatsoever, may in the future be used, through advanced techniques, to identify or individualize a person.[22]

---

[13] Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data COM(90) 314 final — SYN 287 (Submitted by the Commission on 27 July 1990) (90/C 277/03)

[14] Economic and Social Committee, opinion on: — the proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, — the proposal for a Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the integrated services digital network (ISDN) and public digital mobile networks, and — the proposal for a Council Decision in the field of information security. 17. 6. 91 Official Journal of the European Communities No C 159/38-48.

[15] No C94/176, Official Journal of the European Communities, 13 April 1992. Wednesday, 11 March 1992.

[16] Article 6 and 11 Directive 95/46/EC.

[17] No C94/176, Official Journal of the European Communities, 13 April 1992. Wednesday, 11 March 1992.

[18] Article 2 sub a Directive 95/46/EC.

[19] This was even broadened further: ECJ (Third Chamber), Worten – Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho (ACT), 30 May 2013, Case C-342/12.

[20] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN, WP 136, 20 June 2007, Brussels, p. 13.

[21] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), {SEC(2012) 72 final}, Brussels, 25 January 2012, COM(2012) 11 final, 2012/0011 (COD), article 4 (1).

[22] D Skillicorn, Knowledge Discovery for Counterterrorism and Law Enforcement (1st edn, 2009). DT Larose, Data mining methods and models (1st edn, 2006). M. Hildebrandt & S. Gutwirth (red.), 'Profiling the European Citizen Cross-Disciplinary Perspectives', New York, Springer, 2008. C. Westphal, 'Data mining for Intelligence, Fraud & Criminal Detection', Boca Raton, Taylor & Francis Group, 2009. K. Guzik, 'Discrimination by Design: Data Mining in the United States's "War on Terrorism", Surveillance & Society, 2009-7. P. Kuhn, 'Sex discrimination in labor markets: The role of statistical evidence', The American Economic Review, 1987-77. M. LaCour-Little, 'Discrimination in mortgage lending: A critical review of the literature', Journal of Real Estate Literature, 1999-7. G. D. Squires, 'Racial profiling, insurance style: Insurance redlining and the uneven development of metropolitan areas', Journal of Urban Affairs, 2003-25.

Moreover, data that may not alone identify a person can increasingly be linked, among other through interconnecting and harvesting databases, and be used to create profiles so that two or more non-identifying datasets may become identifying datasets if integrated.[23]

In conclusion, the first of the two reasons underlying the creation of the FIPs and the early European data protection rules, as separated from the right to privacy, was that personal data are often neither private nor sensitive. Currently, this is even more so and even non-identifiable information can be connected and harvested through the use of advance techniques in order to create profiles. Consequently, to cope with the fact that personal data are less and less linked to the individual subject, the definition of personal data has been widened and broadened over time.[24] However, the second principle, which moved the concept of subjective rights and the individual's right to control over personal data to the background, in favour of general obligations of fairness and reasonableness for the data controller, is increasingly lost. More and more, emphasis has been put on (1) increasingly detailed and specific obligations for data controllers, (2) specific subjective rights of the data subject and (3) a high level of enforcement of the duties and rights. The gradual development on these three points will be discussed in detail in the following three sections. Finally, an analysis will be provided and it will be suggested on what accounts this approach might fail.

As an example of early data protection legislation, this article focusses on the FIPs and the CoE Resolutions, but the conclusions reached about those rules are equally applicable to the early data protection rules in European countries such as Sweden, Germany (especially Hesse), France and Austria.[25] Similarly, this research will focus on the CoE's Convention from 1981, although similar rules might be found in the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data from 1980 by the Organisation for Economic Co-operation and Development (OECD).[26] Finally, for the sake of clarity and conciseness, reference will be made only to the original proposal of the Commission for a General Data Protection Regulation and not, for example, to the amended LIBE version by Jan Albrecht.[27] Although this proposal is substantially different on certain aspects, this is not so in its view on the importance of data subject control. Consequently, the general argument made in this paper applies both to the Commission's and the Parliament's proposal, but will be exemplified by reference to the former only. At the time of writing, the adoption and final outcome of the Regulation is still uncertain.

The main goal of this paper is to engage critically with scholars and commentators who have focused on the Informational Self-Determination (ISD) aspects of privacy and data protection legislation. Especially, it will address two claims. First, the argument that data protection legislation *is* grounded in concerns over Informational Self-Determination,

---

[23] See among others: M. R. Koot, 'Measuring and predicting anonymity', Amsterdam, Informatics Institute, 2012.

[24] See also: ECJ (Grand Chamber), Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy, Satamedia Oy, 16 December 2008, Case C-73/07.

[25] U. Dammann, O. Mallmann & S. Simitis (eds.), 'Data protection legislation: an international documentation: Engl.-German: eine internationale Dokumentation = Die Gesetzgebung zum Datenschutz', Frankfurt am Main, Metzner, 1977. F. W. Hondius, 'Emerging data protection in Europe', Amsterdam, American Elsevier Pub. Co, 1975. Organisation for Economic Co-operation and Development, 'Policy issues in data protection and privacy: concepts and perspectives: proceedings of the OECD seminar, 24th to 26th June 1974', Paris, Organisation for Economic Co-operation and Development, 1976. H. Burkert, 'Freedom of information and data protection', Bonn, Gesellschaft für Mathematik und Datenverarbeitung, 1983.

[26] <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>.

[27] <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT%2BREPORT%2BA7-2013-0402%2B0%2BDOC%2BXML%2BV0%2F%2FEN&language=EN>.

pointing among others to the German Census Case from 1983,[28] in which the Bundesverfassungsgericht created the basis for a constitutional right to informational self-determination, and to Alan Westin's groundbreaking book Privacy and Freedom from 1967, in which privacy is defined as 'the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others'.[29] Sections 2, 3 and 4 try to tackle this presumption by analyzing the historical development of data protection rules. It is suggested that the focus on Informational Self-Determination is not prominently reflected in most data protection instruments and that the focus on the individual, his interests and his right to control is really more a recent development. Secondly, proponents of the ISD movement argue that data protection rules *should* focus on Informational Self-Determination as this provides the individual with tools to protect his own interests, which is either believed to be valuable in and for itself or to be an (or even the most) effective method of data protection, or both.[30] Section 5 of this paper will address this normative question, discus some challenges for ISD, especially in relation to Big Data, and argue why a re-emphasize on general duties of care might prove worthwhile in the current technological environment.

The table below provides an overview of sections 2, 3 and 4 of this research. In the left column, the data protection instruments (discussed in this study) are listed in chronological order. The FIP's from 1972-1973, the two CoE Resolutions from 1973 and 1974, the CoE Convention from 1981, the EU Directive from 1995 and the proposal for a General Data Protection Regulation from the Commission from 2012. The second column shows the broadening of the concept of 'personal data' over time and with it, an expanded material scope of the data protection instruments. The last column shows an increased emphasis on the protection of the individual, his interests and his right to control personal data in the substantial provisions of those instruments. This is divided in three sub-columns: the development from general duties of care to detailed and technology-specific obligations (column 2a corresponding to section 2 of this study); the development from very marginal subjective rights to a quite strong emphasis on individual rights (column 2b corresponding to section 3 of this study); the development from a model with a focus on soft-law (with code-of-conduct-like rules) to one which embeds strong rules on enforcement (column 2c corresponding to section 4 of this study).

Historical overview of Data Protection instruments:

	(1) Material scope of the instruments: the definition of personal data	**(2) The substantive provisions of the regulations**		
		(2a) Obligations	**(2b) Rights**	**(2c) Enforcement**
FIPs	-	(1) Transparency (2) Principles of	(1) Access to personal data	Mainly a matter of good governance

[28] BVerfG, Urteil v. 15. Dezember 1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/8.
[29] A. F. Westin, 'Privacy and freedom', The Bodley Head, London, 1970.
[30] This argument may be invoked separately from the first. Even if data protection rules did originally not or only to a limited extent protect the individual, it could still be argued that it would be good to introduce such focus.

		fairness	(2) Marginal rights on rectification and erasure	
Resolutions	Information relating to individuals (physical persons)	(1) Transparency (Pub. Sec) (2) Principles of fairness	(1) Access right	Recommends governments to take all steps necessary
Convention	Information relating to an identified or identifiable individual	(1) - (2) Principles of fairness	(1) Access to and communication of personal data (2) Marginal rights on rectification and erasure	(1) Parties shall establish sanctions and remedies (2) Cooperation states & DPAs & role CoM (3) Remedy of data subject if data controller denies request
Directive	Information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;	(1) Information to the data subject & Notification DPA (2) Principles of fairness (3) Grounds for legitimate data processing	(1) Access to and communication of personal data (2) Marginal rights on rectification and objection (3) Marginal right against automatic decision making	(1) Parties shall establish sanctions and remedies (2) Cooperation states & DPAs + harmonization through Directive and WP 29 (3) Marginal subjective right to remedy and compensation
Regulation	An identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;	(1) Notification in case of data breach (2) Principles of fairness (3) Grounds for legitimate data processing – increased emphasis on consent (4) Accountability duty (multifaceted)	(1) Access to personal data (scope broadened) (2) Right to data portability (3) Rights to rectification and objection (4) Right to be forgotten (5) Right against profiling	(1) High sanctions (2) Total harmonization trough Regulation; increased powers Commission and EDPB; one-stop shop system (3) Several subjective rights to remedy and compensation

2. Obligations of the data processor

The Fair Information Practices were developed against the background of the up rise of large data bases. These data bases were used to process large quantities of citizens' data, primarily, though not exclusively, by governmental agencies in relation to civil data, such as regarding marriage, car ownership and number of children, statistical data, for social-

economic policies, and intelligence data, used for security purposes.[31] The principles primarily regarded the general fairness of these processes and specified two general obligations, which may be qualified as duties of care: to be transparent and to process data fair and legitimate. First, agencies were encouraged to publish an annual public notice which contained, among others, the name of the data system, the nature and purpose of the system, the categories and number of persons on whom data are maintained, the categories of data maintained, the organization's policies and practices regarding data storage, duration of retention of data, and disposal thereof. This obligation of transparency was thus primarily linked to the principle of accountability; the public had an interest to know which data the government collected, for what reasons and how they were processed. The annual notice was consequently directed at the public as a whole and not at specific individuals.

Secondly, the principles specified, inter alia, that personal data should not be further processed or transferred to third parties, that controllers should appoint a person in the organization responsible for the data processing, that reasonable precautions should be taken against data breaches and that a complete and accurate record of every access to and use made of any data in the system should be maintained. Moreover, it was lined out that the data should be stored with such accuracy, completeness, timeliness, and pertinence as is necessary to assure accuracy and fairness in any determination relating to an individual's qualifications, character, rights, opportunities, or benefits, that may be made on the basis of such data and that data should be eliminated from computer-accessible files when the data are no longer timely. These principles thus regarded very general obligations of fair processing, which may be linked to the principle of good governance. Note moreover that the requirement of keeping data correct and up to date may require gathering and processing more, not less data.[32]

At around the same time, the Council of Europe adopted two Resolutions, one for data processing in the public sector (1974) and one for the private sector (1973). They contained quite similar obligations for controllers. For the public sector, it specified that the public should be kept regularly informed about the establishment, operation and development of large data bases (the principle of transparency and accountability)[33] and, among others, that the information stored should be obtained by lawful and fair means, accurate and kept up to date, appropriate and relevant, stored safe and processed confidentially and that sensitive data should be processed with special care (the principle of fairness and good governance).[34] For the private sector, the second category of obligations also applied, but the obligation of transparency and accountability did not.[35]

The Convention of the CoE was directed at the members to the Council, who were encouraged to implement the rules, with regard to the public and the private sector. The principles of fairness were transposed to the Convention, such as the rules for data security, extra protection for sensitive data and the quality of data, such as that data must be obtained and processed fairly and lawfully, stored for specified and legitimate purposes and not used in a way incompatible with those purposes, that data should be adequate, relevant and not excessive in relation to the purposes for which they are stored, accurate and, where necessary, kept up to date and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.[36] Remarkably, however, like the Resolution regarding the private sector (1973), the principle of transparency

[31] Records, Computers and the Rights of Citizens (1973).
[32] B. van der Sloot, 'From Data Minimization to Data Minimummization', in: B. Custers, T. Calders, B. Schermer & T. Zarsky (eds.), Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases, Springer: Heidelberg 2012, p. 273-287.
[33] Article 1 Resolution (1974).
[34] Articles 2, 3, 4, 6 and 7 Resolution (1974).
[35] Articles 1, 2, 3, 4, 5, 7, 8 and 9 Resolution (1973).
[36] Article 5, 6 and 7 Convention (1981).

and the obligation to inform the public was omitted, which seems to reflect the consideration, contained in the explanatory report to the Convention, that 'most international data traffic occurs in the private sector'.[37]

The original proposal of the Commission for the Data Protection Directive contained two separate regimes, one for the public sector and one for the private sector. However, on the suggestion of the Parliament, this distinction was deleted and the principles were applied to both. Still, both the original proposal and the adopted version contain an important exemption for security related data processing, so that a large part of governmental data processing does not fall under its scope, but is regulated through a special Council Decision, which contains less strict rules and obligations.[38] Thus the core framework for data protection is primarily aimed at the private sector, which reflected the trend of the so called 'banalisation' of data processing, i.e. that governmental agencies, private companies and individuals alike can process large amounts of data with relative ease.[39]

Under the Directive, two important changes have been made. First, the transparency principle is reintroduced, but in a quite different form. There is on the one hand the obligation to notify the national Data Protection Authority (DPA) about the processing of personal data, although Member States are at liberty to adopt quite far-reaching exemptions. Moreover, the duty to inform the public of large scale data processing was transformed to a duty to notify the data subject itself. Thus, article 10 specifies that the controller must provide a data subject from whom data relating to himself are collected with at least the identity of the controller, the purposes of the processing for which the data are intended and the recipients of the data.[40] Consequently, the transparency principle is transformed from a duty to notify the public, to a duty to notify the data subject himself.

Secondly, the obligations of fairness are broadened. The principles of fair and lawful, safe and confidential data processing, of data quality and special care for sensitive data, among others, have all been transposed to the Directive. New is that it stipulates six grounds for legitimate data processing. The Commission, in its original proposal, suggested that only in specified and limited scenarios, could data be legitimately processed in the private sector without the informed consent of the data subject. On the suggestion of the Parliament, however, the informed consent of the data subject was made but one among several grounds.[41] Accordingly, personal data may only be processed if (a) the data subject has given his consent, when this is necessary (b) for the performance of a contract with the data subject, (c) for compliance with a legal obligation, (d) for the protection of the vital interests of the data subject or (e) for the performance of a task carried out in the public interest[42] or (f) when the interests of the controller to process the data outweigh those of the data subject.[43]

The European Court of Justice (ECJ), remarkably, has held that the principles of data quality and the obligation to obtain a legitimate ground for processing have direct effect, in that they may be relied on by an individual before the national courts to oust the application of rules of national law which are contrary to those provisions.[44] Although this does not make

[37] Article 3 Convention (1981).
[38] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, p. 60.
[39] Council of Europe report: New technologies: a challenge to privacy protection? (1989). <http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/NewTechnologies_1989_en.pdf>.
[40] Article 10 Directive 95/46/EC. See also: Article 11 Directive 95/46/EC.
[41] No C94/181, Official Journal of the European Communities, 13 April 1992. Wednesday, 11 March 1992.
[42] See further: ECJ (Grand Chamber), Heinz Huber v Bundesrepublik Deutschland, 16 December 2008, Case C-524/06.
[43] Article 7 Directive 95/46/EC.
[44] ECJ, Rechnungshof (C-465/00) and Österreichischer Rundfunk, Wirtschaftskammer Steiermark, Marktgemeinde Kaltenleutgeben, Land Niederösterreich, Österreichische Nationalbank,

them a subjective right, the provisions may be invoked by the subject directly, even though they are formulated as obligations of the data processor and not as rights of the data subject. With the proposed General Data Protection Regulation, a reemphasis on the element of consent and the control of the subject over his personal data (echoing the line proposed in the Commission's original proposal for the Directive) seems at hand.[45] The definition of consent has been tightened,[46] it has been clarified that the controller shall bear the burden of proof for the data subject's consent[47] and a provision is inserted which specifies that the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given by the child's parent or custodian.[48] Finally, the Regulation also provides that consent shall not provide a legal basis for data processing, where there is a significant imbalance between the position of the data subject and the controller.[49]

Secondly, although the general rules on fair and lawful processing, conditions regarding sensitive data,[50] grounds for legal processing and the principles data quality have been largely retained, they are supplemented with very detailed and technology-specific rules, which are designed to regulate a specific existing technology. Not only does the controller have the obligation to verify whether he processes personal data of children and whether the consent obtained was given by the child's parents or custodian,[51] the controller also has a general 'accountability duty'.[52] This duty is used as an umbrella concept under which falls a myriad of obligations, such as the keeping of very detailed and precise documentation on all processing operations, making data protection impact assessments,[53] assessing the risk concerned with certain types of data processing, on the basis of which, among others, further and stronger technical measures may need to be taken,[54] the obligation to appoint a data protection officer, etc.[55]

Perhaps most importantly, the principle of transparency has been almost completely lost.[56] The obligation of a general notification to the supervisory authority has been replaced

---

Stadt Wiener Neustadt, Austrian Airlines, Österreichische Luftverkehrs-AG, and between Christa Neukomm (C-138/01), Joseph Lauermann (C-13 9/01) and Österreichischer Rundfunk, 20 May 2003, Joined Cases C-465/00, C-138/01 and C-139/01. See also: ECJ (Third Chamber), Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10), Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) v Administración del Estado, intervening parties: Unión General de Trabajadores (UGT) (C-468/10 and C-469/10), Telefónica de España SAU (C-468/10), France Telecom España SA (C-468/10 and C-469/10), Telefónica Móviles de España SAU (C-469/10), Vodafone España SA (C-469/10), Asociación de Usuarios de la Comunicación (C-469/10), 24 November 2011, Joined Cases C-468/10 and C-469/10.

[45] F. Gilbert, 'EU Data Protection Overhaul: New Draft Regulation', The Computer & Internet Lawyer 2012-3, p. 3. P. De Hert & V. Papakonstantinou, 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals', Computer Law & Security Review 2012-28, p. 137-138. G. Hornung, 'A General Data Protection Regulation for Europe? Light and Shade in the Commissions Draft of 25 January 2012', Scipted 2012-1, p. 74.

[46] Article 4 (8) European Commission Proposal (2012). Compare Article 2 (h) Directive 95/46/EC.

[47] Article 7 European Commission Proposal (2012).

[48] Article 8 European Commission Proposal (2012).

[49] Article 7 European Commission Proposal (2012).

[50] See also: ECJ, Bodil Lindqvist, 6 November 2003, Case C-101/01.

[51] Article 8 European Commission Proposal (2012).

[52] Article 22 European Commission Proposal (2012).

[53] Article 33 European Commission Proposal (2012). See already for risk assessments: R. Sizer & P. Newman, 'The Data Protection Act: a practical guide', Gower, Aldershot, p. 188-193.

[54] Article 30 European Commission Proposal (2012).

[55] This does not apply to small companies. Article 35 European Commission Proposal (2012).

[56] Which is remarkable because the evaluation of the directive showed that very little awareness existed about data processing and the data protection rules. Commission of the European Communities, First report on the implementation of the Data Protection Directive (95/46/EC), COM(2003) 265 final, Brussels, 15 may 2003. The reason for losing the notification requirement may lie partially in the costs associated with it. European

by the obligation for controllers and processors to maintain documentation of the processing operations under their responsibility[57] and the obligation to inform the data subject about data processing has been replaced by the obligation to provide transparent and easily accessible and understandable information with regard of the data processing.[58] Only when a data breach has occurred does the controller have an active obligation to inform the data protection authorities,[59] and only when this has a likely adverse effect on the interests of the data subjects will they be directly informed.[60]

3. Rights of the data subject

Initially, the data protection rules contained basically one subjective right, namely the right of the data subject to obtain information about the processing of his personal data. For example, the U.S. Records, Computers and the Rights of Citizens report from 1973 specified that the controller had a duty to inform an individual, upon his request, whether he is the subject of data processing, what use is made of his personal data, who has access to them and to what reason. Some additional rights were also granted, such as that no personal data should be processed beyond the purpose of the data system, that the data subject may contest the accuracy, completeness and pertinence of the personal data, and the necessity for retaining them and the right to request the data to be corrected or amended.

The CoE's Resolution on the public sector, even more narrowly, provided merely that every individual 'should have the right to know the information stored about him'[61] and the Resolution on the private sector provided that as a general rule, 'the person concerned should have the right to know the information stored about him, the purpose for which it has been recorded, and particulars of each release of this information.'[62] The Convention from 1981 again elaborated the list of subjective rights and specified that any person shall be enabled to establish whether his personal data are processed and if so, which, for what purposes and by whom. The data subject was also granted a right to communication to him of such data in an intelligible form and to request rectification or erasure of such data if these had been processed contrary to the obligations of fairness of the data controllers and to have a remedy if a request for confirmation or communication, rectification or erasure was not complied with.[63]

The Data Protection Directive expanded this somewhat and specified three subjective rights. One contained the right of access to personal data, i.e. begetting information about the data processing of his personal data (which data, who processes them, why, etc.)[64] and the right to communication to him in an intelligible form the data undergoing processing.[65]

Commission, Commission Staff Working Paper, 'Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data', {COM(2012) 10 final} {COM(2012) 11 final}{SEC(2012) 73 final}, Brussels, 25.1.2012, SEC(2012) 72 final, p. 15.

[57] Article 28 European Commission Proposal (2012).

[58] Article 11 European Commission Proposal (2012).

[59] Article 31 European Commission Proposal (2012).

[60] Article 32 European Commission Proposal (2012).

[61] Article 5 Resolution (1974).

[62] Article 6 Resolution (1973).

[63] Article 8 Convention (1981).

[64] See also: ECJ (Grand Chamber), Heinz Huber v Bundesrepublik Deutschland, 16 December 2008, Case C-524/06.

[65] Article 12 Directive 95/46/EC.

Second, the data subject has a right to rectification, erasure or blocking of personal data, the processing of which does not comply the data protection rules[66] and a right to object to the processing of his personal data.[67] However, the right to rectification erasure or blocking only exists when the data have an incomplete or inaccurate nature, and thus violate the data quality principle, and the right to object only exists when the processing is executed for direct marketing purposes or based on grounds (e) and (f) for legitimate data processing. Moreover, both contain a right to request only, meaning that data processors may reject such requests if overriding interests exist. Third and finally, every person has a right to object to an automatic decision making process. However, this only applies if a number of conditions are met: the data processing must have legal effects concerning the data subject or significantly affect him, the decisions should be based solely on automated processing of data and should be intended to evaluate certain personal aspects relating to him. Moreover, the right to object to automatic decision making does not apply if such decisions are taken in the course of the entering into or performance of a contract or if it is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.[68]

With the proposal for a General Data Protection Regulation, a radical shift seems at hand. The right to access personal information has been broadened by stressing, among others, the right to be informed about the storage period.[69] A new right is introduced, which is partially based on the data subject's right to obtain the personal data being processed about him, that specifies the data subject's right to data portability, i.e. to transfer data from one electronic processing system to and into another.[70] It provides the right to obtain from the controller those data in a structured and commonly used electronic format, for example facilitating the transfer from Facebook to another social network.[71] It is clear that the philosophy behind this rule is that personal data should be controlled by the data subject, perhaps even owned. The Commission has accordingly stressed that 'retention by data subjects of an effective control over their own data' is an important precondition for ensuring that individuals enjoy a high level of data protection.[72] The right to control over personal data is also in line with the thought that personal data are the modern currency on the internet, namely with regard to the exchange of free internet services for personal data.[73]

The Regulation goes even further and stresses not only the subject's right to rectification,[74] but also introduces a right to be forgotten,[75] which grants the data subject the

[66] Article 12 Directive 95/46/EC.
[67] Article 14 Directive 95/46/EC.
[68] Article 15 Directive 95/46/EC.
[69] Article 15 European Commission Proposal (2012). This is remarkable because it is questionable how effective this right really is: in the evaluation report of the Commission, it appeared that 'most of the data controllers responding to the questionnaire either did not have figures available or received fewer than 10 requests during the year 2001.' Commission of the European Communities, First report on the implementation of the Data Protection Directive (95/46/EC), COM(2003) 265 final, Brussels, 15 may 2003.
[70] S. Weiss, 'Privacy threat model for data portability in social network applications', International Journal of Information Management 2009-29. U. Bojars, A. Passant, J.G. Breslin & S. Decker, 'Social Network and Data Portability using Semantic Web Technologies', <http://ceur-ws.org/Vol-333/saw1.pdf>.
[71] Compare to number portability: Article 30 Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive)
[72] European Commission, 'Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A comprehensive approach on personal data protection in the European Union', Brussels, 4.11.2010, COM(2010) 609 final, p. 7.
[73] See also: M. Kuneva (then Commissioner for Consumer Protection), European Consumer Commissioner, Keynote Speech, p. 2, Roundtable on Online Data collection, targeting and profiling, Brussel, 31 maart 2009.
[74] Article 16 European Commission Proposal (2012).
[75] See also the prior version: <http://www.statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf>.

right to obtain from the controller the erasure of personal data relating to him and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child.[76] The common fear that underlies this right is that children will post online pictures and videos of themselves and eachother which may contain behavior or reveal aspects of their lives which may hinder them in their development, as these videos and pictures may hunt them the rest of their lives. That is why this right also entails an obligation for the controller who has made the personal data public, to inform third parties on the data subject's request to erase any links to, or copy or replication of that personal data.[77] Although some exceptions remain, most importantly in relation to the freedom of speech, it seems that the underlying philosophy is again that the data subject has a right to control his personal data.

Finally, the rights to object and resist automatic processing have been extended quite considerably. The data subject has the right to object to the processing of his personal information if not based on his consent, a contract or a legal obligation. Moreover, the burden of proof is shifted; while in the Directive, the data subject had to convincingly demonstrate that the data processing should be stopped, the Regulation proposes that the processing shall be stopped unless the controller brings compelling legitimate grounds for the continued processing which override the interests or fundamental rights and freedoms of the data subject.[78] Moreover, the right to object to automatic decision making has been transformed into a right to object to profiling in general.[79] Under the Regulation, every natural person shall have the right not to be subject to a measure which produces legal effects or significantly affects him, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyze or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behavior.[80] This prohibition is lifted when the processing is based on his informed consent, is expressly authorized by a law which also lays down suitable measures to safeguard or when this is done in relation to a contractual agreement with the data subject.[81] However, profiling is never legitimate when based solely on sensitive data, such as regarding

[76] I. Szekely, 'The right to forget, the right to be forgotten: Personal Reflections on the fate of personal data in the informationsociety', in: S. Gutwirth, R. Leenes, P. De Hert & Y. Poullet, 'European Data Protection: In Good Health?', Dordrecht, Springer 2012. S. C. Bennett, 'The "Right to be Forgotten": Reconciling EU and US Perceptives', Berkeley Journal of International Law 2012-30.

[77] Article 17 European Commission Proposal (2012).

[78] Article 19 European Commission Proposal (2012).

[79] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies).

[80] W. N. Renke, 'Who controls the past now controls the future: counter-terrorism, data mining and privacy', Alta. L. Rev. 2006-43. B. W. Schermer, 'The limits of privacy in automated profiling and data mining', Computer Law & Security Review 2011-7. H. T. Tavani, 'Genomic research and data-mining technology: Implications for personal privacy and informed consent', Ethics and Information Technology 2004-6.

[81] L. A. Bygrave, 'Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling', Computer Law & Security Report, 2001-17. M. Hildebrandt, 'Who is Profiling Who? Invisible Visibility', p. 248, in: S. Gutwirth, Y. Poullet, P. de Hert, C. de Terwagne & S. Nouwt, 'Reinventing Data Protection?', Brussel, Springer 2009. M. Hildebrandt, 'The Dawn of a Critical Transparency Right for the Profiling Era', Digital Enlightenment Yearbook, 2012. C. Kuner, 'The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law', Privacy & Security Law Report 2 juni 2012, p. 6-7. Article 29 Data Protection Working, 'Opinion 01/2012 on the data protection reform proposals', 00530/12/EN, WP 191, 23 March 2012, Brussels, p. 19. See also: EDPS, Opinion of the European Data Protection Supervisor on the data protection reform package, Brussels, 7 March 2012.

sexual orientation or health conditions.[82] Thus, although some limitations remain, this right too has been extended in scope and the level of protection has been raised.

4. Enforcement

Initially, the data protection rules contained no or only marginal provisions on law enforcement. As has been stressed, the rules were primarily seen as principles of good governance for governments. Subsequently, the two Resolutions of the Council of Europe merely recommended states member to the CoE to adopt rules to protect the principles contained in the Resolutions. It was at their liberty to implement sanctions or rules regarding liability. Only in the Convention of 1981 was it explicitly provided that: 'Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.'[83] The explanatory report to the Convention stressed that this could either be done through civil, administrative or criminal sanctions.[84] Moreover, the Convention explicitly provided a number of rules regarding the application and enforcement of the rule on transborder data flows,[85] which was considered 'the most vague and elusive' of any of the data protection concerns.[86] It stimulated, among others, the cooperation between states and the national Data Protection Authorities to assist each other by providing full and detailed information of their laws and of data processing within their borders[87] and it specified that states and DPAs shall assist citizens living abroad, on the territory of another state.[88] Finally, the Convention installed a Consultative Committee,[89] which could advise the Committee of Ministers (CoM) on revising the Convention.[90]

Adopting a EU wide Directive aimed at bringing uniformity in the national legislations of the different countries,[91] to provide an equal level of protection,[92] but also to facilitate the transfer of personal data in Europe.[93] This uniformity is further promoted by providing further and more detailed rules for crossborder data processing.[94] For example, personal data may only be transferred to third countries if they have an adequate level of data protection, similar to that of the European Union.[95] As eluded to before, the Working Party was installed, consisting of the representatives of all national DPAs, which has a broad mandate to give opinions on almost every aspect of the Directive, on how it should be interpreted,

[82] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling.
[83] Article 10 Convention (1981).
[84] Article 11 Convention (1981).
[85] Article 12 Convention (1981).
[86] Organisation for Economic Co-operation and Development, 'Policy issues in data protection and privacy : concepts and perspectives: proceedings of the OECD seminar, 24th to 26th June 1974', Washington, D.C, OECD Publications Center, 1976, p. 197
[87] Article 13 Convention (1981).
[88] Article 14 Convention (1981).
[89] Article 18 Convention (1981).
[90] Article 19 and 21 Convention (1981).
[91] See among others: U. Dammann, O. Mallmann & S. Simitis, 'Data protection legislation: an international documentation', Frankfurt am Main, Metzner, 1977. B. Niblett, 'Data Protection Act 1984', Oyez Longman Publishing Limited, London, 1984.
[92] Article 1 Directive 95/46/EC.
[93] See for the tension between e-commerce and data protection among others: H.W.K. Kaspersen, 'Data Protection and e-commerce', in: A. R. Lodder & H. W. K., 'eDirectives: guide to European Union Law on E-Commerce', Kluwer Law International, The Hague, 2002.
[94] See further: R. Laperrière, 'Crossing the borders of privacy: transborder flows of personal data from Canada', Ottawa, Communications and Public Affairs, Department of Justice Canada, 1991.
[95] Article 25 Directive 95/46/EC.

implemented and amended, among others. The Directive also specifies that the Commission shall be assisted by a Committee composed of the representatives of the Member States when adopting measures pursuant to the Directive.[96]

Furthermore, the enforcement of the rules was further promoted by providing that each state should install an independent DPA,[97] which must be endowed with investigative powers, effective powers of intervention and the power to engage in legal proceedings.[98] The Directive further enlarges the role of these supervisory authorities by specifying that they shall hear claims lodged by any person and that they may carry out prior checks of data processing which is likely to present specific risks to the rights and freedoms of data subjects.[99] Finally, the Data Protection Directive lays down further and more specific rules by providing the right of every person to a judicial remedy for any breach of his rights, that any person who has suffered damage as a result of processing against the data protection rules is entitled to receive compensation from the controller for the damage suffered and that Member States shall lay down the sanctions in case of an infringement of the data protection rules.[100]

Under the Regulation, again, a quite radical shift seems at hand.[101] The most important change is that a Regulation, in contrast to a Directive, has direct effect and needs not to be implemented in the national legal frameworks of the different countries. Right now, countries have adopted a variety of different implementations and interpretation of the data protection rules in their national legislation, which means that a number of (American) companies choose the country with the least strict rules (i.e. Ireland) for their European headquarters.[102] The first evaluation of the Directive found an 'overly lax attitude in some Member States – in addition to being in contravention of the Directive – risks weakening protection in the EU as a whole, because with the free movement guaranteed by the Directive, data flows are likely to switch to the "least burdensome" point of export.'[103]

Consequently, besides extended rules for crossborder data processing,[104] among others to cope with new techniques such as cloud computing,[105] the Regulation grants DPAs more and wider powers[106] and introduces a so called 'one-stop shop' system. This entails that not only shall each supervisory authority exercise, on the territory of its own Member State, the powers conferred on it in accordance with the Regulation, but also that where the processing of personal data takes place in the context of the activities of an establishment of a controller

[96] Article 31 Directive 95/46/EC.
[97] See also: ECJ (Grand Chamber) European Commission, v Federal Republic of Germany, 9 March 2010, Case C-518/07. ECJ (Grand Chamber) European Commission v Republic of Austria, 16 October 2012, Case C-614/10.
[98] See further: ECJ (Grand Chamber), Volker und Markus Schecke GbR (C-92/09), Hartmut Eifert (C-93/09) v Land Hessen, 9 November 2010, Joined Cases C-92/09 and C-93/09.
[99] Article 20 Directive 95/46/EC.
[100] Article 22, 23 and 24 Directive 95/46/EC. See further: C. Kuner, 'European Data Protection Law: Corporate Compliance and regulation', Oxford University Press, New York, 2007.
[101] Article 29 Data Protection Working, 'Opinion 8/2010 on applicable law', 0836-02/10/EN, WP 179, 16 December 2010, Brussels.
[102] 3.2. Subsidiarity and proportionality, European Commission Proposal (2012).
[103] Commission of the European Communities, First report on the implementation of the Data Protection Directive (95/46/EC), COM(2003) 265 final, Brussels, 15 may 2003.
[104] Articles 40-45 European Commission Proposal (2012).
[105] European Commission, 'Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A comprehensive approach on personal data protection in the European Union', Brussels, 4.11.2010, COM(2010) 609 final, p. 5. See also: See the Study on the economic benefits of privacy enhancing technologies, London Economics, July 2010, (http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf), p. 14. Article 29 Data Protection Working, Opinion 05/2012 on Cloud Computing, 01037/12/EN, WP 196, Brussels, 1 July 2012.
[106] Articles 46-50 European Commission Proposal (2012).

or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States. Thus, not only is cooperation between DPAs encouraged, it is also ensured that there is one approach to the enforcement of the Regulation regarding a certain practice or towards a certain company across the European Union.[107]

The Working Party is replaced by a European Data Protection Board, which is granted wider powers,[108] and the Commission may adopt specific Regulations on a number of the provisions entailed in the Regulation, to provide further clarity and details on the interpretation of the rights and obligations therein contained.[109] Both elements ensure that a further and increased level of harmonization and an effective protection of the data protection rules is achieved. Finally, the fines and sanctions connected to the violation of the provisions in the Regulation have gone up dramatically. For example, the supervisory authority can, in certain circumstances, impose a fine up to 1.000.000 euro or, in case of an enterprise, up to 2% of its annual worldwide turnover, which for companies like Facebook and Google, would be a dramatically high figure.[110] Interestingly, the enforcement of the rules is no longer seen as the primary concern and duty of the DPAs, but increasingly as a right of the data subject to get redress and file a complaint or a law suit. Among others, a right to lodge a complaint with a supervisory authority is introduced,[111] a right to a judicial remedy against a supervisory authority,[112] a right to a judicial remedy against a controller or processor[113] and a right to compensation and liability, which was already partially contained in the Directive,[114] exist. These are all subjective rights of the data subject which may be directly invoked by the individual, given that the Regulation has direct effect.

Thus, the provisions on the enforcement of the data protection instruments have been extended quite considerably. This fits in the general trend towards an increased focus on the individual and his interest as the core of data protection rules, since the tightened rules on enforcement have the explicit aim of safeguarding the interests of the data subject. For example, recital 11 to the proposal for a General Data Protection Regulation stresses that: 'In order to ensure a consistent level of protection for individuals throughout the Union and to prevent divergences hampering the free movement of data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide individuals in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective co-operation by the supervisory authorities of different Member States.'[115]

Secondly, there is a sharp increase in the number of subjective rights on this specific point as well, namely to engage in legal proceedings, submit complaints and request (financial) compensation. Finally, the focus on the individual and his interests in terms of enforcement measures may also be witnessed from the structure of the Regulation's Article

[107] See further: E. M. L. Moerel, 'Binding corporate rules corporate self-regulation of global data transfers', Oxford, Oxford University Press, 2012.
[108] Articles 64-72 European Commission Proposal (2012).
[109] See also: Articles 86-87 European Commission Proposal (2012).
[110] Article 79 European Commission Proposal (2012).
[111] Article 73 European Commission Proposal (2012).
[112] Article 74 European Commission Proposal (2012).
[113] Article 75 European Commission Proposal (2012).
[114] Article 77 European Commission Proposal (2012).
[115] Recital 11 European Commission Proposal (2012).

79, regarding administrative sanctions.[116] It lays down three regimes: one in which the supervisory authority may impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, the second regards a fine up to 500 000 EUR or 1 % of the annual worldwide turnover, and the third a fine up to 1 000 000 EUR or 2 % of the annual worldwide turnover. The first is applied to instances in which the data controller has disrespected the principles on transparency, the second regards, among others, a violation of the individual's right to information, access to personal data, the right to rectification, the right to be forgotten and the right to data portability and the third applies, among others, to instances in which the principles on the processing of sensitive personal information have not been respected, the principles for consent have been violated or the personal data of a child have been processed without the agreement of the parent, the right to object and the right to protection against profiling have been violated, the accountability duty has been disrespected or personal data have been processed unlawfully. Although the precise explanation for this tripartite is unclear, it seems as though the guiding principle behind this differentiation is that the more a data subject's personal interests are or may be violated, the higher the sanctions may be.

5. Analysis

In conclusion, over time, the obligations for data processors under the various data protection regimes have significantly changed. One of the original pillars, the transparency principle, which maintains that the general public has to be informed, through a notification, about data processing, has been transformed into right of the individual data subject to be notified when a data leak has a potential detrimental effect on his personal interests and to a duty of the controller to have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights. The principles of fairness have been retained, although they have been elaborated and have partially been given direct effect by the ECJ. Finally, they will, if the Regulation is accepted and adopted as proposed by the Commission, be supplemented with a general accountability duty, which entails a number of specific and detailed obligations for data processors; these all have the purpose of providing the individual with adequate protection of his fundamental right to data protection and of protecting his personal interests.

Similarly, the data subject has gradually gained more and stronger rights. The first data protection documents contained merely a right to access files in which personal data were stored and to obtain information about who processed them and for what reasons. Some marginal rights to rectification were sometimes also accorded to the individual. The Data Protection Directive granted several additional individual rights, such as a right to rectification and objection and a right to object to automatic decision making, even though a number of thresholds were installed for invoking these rights. With the Regulation, not only have most of these thresholds been removed, new rights have been introduced which give the individual control over his personal data, such as the right to data portability and the right to be forgotten.

Third and finally, the data protection rules originally could be regarded best as principles of good governance. The documents contained very wide and general principles of transparency and fair data processing, which were seen as the obligation and responsibility of the data processor. They were not framed as rights of the individual and not even linked to the private interests of data subjects, but rather to the quality and fairness of the process as such. Gradually, however, data protection has shifted from duties of care for data processors to a

[116] Article 79 European Commission Proposal (2012).

fundamental right of the data subject, as acknowledged in the Charter of Fundamental Rights of the European Union.[117] Subsequently, the data protection rules are increasingly harmonized (from total discretion for states to total harmonization through a Regulation), the enforcement is harmonized (cooperation DPAs and one-stop shop system) and the interpretation and implementation of the rules are harmonized (EDPB and discretion of the Commission), crossborder data processing is regulated to a large extent and a minimum level of protection for third countries to which data are transferred is required. Moreover, the fines for violations of data protection principles have gone up dramatically and the data subject is granted more and individual rights to submit legal procedures regarding personal injury and compensation.

Consequently, the data protection rules have transformed significantly over time on a number of points. First, data protection is increasingly seen as an independent right, separated from the right to privacy. For example, the Resolution from (1974) explicitly held: 'Bearing in mind Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, Recommends the governments of member states: a. to take all steps which they consider necessary to give effect to the principles set out in the annex to the present resolution'.[118] The Convention (1981) explicitly stressed that its aim was to provide protection to the right to privacy in automatic data processes.[119] Article 1 of the Directive, mapping out the object of the document, holds: 'In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data'.[120] In contrast, the proposed Regulation holds: 'This Regulation protects the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data.'[121] While the Directive refers to the concept of privacy 13 times, it is mentioned only 4 times in the Regulation, even though the latter is considerably longer.

The leads to the second change, namely that data protection rules have become increasingly detailed. The two Resolutions from 1973 and 1974 contained 8 and 10 articles respectively. The Convention (1981) contained 27 provisions, the Directive 34 and the proposed Regulation 91. While the two Resolutions were literally one-pagers, the proposed Regulation consists of 60 pages of rules (83 if the recitals are included). This has had as consequence that the rules have become increasingly detailed and technology-specific. The right to data portability, for example, is specifically designed to break the dominance of Facebook; it aims at tackling a problem specific to the current technological environment. The right to be forgotten and the right against profiling too, have a highly technology-specific character, as for example, the first relates to how websites and search engines are designed in relation to erasing personal data or making them unretrievable. This has the advantage that those rules tackle very real and concrete problems individuals are currently facing. As downside, such rules may be problematic because the problems of today may not be the problems of tomorrow (keeping in mind that it will be well over 20 years before the Directive from 1995 will be replaced); moreover, technological dependent rules may be easily circumvented, among others by inventing new techniques which do not fit the definition or scope of an article.

Thirdly, the detailed and increasingly harmonized rules of the proposed Regulation bring with it that the right to data protection is the only human right across the European Union that is regulated in such detail on European level through a Regulation, which leaves

[117] This also creates a new legal basis for data protection rules within the EU. See also: <http://www.statewatch.org/analyses/no-176-leas-data%20protection.pdf>.
[118] Preamble of Resolution (1974).
[119] Article 1 Convention (1981).
[120] Article 1 Directive 95/46/EC.
[121] Article 1 European Commission Proposal (2012).

no room for Member States to interpret the rules according to their own traditions. The reason for this is that data protection has an particular international and transnational character, due to cloud computing and other modes of cross-border data transmission. Consequently, effective regulation needs a form of harmonization. However, this also restricts the margin of appreciation afforded to national parliaments. In analogy, it seems that regulating, for example, the freedom of expression or freedom of religion on European Union level through a Regulation would face serious resistance, as national governments would want to approach a and regulate these doctrines according to their own traditions and cultural standards. By adopting a Regulation for data protection rules, this possibility will be blocked, even though Anglo-Saxon countries traditionally have less strict rules on data processing, reflecting their business oriented approach, the southern European countries usually align data protection rules to the protection of individual's reputation and identity, the eastern European countries and Germany usually have quite strict data protection rules given the historic background of abuse of personal data by totalitarian regimes, etc.[122] By undermining the diversity in national approaches, the democratic legitimacy of the right to data protection may be undermined as well.

Finally, as recounted in the introduction of this article, the definition of personal data has been widened and broadened and has become less and less concerned with the physical (natural) person. Not only the identified person, but also the person who may be identified in the future through the use of reasonable means is now qualified as a data subject. Not only the directly identifiable individual, but also the indirectly identifiable person may be treated as a data subject. Likewise, a long, though non-exhaustive, list of possible identifying factors is included in the definition of the proposed Regulation, such as an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. This trend reflects the fact that data which at one moment in time may contain no information about a specific person whatsoever, may in the future be used, through advanced techniques, to identify or individualize a person. Moreover, even data that may not alone identify a person can increasingly be linked, among others through interconnecting and harvesting data bases, and be used to create profiles so that two or more non-identifying datasets may become identifying datasets.[123]

There have thus occurred some major changes in the data protection instruments. Most importantly, this study has tried to show that although concerns over Informational Self-Determination were not absent in the older data protection instruments, these instruments provided the individual and his interests only marginal protection. The trend toward Informational Self-Determination is of more recent origin and seems to be one of the basic philosophies behind the proposed Regulation. A move away from data protection as originally foreseen in the 1970s is of course not in itself a bad thing. It may be asked why the original framing of data protection should be retained; societies, technologies, and law and policy evolve over time, and it is not immediately obvious why the origins of data protection, dating from the 1970s, should as such have any normative thrust over forty years later. So the

[122] See among others: D. Campbell & J. Fisher (eds.), 'Data transmission and privacy', Dordrecht, Nijhoff, 1994. U. Dammann, O. Mallmann & S. Simitis (eds.), 'Data protection legislation: an international documentation: Engl.-German: eine internationale Dokumentation = Die Gesetzgebung zum Datenschutz', Frankfurt am Main, Metzner, 1977. H. Burkert, 'Freedom of information and data protection', Bonn, Gesellschaft für Mathematik und Datenverarbeitung, 1983. S. Nouwt, B. R. de Vries & P. Balboni (eds.), 'Reasonable expectations of privacy?: eleven country reports on camera surveillance and workplace privacy', The Hague, T.M.C. Asser Press, 2005.

[123] See also the new opinion by the Working Party 29: Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques', 0829/14/EN, WP216, 10 April 2014, Brussels.

question should be asked: should data protection rules focus on the individual and his interests and what could be the arguments for doing so?[124]

First, the trend towards an increased focus on the individual and his interests could be embedded in a wider perspective of policy development over the past decades.[125] It might be suggested that this is the result of a more general tendency towards individual rights over the years. More generally, the European Union has consistently promoted individual rights and consumer empowerment and has often regarded the individual as rational homo economicus, who is capable of pursuing and protecting his own interests if provided with clear information and sufficient tools.[126] In a similar vein, there is a strong general trend towards accountability since a decade or so, and the Regulation's focus on stronger enforcement and accountability fits well within that trend. It might be suggested that these developments are not specific to data protection instruments, but are part of a bigger development, of which the changes signaled in this study are merely an example. It is, however, beyond the scope of this study to assess whether the move away from general rights and duties and towards individual control is specific for the domain of data protection or not.[127]

Second, one of the reasons for an increased focus on the individual and his interests may be the so called 'banalisation' of data processing.[128] Data processing has generally moved from the public sector to the private sector and from large organizations to private individuals. General rules of fairness and accountability have historically played an important role in relation to governmental organizations, more so than with regard to private companies.[129] Moreover, a difference is that governments will usually have a fair and legitimate ground for data processing, while with regard to private companies and individuals, this will only be so if the data subject has consented or if the interests of the first outweigh those of the latter. A final difference is that citizens are mostly obliged to provide the government with the information requested, while this is usually not so with private individuals or companies. In the private sector, a right to control over personal data seems better fit.[130]

---

[124] The points have been taken from the following books, chapters and articles specifically: A. Roosendaal, 'Digital Personae and Profiles in Law: Protecting Individuals' Rights in Online Contexts', Oisterwijk, Wolf Legal Publishers, 2013. P. Schwartz, 'The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination', 37 the American Journal of Comparative Law. 675, 1989. G. Hornung & C. Schnabel, 'Data protection in Germany I: The population census decision and the right to informational self-determination', Computer Law & Security Review, Volume 25, Issue 1, 2009. S. Fisscher-Hübner, C. Hoofnagle, I. Krontiris, K. Rannenberg, M. Wiadner & C. Bowden, 'Online Privacy – Towards Informational Self-Determination on the Internet', in: M. Hildebrandt et al. (Eds.), 'Digital Enlightenment Yearbook 2013', IOS Press, 2013. E. J. Eberle, 'The Right To Information Self-Determination', 2001 Utah Law Review 965. C. Voigtmann, K. David, J. Zirfas, H. Skistims & A. Roßnagel, 'Prospects for Context Prediction Despite the Principle of Informational Self-Determination', Third International Conference on Advances in Human-Oriented and Personalized Mechanisms, Technologies and Services, 2010. A. Rouvroy & Y. Poullet, 'The right to informational self-determination and the value of self-development: reassessing the importance of privacy for democracy', in: S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwagne & S. Nouwt, 'Reinventing data protection?', Dordrecht, Springer, 2009. G. Marc Rehm, 'Just Judicial Activism? Privacy and Informational Self-Determination in U.S. and German Constitutional Law', <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=216348>.

[125] The author would like to thank Reviewer 1 for this point specifically, but more in generally for his/her very sharp questions and insightful suggestions.

[126] See in general: K. Mathis, 'Law and economics in Europe: foundations and applications', Dordrecht, Springer, 2014.

[127] <http://ec.europa.eu/consumers/index_en.htm>.

[128] Council of Europe report: New technologies: a challenge to privacy protection? (1989). <http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/NewTechnologies_1989_en.pdf>.

[129] See however also: Van Eijk et al., 'Moving Towards Balance: A study into duties of care on the Internet', <http://www.ivir.nl/publications/vaneijk/Moving_Towards_Balance.pdf>.

[130] See also on this topic: <http://www.scandinavianlaw.se/pdf/47-14.pdf>.

Third, proponents of Informational Self-Determination argue that granting data subjects individual rights provides for a system in which everyone may attain his own desired level of data protection. As need not be recounted, the value of privacy and data protection differs not only from century to century,[131] from culture to culture[132] and from situation to situation,[133] but also from person to person.[134] What may be regarded as a severe infringement upon his right to privacy or data protection by one person may be regarded as futile and unimportant by another. Some people do not mind putting their whole lives on Facebook and other online platforms, others are very protective and take recourse to encryption, tor-networks and the likes.[135] Granting a right to individuals to control their own data ensures that each person can attain the desired level of protection; in contrast, a focus on general duties for processors, which may be enforced through self-legislation or through a National Data Protection Authority, lays down one general level of protection for everybody, therewith over-protecting some and under-protecting others.[136]

Fourth, it is generally assumed that the current data protection regimes in Europe, most importantly the Directive, do not provide a sufficient level of data protection.[137] The rules are generally seen as to vague and abstract, not all DPAs are known for their decisive actions, and individuals often only have a limited awareness concerning possible violations of their right to data protection, the possible consequences of that and the tools at their disposal to address such issues.[138] Specifying specific and detailed rules, instead of general duties of care, harmonizing the rules and the enforcement of the data protection provisions, instead of leaving the enforcement to national authorities, and granting individuals subjective rights to take matters in their own hands, instead of leaving the issue of compliance to the discretion of DPAs, might help to tackle these problems. Consequently, it seems to be a very conscious choice to diverge from the old tradition of data protection, as the focus on general duties of care has not resulted in the desired level of data protection.[139]

Fifth and finally, there is a specific branch of Informational Self-Determination that argues not only for a right to control personal information, but also to vest a (intellectual) property right in personal data.[140] This would enable a person to trade his personal data with other parties or issue some sort of license. This would ensure that consent is not only one of the possible grounds for legitimate data processing, but that it would become the only possible

[131] P. Ariès & G. Duby, 'A history of private life', Cambridge, Belknap Press of Harvard University Press, 1987-..

[132] See for example: S. Van der Geest, 'Toilets, privacy and perceptions of dirt in Kwahu-Tafo'. In: S.van der Geest and N.Obirih-Opareh (eds), 'Toilets and Sanitation in Ghana: An urgent matter', Accra, Institute of Scientific and Technological Information(INSTI), CSIR , 2001.

[133] See also Nissenbaum who coins privacy as a contextual concept. H. Nissenbaum, 'Privacy in context: technology, policy, and the integrity of social life', Standord University Press, Standford, 2010.

[134] D. J. Solove, 'Understanding privacy', Cambridge, Harvard University Press, 2008.

[135] See also: J. P. Mifsud Bonnici, 'Self-regulation in cyberspace', The Hague, T.M.C. Asser Press, 2008.

[136] One of the common critiques of American privacy and data protection specialists is that the European legal framework is overprotective. See among others: A. Bartow, 'Our Data, Ourselves: Privacy, Propertization, and Gender', University of San Francisco Law Review, 34 2000.
Available at: http://works.bepress.com/ann_bartow/35

[137] See among others: D. Korff (consultant to the European Commission), 'EC study on Implementation of Data Protection Directive (Study Contract ETD/2001/B5-3001/A/49) comparative summary of national laws', Human Rights Centre, University of Essex, Colchester (UK), Cambridge (UK), September 2002.

[138] Commission of the European Communities, First report on the implementation of the Data Protection Directive (95/46/EC), COM(2003) 265 final, Brussels, 15 may 2003.

[139] See more in general also: European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe', Brussels, 19.5.2010, COM(2010)245 final.

[140] N. Purtova, 'Property rights in personal data: a European perspective', Alphen aan den Rijn, Kluwer Law International, 2012.

ground.[141] Moreover, such right would ensure that individuals could ask a return for their personal data, possibly even money. One of the arguments the defenders of such a model put forward is that this reflects quite accurately what is already happening in the current internet environment, in which internet services are offered for free in return for personal data. The business model of many internet companies is based on using personal data to create profiles and distribute personalized advertisements.[142] Secondly, it is often said to be unfair that businesses such as Google and Facebook make high profits using the personal data of individuals, while those individuals 'only' get a free service in return.[143] Providing individuals with a property right gives them the opportunity to share in the profit made.

Although it is impossible to provide an exhaustive list of arguments in favour of Informational Self-Determination, these points seem to figure most prominently in the scholarly literature. It goes too far to discuss all possible benefits and pitfalls of Informational Self-Determination, but given the fact that the ISD movement is increasingly prominent and that it appears to be one of the basic philosophies behind the proposed Regulation, some questions and counter-arguments should be answered and addressed before embracing this new approach in data protection. Some of those questions are well-known and have been put forward for many years, others are of more recent origin and are directly linked to current developments, such as that of Big Data.

As has been emphasized earlier, the data protection rules and Fair Information Principles were developed against the background of the up rise of large data bases which raised a number of problems for the traditional conception of the right to privacy, which is aimed at protecting the private interests of the citizen, among others, by giving him a right to control over private and sensitive data. First, data processing often does not regard private or sensitive data, but public and non-sensitive data and second, the right to control information by the data subject was felt neither legitimated by his private interests nor feasible. Although the first of these two elements has been retained and even further broadened, the second principle is not. The question is how these two developments are to be reconciled, as they seem fundamentally at odds. The definition of personal data has been increasingly disconnected from the physical person, while the substantial rules have increasingly focussed on the individual and his interests, among others by granting him a right to control over his personal data.

Moreover, the question may be posed what the legitimisation for granting such a right to control is. With private data or privacy sensitive data, directly identifying a person and revealing a specific and sensitive aspect of his life, for example related to a disease or sexual orientation, a right to control such information does not seem unreasonable. However, by broadening the concept of personal data, the subjective element is lost and the question arises why an individual should have a right to control data (or have influence over the processing) which alone do not identify him (e.g. the person living in neighbourhood x with the blue car), but might, if combined with other data (and has a red bicycle),[144] which do not identify him, but might do so in the future (through the use of advanced (re-identification) techniques),[145] or which do not identify him personally, but only as part of a larger group (people with red

[141] See further: P. Schwartz, 'Property, Privacy, and Personal Data', Harvard Law Review, 2004, Vol. 117, No. 7.
[142] See further: J. Kang, 'Information Privacy in Cyberspace Transactions', Stanford Law Review, 1998, Vol. 50, No. 4.
[143] See further: P. Samuelson, 'Privacy As Intellectual Property?', Stanford Law Review, 2000, Vol. 52, No. 5.
[144] See among others: J. Han, M. Kamber & Jian Pei, 'Data mining: concepts and techniques', Amsterdam, Boston, Elsevier/Morgan Kaufmann, 2012. F. Giannotti & D. Pedreschi (eds.), 'Mobility, Data Mining and Privacy: Geographic Knowledge Discovery', Springer-Verlag, Berlin Heidelberg, 2008.
[145] S. Claus, D. Kesdogan & T. Kölsch, 'Privacy enhancint identity management: protection against re-identification and profiling', DIM '05 Proceedings of the 2005 workshop on Digital identity management.

bicycles have a 70% change of being interested in cereal products).[146] Consequently, it is uncertain what the ratio is behind an individual control-right over non-private and non-privacy sensitive data, group profiles and statistical correlations.[147]

Secondly, it is questionable how feasible such a right to control really is. (1) Aggregated data and group profiles are used to identify and individualize a large number of people. It seems undoable to give all of them a right to control the data, not in the last place because their respective desires concerning one profile may differ.[148] (2) Even non-aggregated personal data contains information about friends and relatives. If a child has a hereditary disease, this says something about his parents, if a man posts on Facebook a picture of his new luxurious mansion, it usually also tells something about the living conditions of wife, or if a person posts a picture of him in a bar online, his friends may be identified and seen with a glass of beer in their hands.[149] (3) Specific to information is precisely that it cannot be privatised. That a person is a man, has an expensive care, has a disease (e.g. is paralyzed), etc., might simply be witnessed by everyone.[150] Giving a right to control non-private information seems difficult for this reason. (4) Specific to information, even if it is private, is precisely that it is difficult to control. If a person knows that his neighbour is cheating on his wife and tells his friends, he has the information and his friends do too. They may tell it to others and so the control over this datum is lost. In the digital environment, of course, control over information seems even more unpractical.[151]

Thirdly, it is questionable whether this approach tackles the problems that citizens and consumers are currently facing.[152] In Big Data processes, companies and governments gather large amounts of personal data by means of cameras, telephone taps, GPS-systems, cookies and internet monitoring, which are stored in large databases and analyzed by computer algorithms.[153] These data are then aggregated, used to create group profiles and analyzed on the basis of statistical relationships and mathematical patterns. The essential characteristic of this process is thus that the individual is not central to the process. Data collection and processing do not start after a particular ground or reason has arisen, but the value and use of the information will only become apparent at a later stage. In these processes, no reasonable suspicion is needed to individualize someone. Even a 1% chance that someone will buy an expensive luxury product or will engage in terrorist activities may provide sufficient ground to do so. The point here is not that this or that specific person has been subjected to data processing, but rather that everyone is or might be.

---

[146] B. H. M. Custers, 'The power of knowledge : ethical, legal, and technological aspects of data mining and group profiling in epidemiology', Nijmegen, Wolf Legal Publishers (WLP), 2004.

[147] See for an insightful discussion on the ratio behind property/ownership: S. Gompel, 'Formalities in copyright law: an analysis of their history, rationales and possible future', Alphen aan den Rijn, Kluwer Law International, 2011.

[148] The problem here is that the group is created by the profiling and did not exist prior to it (such as with indigenous people). Therefore, group rights seem difficult to implement. See further: A. R. Riley, 'Recovering Collectivity: Group Rights to Intellectual Property in Indegenous Communities', 18 Cardozo Arts & Entertainment Law Journal 175, 2000.

[149] This is sometimes also called the network effect of personal data. See also: <https://www.econstor.eu/dspace/bitstream/10419/18430/1/dp698.pdf>.

[150] See also: T. A. Lipinski & J. Britz, 'Rethinking the ownership of information in the 21st century: Ethical implications', Ethics and Information Technology, 2000, Volume 2, Issue 1.

[151] D. L. Stone, 'Relationship between introversion/extraversion, values regarding control over information, and perceptions of invasion of privacy', Perceptual and Motor Skills, Volume 62, 1986.

[152] See also: 'B. van der Sloot, Privacy in the Post-NSA Era: Time for a Fundamental Revision?, JIPITEC, 2014-1.

[153] V. Mayer-Schonberger & K. Cukier, "Big data: A revolution that will transform how we live, work, and think", Boston, Houghton Mifflin Harcourt, 2013.

The question with Big Data processes, of which the NSA affair might be an example, seems simply whether such large data sets regarding so many people and collected over such a large time span is at all necessary and proportionate to the goal pursued (in this case the public safety), even apart from any individual interest, and whether there are no less intrusive means at the disposal of the processor to achieve this aim. In addition, it might be asked how effective such data processing systems really are. For example: 'Some agency insiders now believe that NSA is only able to report on about 1 percent of the data that it collects, and it is getting harder every day to find within this 1 percent meaningful intelligence. Senior Defense and State Department officials refer to this problem as the "gold to garbage ration," which holds that it is becoming increasingly difficult and more expensive for NSA to find nuggets of useful intelligence in the ever-growing pile of garbage that it has to plow through.'[154] Consequently, it seems that it is not the individual and his interests that are central to those systems; the issue Big Data systems raise seems a more structural and fundamental one, connected to the interests of society as a whole.[155] It is therefore questionable whether the focus on the individual, his interests and his right to control personal data are fitting in this technological environment.

Finally, it is questionable whether the right to control would provide the citizen with any protection in a realistic sense. If an individual has a right to file a law suit and start a legal procedure to protect his personal interests, not only remains the requirement for an individual to demonstrate his personal interest (e.g. what personal damage have the NSA-practices caused to the ordinary citizen?), which is rather difficult in such large data systems, there also is a practical threshold for citizens who do not know whether they have been targeted by a particular data processing practice (even a request to beget such information will usually only be done if a data subject has reason to believe that this is so, while in the current technological environment, persons remain mostly unaware of data processing regarding them). Even if this knowledge would exists and even if personal damage could be convincingly demonstrated, it is still questionable of which practical use such an individual right of complaint is. In a world were not only secret services and governmental organizations, but also large companies like Google and Facebook and even ordinary citizens, assisted by their smart-phones, can gather and process large amounts of personal data, it is likely that it will simply become undoable for a person to keep track of everyone who is in possession of his personal data, to assess whether they use that data legitimately and if there is reason to believe this is not so, to seek justice trough a legal procedure.

Consequently, it might be worthwhile considering whether, if the subjective element in the definition of personal data is moved to the background, the substantive provisions should also be primarily aimed at safeguarding the fairness and reasonableness of the data processing as such. In short, it might be argued that originally, data protection concerned primarily a societal, and not an individual, interest. This seems again a very valid concern with regard to the trend of Big Data. With such structural and societal tendencies, it seems that the individual is as powerless as king Canute trying to turn the tide. Consequently, it might be questioned whether the trend of giving controllers more obligations to protect the interests of the data subject, giving individuals broader rights to control their data and giving them more tools for protecting their own interests through legal means is either effective, feasible, topical or even legitimate. It seems that now more than ever, emphasis should be placed on the general obligation of the controller to process personal data fairly, reasonably and carefully.

[154] M. M. Aid, 'The secret sentry: the untold history of the National Security Agency', New York, Bloomsbury Press, 2009, p. 304.

[155] See further: L. Floridi, 'The philosophy of information', Oxford, Oxford University Press, 2011. L. Floridi (ed.), 'The Blackwell guide to the philosophy of computing and information', Malden, Blackwell Publ, 2004.

In this sense, it could be left to the DPA or a general consumer organization to enforce the general duties of care for the data processors. An advantage may be that they would not have to specify any individual interest in a legal process, which is normally required, but would file a case in the general interest. It would not be necessary to demonstrate any personal damage, so that claims could be submitted *a priori* and in an early stage, so as to prevent any damage instead of remedying it. Moreover, general rules of fairness have the advantage over specific and technological dependent rules of never becoming outdated, as data, however collected, processed and distributed, must always be correct and kept up to data, necessary and proportional to the purpose of the processing, processed safely and confidentially, etc.

This is not to say that any right to control should be rejected. As recounted earlier, there are valid reasons to give individuals such a right. At the same time, alternatives should be considered and some realistic questions and problems remain with regard to Informational Self-Determination, which should be addressed before embracing the new trend as championed by the proposed Regulation. At least, the questions posed here deserve further discussion. (1) Why should the individual have a right to control personal information and what would be the legitimation for this? (2) How could such a model of control be practically effected and applied to information? (3) Is such a model feasible given the developments of Big Data and group profiling? (4) Would it provide the individual with any protection in a realistic sense? If a radical break with the historic data protection tradition is forged with the new Regulation, better thought should be given about what legitimizes this break, whether it would provide for a higher level of protection and whether a focus on general duties of care on the one hand and on individual rights to control personal data on the other hand can coexist within one framework, so that they might strengthen each other, or whether these systems have principally different foundations, which would come into conflict with each other when embedded in one data protection instrument.

Questions regarding control rights over person data, contrasted with a model which emphasizes general obligations and duties of care for data controllers:

	Control rights for data subjects	**General obligations data controller**
Legitimate	Questionable as it is uncertain why a person should own or control non-private and non-sensitive data	Seems to be in line with the widened scope of the definition of 'personal data'
Feasible	Questionable as information cannot be privatized or controlled and often regards a group or concerns relatives and friends	Seems to have the advantage of not becoming outdated or outpaced by technological developments
Future-oriented	Questionable as Big Data precisely does not regard the individual and his private interests	Seems to strike at the core of Big Data processes and the question of whether they are necessary, proportionate and effective
Effective	Questionable as it seems undoable for an individual to know which data are processed, by whom, whether this is done fairly and if not, to engage in a legal dispute	Seems more reasonable to require of a DPA or a general consumer organization to safeguard the data protection rules than of an individual to protect his own interests