The legal framework for access to data from a data protection viewpoint – especially under the GDPR

Indra Spiecker genannt Döhmann[*]

A. Introduction to data protection's regulatory impulse

I. Free data for all?

Access to data and information[1] can be paraphrased with a common saying: 'My data is freely available for anyone to access and use, I do not have anything to hide'. This may be true, but it is certainly wrong. Data access cannot be discussed without focusing on the reasons why completely free access to data is not only impossible but also not desirable.

Since their beginnings in the 1960s and 1970s, with the rise of automated decision-making, efforts to protect data and privacy have tried to act on this common misunderstanding of the equality of factual access to data and the normative 'nothing to hide'.[2] This is because the risk that data protection is intended to prevent is easily undervalued.

---

* I would like to thank members of my staff Mona Winau for further research and Charlotte Humpert for additional information and thorough reading. All references were last checked on 7 August 2020.

1 The terms *data* and *information* are treated synonymously for the purposes of this paper although the author is well aware that there is a substantial difference both between them and to the concept of knowledge. This, however, does not play out for the content of this paper.

2 Spiros Simitis, Gerrit Hornung and Indra Spiecker gen. Döhmann, in Spiros Simitis, Gerrit Hornung and Indra Spiecker gen. Döhmann (eds), *Datenschutzrecht. DSGVO mit BDSG* (Nomos 2019) Einleitung paras 6–13; cf. Alan F. Westin, *Privacy and Freedom* (Atheneum Press1967) 158–168; Jürgen Kühling and Johannes Raab, in Jürgen Kühling and Benedikt Buchner (eds), *Datenschutzgrundverordnung Kommentar* (C.H. Beck 2017) Einführung para. 37; Spiros Simitis, 'Reviewing Privacy in an Information Society' (1987) 135 University of Pennsylvania Law Review 707, 709–710; Alan F. Westin, 'Science, Privacy, and Freedom: Issues and Proposals for the 1970's: Part I-The Current Impact of Surveillance on Privacy' (1966) 66 Columbia Law Review 1003, 1003. Similar to the dictum 'nothing to hide' is the misunderstanding that 'nobody is going to bother'; Jessica Litman, 'Information Privacy/Information Property' (2000) 52 Stanford Law Review 1283, 1285.

The above assessment is based on two assumptions which contradict this seemingly convincing finding: First, freely available information does not mean equal use of the information. Not everyone who has access to data can also use it. So it is the availability of technology that determines the potential threats. Secondly, there are effects of the use of data that the individual does not control: If an individual's data is being used to assess others, then the effect on these others is not something included in the individual's decision to grant access. There is no direct interaction between the person whose data is being used and the entity using the data, and there is certainly no direct return between the use of data and the making accessible of it.

Data protection law is a core regulatory answer to data protection needs. It addresses at its centre the information-based power asymmetry which derives from the inequality of use and accessibility.[3] However, it naturally does not include all types of data. Rather, data protection law concentrates on personal data, where the risk of imbalanced decisions is most prominent, where the rationality of self-protection cannot necessarily be relied upon and where the consequences for the well-being of society are most pressing.

II. Data protection as a regulatory regime to link data and decision-making

The following insights into data access under the current EU legal regime of the General Data Protection Regulation (GDPR)[4] concentrate on these types of data. It should be noted, however, that there are many other data-

3 Cf. Walter Schmidt, 'Die bedrohte Entscheidungsfreiheit' (1974) 29 Juristen-Zeitung 241, 246; Lorna Stefanik, *Controlling Knowledge – Freedom of Information and Privacy Protection in a Networked World* (Athabaska University Press 2011), 29; Orla Lynskey, 'Deconstructing data protection: the "added-value" of a right to data protection in the EU legal order' (2014) 63 International & Comparative Law Quaterly 569, 589–590; See especially on privacy rights of defence against the state, Serge Gutwirth and Paul De Hert, 'Privacy, Data Protection and Law Enforcement: Opactiy of the Individual and Transparency of Power' in Eric Claes and others (eds), *Privacy and the Criminal Law* (Intersentia 2006) 61, 72–74; Herbert Burkert, *Informationszugang und Datenschutz. Ein kanadisches Beispiel* (Nomos 1992) 12. For an overview of the scientific discourse in Germany at the beginning of data protection law, see Klaus Tiedemann and Christoph Sasse, *Delinquenzprophylaxe, Kreditsicherung und Datenschutz in der Wirtschaft* (Carl Heymanns Verlag 1973) 89–100.

4 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of

protecting regimes present, such as the frequently discussed copyright law, which is also covered in this volume, but also, much less focused on, the protection of business and trade secrets or whistleblower protection, which are also present in this volume.

Data protection is one important way to look at guidance for an overall legal regime for access of data. The concept is based on the particular perspective on decision-making and the role information plays in it. According to this perspective, including the present difficulties in establishing an information and knowledge society[5] as well as the manifold perspectives and consequences of legal intervention, data protection scholars are capable to deliver their own and integrating answers on pressing questions on access of data. Though the full range of problems cannot be covered here, questions that remain unsettled include: whether data can be the object of services for the public (*Daseinsvorsorge*) and social participation, how concepts of transparency versus secrecy can be evaluated and established, what the consequences of ubiquitous computing and prolific availability of information are on society and numerous levels of decision, how the value, worth and accounting of information can be construed and legally implemented, whether solidarity concepts require a sharing of data, especially in health care provision, how horizontal and vertical integration of data and information technology can be guided, or who shall, in an international data transfer market, have the power to control data.

Most of the many approaches to solving these questions do not take into account that access to data and access to the infrastructure to use and exploit this data are separate from each other. Data protection law, however, offers solutions combining both venues because it is interested not only in the information part but also in the results and purposes of the use of data. Article 5 (1) lit. b GDPR, with the purpose limitation, makes that clear, as does Article 20 GDPR, with the limitation of automated decision-making. In the end, data protection law offers some concepts on how to deal with the new central resource of data as the 'new oil', and how it can be used for the public and private good without overburdening the individual. The core element of data protection, however, that self-restriction and a moderate use of data may be the way towards a sustainable, democracy-and-free-

---

personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2018] OJ L127/2.

5 The term 'knowledge society' was coined by Helmut Wilke, *Systemisches Wissensmanagement* (2nd edn, Lucius & Lucius 2001) 289.

dom-driven society and economy, usually encounters a lot of opposition and misconception.

III. The lack of control

The GDPR sees data as an important resource and an influencing factor for decision-making. In this decision-oriented framework, data processing has an impact both on the individual itself and on all groups of individuals within society which are being judged on the basis of information. Typically, the most severely infringing types of data processing such as profiling or scoring are achieved by transforming sets of individual data into generalised information that is then re-applied to individuals by decision-making. Therefore, power over information (and the technology to make use of it) may cause structural disparity and imbalance between those who are decided upon and those who decide with the aid of information and information technology.

The latter are typically unable to control for the data reflected within the decision, which strengthens the position of those using the information to use all accessible information without normative barriers.[6] Thus, a decision may seem to be in accordance with accepted values but really is not. Control over the substantive standards of a decision is therefore difficult, and control over the information input even more so. Thus a number of GDPR provisions are intended to establish control and normative standards for the use of data, among them the requirement to use data primarily directly gathered from the individual.

The GDPR also addresses the additional problem that maintaining control over the decision is typically difficult because individuals do not have the resources to control the technological means of using and assessing information.[7] If artificial intelligence is used to reach an administrative deci-

---

6 Indra Spiecker gen. Döhmann, 'Profiling, Big Data, Artificial Intelligence und Social Media – Gefahren für eine Gesellschaft ohne effektiven Datenschutz' in Walter Hötzendörfer, Christof Tschohl and Franz Kummer (eds), *International Trends in Legal Informatics: Festschrift für Erich Schweighöfer* (bpa media 2020) 345, 351–355.

7 Sebastian Bretthauer, 'Verfassungsrechtliche Grundlagen, Europäisches und nationales Recht' in Louisa Specht and Reto Mantz (eds), *Handbuch Europäisches und deutsches Datenschutzrecht* (C.H. Beck 2019) § 2 para. 2; Specifically on Art. 22 GDPR see Philip Scholz, in Spiros Simitis, Gerrit Hornung and Indra Spiecker gen. Döhmann (eds), *Datenschutzrecht. DSGVO mit BDSG* (Nomos 2019) Art. 22 para. 3. Isak Mendoza and Lee A. Bygrave, 'The Right Not to Be Subject to Automated Decisions Based on Profiling' (University of Oslo Faculty of Law Stud-

sion, hardly any citizen will be able to attack this decision based on a critique of the functioning of the technology applied. Thus, means like the data protection impact assessment procedure of Article 35 GDPR attempt to limit the harm of uncontrolled use of potentially infringing technology.

IV. The general answer of the GDPR regulatory regime

European data protection law offers a number of tools by which to assist the data subject in controlling data flows and intransparent decision-making. Without going into detail and with an eye on the special perspective of this contribution to a data access regime, there should be a few core elements named for a common understanding when looking at exact regulations on the access to data.

First, the GDPR intervenes as early and as long as possible and thus accompanies every aspect of data use. It does so by using a well-known technology-law instrument, the establishment of the principle of precaution (*Vorsorgeprinzip*), thus reversing the burden of reasoning and potentially proof in general: The data controller in many instances has to establish the use and the exact purposes of the data use rather than the data subject having to demonstrate risks and dangers.

The control of the data protection legal regime begins as early as possible and that is the moment when personal data leaves the sphere of the data subject's immediate and sole control. This can be as early as the emergence of data if this takes place in a social setting with others; it can also be at a much later stage e.g. when entries made in a diary on a computer years ago are exploited in the course of an administrative assessment of potential foster parents. On the other side, in the life cycle of data,[8] the GDPR also controls for the decision and its outcome and in many instances takes the potential consequences of the use of data into account when assessing the lawfulness of an act of or a type of data processing.

---

ies, Research Paper Series No. 2017–20) 7–8 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2964855> accessed 22 July 2020.

8 Cf. Indra Spiecker gen. Döhmann, 'Information Management' in Peter Cane and others (eds), *The Oxford Handbook on Comparative Administrative Law* (2020, forthcoming).

Secondly, the GDPR – and in this, it differs greatly from its predecessor, the Data Protection Directive (DPD)[9] – does not only rely on substantive safeguards but establishes effective means of control and sanctions and institutionalises them.[10] This can be seen in the clarified and increased tasks and powers of the supervisory authorities, Articles 56 and 57 GDPR, but also in the extensive set of sanctions now established under Articles 77 et seq. GDPR or the possibility of representation of data subjects under Article 80 GDPR. It also increases the pressure on data controllers by sharpening and furthering procedural safeguards such as a mandatory internal data protection impact assessment for infringing or risky data processing according to Article 35 GDPR, the duty to demonstrate according to Article 24 (1) GDPR or the duty to inform the data subject according to Articles 13 and 14 GDPR.[11]

---

9 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 [1995] OJ L281/31.

10 Jürgen Kühling and Mario Martini, 'Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?' (2016) 27 Europäische Zeitschrift für Wirtschaftsrecht 448, 451–454; Benedikt Buchner, 'Grundsätze des Datenschutzrechts, Datenschutzkontrolle' in Marie-Theres Tinnefeld and others (eds), *Einführung in das Datenschutzrecht, Datenschutz und Informationsfreiheit in europäischer Sicht* (7th edn, De Gruyter 2020) 314–332; Quite positively forecasting an effective and consistent authority, Jan P. Albrecht, 'How the GDPR Will Change the World' (2016) 2 European Data Protection Law Review 287, 289; opposing to Albrecht's viewpoint, Sebastian J. Golla, 'Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR' (2017) 8 Journal of Intellectual Property, Information Technology and E-Commerce Law 70, 77–78.

11 For an overview, see Peter Schantz, 'Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht?' (2016) 26 Neue Juristische Wochenschrift 1841, 1846–1847. On the data protection authority's extended responsibilities and powers, Alexander Roßnagel, *Datenschutzaufsicht nach der EU-Datenschutz-Grundverordnung* (Springer 2017); and the Europeanisation of supervisory authority, Hielke Hijmans, 'The DPAs and Their Cooperation: How Far Are We in Making Enforcement of Data Protection Law More European?' (2016) 2 European Data Protection Law Review 362. With regard to sanctions, Golla (n. 10) 74–78. Concerning the implications for foreign companies and states, Cedric Ryngaert and Mistale Taylor, 'The GDPR as Global Data Protection Regulation?' (2020) 114 American Journal of International Law Unbound 5, 7. Pointing out the advantage of willingness to cooperate from an entrepreneur's viewpoint, Michael Wenzel and Tim Wybitul, 'Vermeidung hoher Bußgelder und Kooperation mit Datenschutzbehörden' (2019) Zeitschrift für Datenschutz 290; on the increasing pressure on data processors in business, Tal Z. Zarsky, 'Incompati-

On this general understanding of what data protection law aims to achieve, this paper will first develop some core elements of data protection law without which the concept of access to data under the GDPR as the legal regime of data protection in Europe cannot be understood properly (B.). It will then point out the special qualities of data and information that do not allow for regulatory frameworks typically used for market goods and how data protection law implicitly takes these into account (C.). With this general understanding, the different rights to access to data under the GDPR (and partly national law) and their limits will be analysed (D.). Guidelines for a data-protection-compatible regulatory regime are directed towards an impact of these findings to legislators (E.) before the chapter closes with a conclusion and an outlook (F.).

B. Prerequisites on Access under Data Protection Law

I. Personal Data as the Threshold for Application of Data Protection Regimes

As personal data is the core element to open up the wide regulatory regime of data protection law, it is essential to understand what falls under this terminology and what does not. A data-protection-friendly regulatory regime of data access has to accept that a mixture of personal data and non-personal data will lead to the application of the stricter data protection regime. Thus, whenever there are some personal data elements within a pool of data, any access to this pool in general has to follow the rules of the GDPR.[12]

Article 4 (1) GDPR provides for a legal definition of 'any information relating to an identified or identifiable natural person', clarifying that the critical characteristic of identifiability is constituted if a person can directly or indirectly be identified. Thus, additional knowledge and information that needs to be accessed in order to identify a person has to be taken into account in order to determine whether there is in particular a 'reference […] such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural per-

---

ble: The GDPR in the Age of Big Data' (2017) 47 Seton Hall Law Review 995, 1005.

12 Cf. Case C-131/12 *Google Spain v AEPD and Mario Costeja González* [2014] ECLI:EU:C:2014:317.

son'. This legal definition makes it clear that the GDPR follows in the footsteps of the Data Protection Directive,[13] creating in general a large scope of applicability of data protection law as additional information has to be taken into account when determining whether data is personal data or not. In other words: Even if data does not immediately refer to an individual, it can still fall under the regime of the GDPR if additional data allows for a connection.

What remains unclear, however, is how much additional information has to be taken into account and whether or not this additional information must be accessible by the data controller. This ongoing feud over whether to take a more objective or more subjective approach[14] has been in parts decided by the ECJ in the *Breyer* case.[15] There, the ECJ ruled that dynamic IP addresses are typically considered to be personal data unless the identification is prohibited by law or access to the combination of data is only possible if totally disproportionate measures have to be taken. This could be redefined as an objective perspective with subjective elements/restrictions: In general all additional information which can legally and

13 There is no difference between the wording of Art. 4 (1) GDPR and Art. 2 lit. a) DPD in the English version. The altered wording in the German version from 'bestimmt/bestimmbar' to 'identifiziert/identifizierbar' does not have any practical implications; Moritz Karg, in Spiros Simitis, Gerrit Hornung and Indra Spiecker gen. Döhmann (eds), *Datenschutzrecht. DSGVO mit BDSG* (Nomos 2019) Art. 4 No. 1 para. 6; Stefan Ernst, in Boris P. Paal and Daniel A. Pauly (eds), *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz* (2nd edn, Beck 2018) Art. 4 No. 1 para. 3; Tina Krügel, 'Das personenbezogene Datum nach der DSGVO' (2017) Zeitschrift für Datenschutz 455, 455–456.

14 Karg (n. 13) Art. 4 No. 1 paras 58–59; supporting the subjective approach, Mark J. Taylor, 'Data Protection: Too Personal to Protect' (2006) 3 SCRIPTed (Journal) 71, 79–80; Worku G. Urgessa, 'The Protective Capacity of the Criterion of Identifiability under EU Data Protection Law' (2016) 2 European Data Protection Law Review Journal 521, 522; concerning the subjective approach in The UK Data Protection Act 1998, Taylor (ibid) 79; about the former version of the German Federal Data Protection Act (BDSG), Paul Voigt, 'Datenschutz bei Google' (2009) Multimedia und Recht 377, 379.

15 Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] ECLI:EU:C:2016:779.
Frederik Zuiderveen Borgesius, 'The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition' (2017) 3 European Data Protection Law Review Journal 130, 131, 137. With regard to assignability of the *Breyer* jurisprudence to Art. 4 (1) GDPR, Jens Brauneck, 'DSGVO: Neue Anwendbarkeit durch neue Definition personenbezogener Daten?' (2019) 30 Europäische Zeitschrift für Wirtschaftsrecht 680, 682–688; Krügel (n. 13) 455–456.

not totally against all proportionality be accessed has to be taken into account, and this includes information which the data controller might not actually retrieve. This leaves a wide range of application of the GDPR to many sets of data, although at first sight they might not seem to be personal data. This should be considered when developing a regime for wide data access: Much data processing is thus restricted by the GDPR.

II. Lawfulness of Data Processing and Procedural Requirements in combination

One of the core elements of data protection law is that any type of data processing has to be justified.[16] Article 6 (1) GDPR (and Article 9 GDPR for data with a high potential of discrimination, e.g. health data, racial or political data) provides for legal grounds, among them consent of the data subject but also overriding public interests. Nevertheless, despite wide possibilities for data processing of personal data, the GDPR also provides for a number of additional requirements and restrictions of these data processings. One could describe this process as a continuous pendulum: Requiring justification lets the pendulum swing in one direction, allowing wide justifications then lets it sway in the other direction, the procedural safeguards send it back again, and the possibilities for loosening these safeguards allow it to turn in the other direction, once more.

16 Jan P. Albrecht, in Spiros Simitis, Gerrit Hornung and Indra Spiecker gen. Döhmann (eds), *Datenschutzrecht. DSGVO mit BDSG* (Nomos 2019) Art. 6 para. 1; Eike M. Frenzel, in Boris P. Paal and Daniel A. Pauly (eds), *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz* (2nd edn, C.H. Beck 2018) Art. 6 para. 1; Benedikt Buchner and Thomas Petri, in Jürgen Kühling and Benedikt Buchner (eds), *Datenschutzgrundverordnung Kommentar* (C.H. Beck 2017) Art. 6 para. 1. In this respect, data protection law takes an exceptional position compared to other information obtained regulatory approaches, Spiecker gen. Döhmann (n. 8) sec. 33.6.1. Alexander Roßnagel speaks out against the frequently used term 'ban with an exemption option' in this context: Alexander Roßnagel, 'Kein "Verbotsprinzip" und kein "Verbot mit Erlaubnisvorbehalt" im Datenschutzrecht' (2019) Neue Juristische Wochenschrift 1. About the intrusive character of data processing, see Herke Kranenborg, 'Article 8 – Protection of Personal Data' in Steve Peers and others (eds), *The EU Charter on Fundamental Rights. A Commentary* (Hart Publishing 2014) Nos 08., 08.88 – 08.90; cf. Case C-131/12 *Google Spain v AEPD and Mario Costeja González* [2014] ECLI:EU:C:2014:317, para. 86.

III. Data Protection for both private and public data processing

Considering the broadness of the application of the GDPR and thus the general standards of data protection, the GDPR creates an extensive framework which regulates in an intensive way the processing of data. However, it should be seen that the GDPR differentiates in many regards – in contrast to the previous DPD – between private and public use of data.[17]

The regulation recognises that there are different interests involved. While private data processing is an expression of the freedom and liberties of the individual and thus might happen arbitrarily and completely in the own interest of both the data subject and the data controller, public (state) processing of data is in general bound by the common good and by the duty to serve a public interest. Public data processing is thus under a double requirement for justification, arising firstly from the special dangers and risks associated with the processing of data, but secondly also deriving from the special obligation of the state to serve the interests of the people.

C. Data as a special good and its effect on regulation

Without going into detail in regard to the special topic of this contribution, data protection law also takes into account that personal data has special qualities. Any type of regulation of personal data – be it a restriction or be it wide access to unlimited use of it – has to take this into account. Data and information cannot be treated as any other good, commodity or content of contractual relations.

This is the case, for one thing, because information and privacy are common goods in the economic sense.[18] This means that there exists no rivalry

17 Kühling and Raab (n. 2) Einführung para. 78. Art. 6 (1) lit. c and lit. e GDPR specifically address data processing in public responsibility. Emphasising broad flexibility clauses, Julian Wagner and Alexander Benecke, 'National Legislation within the Framework of the GDPR' (2016) 2 European Data Protection Law Review 353, 354–355. Pointing out the lack of a comprehensive data protection administrative law, Philipp Reimer, 'Verwaltungsdatenschutzrecht' (2018) Die Öffentliche Verwaltung 881, 881–882; more generally concerning different regulatory approaches in information law, Spiecker gen. Döhmann (n. 8) Introduction.

18 They are also experience goods, but this aspect shall not be further pursued in the course of this paper.

in consumption, and also no excludability from consumption of the good:[19] Anyone may use it, may use it again and may pass it on without the originator of the information being able to prevent this or control the flow of information. As a common good can be used multiple times by multiple users it is difficult to make such a good marketable: Market failure and enforcement deficits are typical effects in regard to such a good.[20] For regulatory impact, this means that legal protection of common goods has to start at the beginning of any transfer as any later use of information can hardly be traced. This is one of the reasons why data protection law does not only take into account specific risky handling of data but every step of data processing.

Personal information and privacy are special goods for another reason, as well. Information on a person is not something that cannot be separated from the person it is connected to and to the personality of the person. Information is never free of context. The individual traits and characteristics of a person are inseparable from the personal content of information on this person. Of course, some such links are stronger than others: A diary reveals more about a person than the name or the employer of that person. However, as context always matters, even those seemingly unimportant aspects of a person and his or her personality can, together with other infor-

---

19 See the report of the German Federal Justice Minister's conference, 'Arbeitsgruppe 'Digitaler Neustart' der Konferenz der Justizminister und Justizministerinnen der Länder' (2017) 30 <https://jm.rlp.de/fileadmin/mjv/Jumiko/Fruehjahrskonferenz_neu/Bericht_der_AG_Digitaler_Neustart_vom_15._Mai_2017.pdf> accessed 26 July 2020. Regarding the characters and difference between property rights and personality rights (192–194), giving a review of the discoursive question whether European Data Protection Law under GDPR contains property right aspects (199–204) and depicting the non-absolute character of data protection rights (201–202), Henry Pearce, 'Personality, Property and Other Provocations: Exploring the Conceptual Muddle of Data Protection Rights under EU Law' (2018) 4 European Data Protection Law Review 190. Arguing for a propertisation of data protection law while recognising privacy as a common good, Paul M. Schwartz, 'Property, Privacy, and Personal Data' (2004) 117 Harvard Law Review 2056, 2084–2090. Pointing out the property-derived rights under GDPR, Jacob M. Victor, 'The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy' (2013) 123 Yale Law Journal 513.

20 See Alan Randall, 'The Problem of Market Failure' (1983) 23 Natural Resources Journal 131; David Bollier, *Silent Theft: The Privat Plunder of Our Common Wealth* (Routledge 2013) 7; Richard J. Sweeney, Robert D. Tollison and Thomas D. Willett, 'Market Failure, the Common-Pool Problem, and Ocean Resource Exploitation' (1974) 17 Journal of Law and Economics 179, 180. Criticising the ideas of property of facts from a US-law viewpoint, Jessica Litman, 'Information Privacy/Information Property' (2000) 52 Stanford Law Review 1283, 1294, 1297.

mation, become very revealing as to individuality. This makes clear why in the German constitutional understanding of data protection rights (ie the right to informational self-determination[21]) there is a direct link to the constitutional guarantee of the person's dignity in Article 1 (1) of the Basic Law (*Grundgesetz*).

The consequences of this special character trait of information and privacy are – in legal terms – manifold. They include, first, that a property-based approach, similar to the US approach based on trespass,[22] is incompatible with this understanding.[23] Thus, the construction of data protection rights and privacy rights as property rights which can be sold and bought does not fit this quality of information. Secondly, further conclusions cannot be drawn from this concept of property-based information rights: A 'data donation' as has been discussed lately[24] is impossible under such conditions as no person is able to disconnect the information from its

21 Cf. German Federal Constitutional Court, 15 September 1983, Case 1 BvR 209/83, (1983) 65 Entscheidungen des Bundesverfassungsgerichts 1 – *Volkszählung*.

22 Cf. Patricia Mell, 'Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness' (1996) 11 Berkeley Technology Law Journal 1, 34; James Q. Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004) 113 Yale Law Journal 1151, 1211–1213; Russell L. Weaver and Steven I. Friedland, 'Privacy and the Fourth Amendment' in Dieter Dörr and Russell L. Weaver (eds), *Perspectives on Privacy – Increasing Regulation in the USA, Canada, Australia and European Countries* (De Grutyer 2014) 1, 2–3, 5 (giving an overview about the modified comprehension in jurisprudences reacting to technological progress), 5–17; Indra Spiecker gen. Döhmann, 'Datenschutz in der Globalisierung – Mission Impossible in einer Welt der Technikzukünfte unter Einwirkung einer neuen Datenschutz-Grundverordnung?' in Thomas Dreier and Indra Spiecker gen. Döhmann (eds), *Informationsrecht@KIT – 15 Jahre Zentrum für Angewandte Rechtswissenschaft* (KIT Scientific Publishing 2015) 63, 77; Schantz (n. 11) Art. 45 paras 41–43; about the lack of a comprehensive regulatory approach and the concept of privacy protection in specific areas, Paul M. Schwartz, 'Privacy and Democracy in Cyberspace' (1999) 52 Vanderbilt Law Review 1607, 1632–1634; Vera Bergelson, 'It's Personal but Is It Mine – Toward Property Rights in Personal Information' (2003) 37 UC Davis Law Review 379, 391–393.

23 Differentiating between the perception of data protection as a privacy law and property, the latter originated from USA, Henry Pearce, 'Personality, Property and Other Provocations: Exploring the Conceptual Muddle of Data Protection Rights under EU Law' (2018) 4 European Data Protection Law Review 190, 197–198. From Pearce's point of view the conception of data protection which the GDPR establishes is not incompatible with a property-right approach all together, but can rather be described as quasi-property rights, 204–205.

24 The German public health authority (Robert Koch Institute) provides an app that collects personal data (residence, height, weight) and has vital data transferred

personal connection. The only way to do this is to anonymise – and then data donation will no longer be necessary because there will be no personal data left. On the other hand, in contradiction to the concept of information/data protection as a property right, the present privacy- and personality right-oriented concept also allows for an acceptance of data to be rarely only one person's data. As the German Constitutional Court put it, human beings are social beings,[25] and as such, they continuously distribute data about themselves, and most of this information is connected to others.

Another consequence of this special character trait of information is the duration of this bond between person and information: Typically, there is a lifelong connection to all information acquired during the lifespan of a person. Age of data or the time span between the emergence of an information and its use do not in general diminish the power of data protection or privacy.[26]

Finally, in reference to an earlier observation: Information typically has no value on its own. It is a resource for making decisions: By incorporating the information present, decision-makers can act on it. However, this relationship between decisions and information only works one way, if at all. It is typically impossible to deduct from a decision the information and the sources which went into it. This has two effects: One is that the price for information is highly dependent on the individual preferences and contexts of the decision-maker; the other is that control of the flow of information is highly difficult to obtain as it would require exact knowledge not only of the information present and its sources but also of the normative values of the decision and the evaluation of potentially uncertain information.

---

from smart watches or activity trackers. The authority uses the app user's 'donated' data for research improving the calculation basis for early recognition of Covid-19 infections. See <https://corona-datenspende.de/>; <www.aerzteblatt.de/nachrichten/112636/RKI-Mehr-als-eine-halbe-Million-Teilnehmer-bei-Datenspende-App>; <www.heise.de/ct/artikel/Corona-Datenspende-App-des-RKI-4704898.html>; <www.reuters.com/article/us-health-coronavirus-germany-tech/germany-launches-smartwatch-app-to-monitor-coronavirus-spread-idUSKBN21P1SS> accessed 27 July 2020.

25 Cf. German Federal Constitutional Court, 15 September 1983, Case 1 BvR 209/83, (1983) 65 Entscheidungen des Bundesverfassungsgerichts 1 – *Volkszählung*.

26 This was recognised by the CJEU in the Google Spain decision; Case C-131/12 *Google Spain v AEPD and Mario Costeja González* [2014] ECLI:EU:C:2014:317.

All three specialties of information and privacy lead to one core conclusion: It is impossible for the individual, the so-called data subject,[27] to enact effective control over the use and processing of his or her data. This is the case, first, because of the huge amount of data in connection with his or her person, second, because of the huge amount of data processing involving personal data that goes unnoticed due to the quality of information as non-rival and non-excludable in consumption, and third, because of the decision to not reveal which information went into building the data set.

D. Data Access under the GDPR

I. Access and Data Processing

According to Article 4 (2) GDPR, data processing covers all and any operation or even sets of operations. Examples given of data processing include 'collection, recording', 'retrieval', 'disclosure' and 'dissemination or otherwise making available'. Thus, any access to personal data is covered by data processing under the GDPR. It does not matter whether this access is provided by activities performed on the side of the data subject (e.g. disclosure or submittal) or by activities on the side of the data controller (e.g. by tracing). Similarly, it does not play a role for the categorisation as processing whether the access to the data is granted by free will or whether it is exercised in the course of *force majeur* or vested powers, e.g. by the state.

II. Right to access of data under the GDPR

The GDPR contains a number of rights and obligations which can be categorised as granting access to personal data. They can be clustered according to the claimant: With most rights, the data subject is the one to demand access; with some rights a third party may do so.

27 Art. 4 (1) GDPR.

1. Rights to access by the data subject, Article 15 GDPR

The most prominent right to access of personal data is that regulated in Article 15 GDPR: It is considered to be the backbone of the power of the data subject: Only if it is known what is saved and how personal data has been processed can the data subject claim any further rights. Therefore, transparency is the first step, but it does not suffice to enact control.

Article 15 GDPR also specifies how far the right of access can be extended: According to Article 15 (1) GDPR, certain information typically has to be revealed on request beyond the fact that there is data processing taking place, e.g. the recipients of data transfers, the duration of data storage, the source of the data if it was not collected from the data subject etc.[28]

What is problematic, however, is whether the right to access under Article 15 GDPR also extends to data which has been recombined with other data, e.g. for the purposes of profiling or scoring where the result of the profile or the score may not necessarily be connected to the data subject.[29]

It also remains questionable whether the precise technology used for these analyses may be covered by the right to access. Article 15 (1) lit. h GDPR states, of the right to access in regard to automated decision-making, that the claim also includes 'meaningful information about the logic involved' as well as consequences and significance.[30] Thus, in a first step

---

28 Matthias Bäcker, in Jürgen Kühling and Benedikt Buchner (eds), *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz Kommentar* (2nd edn, Beck 2018) Art. 15 para. 9; Alexander Dix, in Spiros Simitis, Gerrit Hornung and Indra Spiecker gen. Döhmann (eds), *Datenschutzrecht. DSGVO mit BDSG* (Nomos 2019) Art. 15 para. 16. Art. 15 (1) GDPR contains a right to an affirmation of process and a right of access to all processed personal data, supplemented by the right to be provided with a copy in Art. 15 (3) GDPR. It is limited by rights and freedoms of others (Art. 15 (4) GDPR) and in case of a 'manifestly unfounded or excessive' request (Art. 12 (5) GDPR), Dix (n. 28) Art. 15 paras 12–17, 28–35; a controversy arose about the right's scope. See Philipp Zikech and Daniel Sörup, 'Der Auskunftsanspruch nach Art. 15 DSGVO' (2019) Zeitschrift für Datenschutz 239. Reacting to the decision of Regional Labour Court (*Landesarbeitsgericht*) Baden-Württemberg, 20 December 2018, Case 17 Sa 11/18, (2018), Stefan Brink and Daniel Joos, 'Reichweite und Grenzen des Auskunftsanspruchs und des Rechts auf Kopie' (2019) Zeitschrift für Datenschutz 483; Tim Wybitul and Isabelle Brahms, 'Welche Reichweite hat das Recht auf Auskunft und auf Kopie nach Art. 15 DSGVO? – Zugleich eine Analyse des Urteils des LAG Baden-Württemberg vom 20 December 2018' (2019) Neue Zeitschrift für Arbeitsrecht 672.

29 For further references see Dix (n. 28) Art. 15 No. 25 para. 58.

30 Giving an overview on the academic debate on a 'right to explanation' granted by the GDPR, Diana Dimitrova, 'The Right to Explanation under the Right of Ac-

the data subject may indeed claim the information about the applied technology. This does not, however, include an explanation of the precise decision-making method. Also, the phrasing of Article 15 (1) lit. h GDPR shows that the envisaged consequences have to be revealed and thus not the exact use and the exact consequences. While the claim is precise in regard to the technology, it remains fuzzy in regard to the application of the information.

The right to access does not include, however, the requirement that all material be released in which the personal data is present.[31] Right to access is not the same as a right to the inspection of records or files.[32] This is in accordance with the provision of Article 15 (3) GDPR (right to a copy of the personal data), as that provision allows for presentation of the data in

---

cess to Personal Data: Legal Foundations in and Beyond the GDPR' (2020) 6 European Data Protection Law Review 211, 214–126. Including systematic data and factors of automated decision making, Bäcker (n. 28) Art. 15 para. 27; Dix (n. 28) Art. 15 No. 25 para. 16; similar, Bryce Godman and Seth Flaxman, 'European Union regulations on algorithmic decision-making and a "right to explanation"' (2016) Oxford Internet Institute <https://arxiv.org/pdf/1606.08813.pdf> accessed 29 July 2020. Supporting a wide reading containing logic and systematic data that is not immediately personal counteracting the discriminatory potential of automated decision-making, Johanna Mazur, 'Right to Access Information as a Collective-Based Approach to the GDPR's Right to Explanation in European Law' (2018) 11 Erasmus Law Review 178, 183–184. Recognising a right to explanation rooted in Art. 15 GDPR in conjunction with Art. 22 and Recital 71 GDPR while evincing legal and technical limitations, Maja Brkan and Grégory Bonnet, 'Legal and Technical Feasibility of the GDPR's quest for Explanation on Algorithmic Decisions: Of Black Boxes, White Boxes and Fata Morganas' (2020) 11 European Journal of Risk Regulation 18, 20–22. Arguing that a right to explanation of specific decisions cannot be derived from the right to access, Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76, 83–90. Criticising the focus of discussion on a right to explanation as a core solution for opacity of automated decisions and algorithmic faults, Lilian Edwards and Michael Veale, 'Slave to the Algorithm: Why a Right to an Explanation Is Probably Not the Remedy You Are Looking for' (2017–2018) 16 Duke Law & Technology Review 18, 24–61.

31 Dix (n. 28) Art. 15 para. 17. Concerning inspection of records in German taxation procedure, Anna Sophie Poschenrieder, 'Ein Recht auf Auskunft begründet kein Akteneinsichtsrecht. Grenzen von Art. 15 DSGVO im Besteuerungsverfahren' (2020) 1–2 Deutsches Steuerrecht 21, 23.

32 Dix (n. 28) Art. 15 para. 17.

that format in which they are present with the data controller.[33] The right to obtain a copy in Article 15 (3) GDPR allows for additional control by the data subject because the right to access according to Article 15 (1) GDPR by itself would require the data subject to accept the information presented by the data controller while the copy of the data undergoing processing allows for further, including technological, conclusions.[34]

Finally, the result of the right of access is that the data subject may be able to enact a better judgment on further steps of action, e.g. a complaint to the supervisory authority or a request for erasure. The right of access is not originally meant to enable the data subject to make use of this data.[35] It remains questionable, therefore, whether the right to access gives the data subject the right to use the data from the data controller in an unrestricted way,[36] as trade and business secrets or at least trade and business interests of the data controller may be affected if the data subject makes use of the accessed data. It is clear, however, that the data subject may use the right of access and all information received under it in data-breach-related

---

33 Touching upon synchronous extent and difference in presentation format as regards right of access from Art. 15 (1), Malte Engeler and Daniel Quiel, 'Recht auf Kopie und Auskunftsanspruch im Datenschutzrecht' (2019) Zeitschrift für Datenschutz 2201, 2202–2203; with reference to the CJEU's decision relating to Art. 12 lit.a DPD (Joined Cases Case C- 141/12 and C-372/12 *YS v Minister voor Immigratie, Integratie en Asiel, and Minister voor Immigratie, Integratie en Asiel v M, S* [2014] ECLI:EU:C:2014:2081), Tim Wybitul and Isabelle Brahms, 'Welche Reichweite hat das Recht auf Auskunft und das Recht auf eine Kopie nach Art. 15 I DSGVO?' (2019) Neue Zeitschrift für Arbeitsrecht 672, 674–676. Dissenting, Sascha Kremer, 'Das Auskunftsrecht der betroffenen Person in der DSGVO' (2018) Computer und Recht 560, 564 para. 34.

34 Dissent exists on the basis of the exact nature and scope of the relationship between the right of access and the right of being provided a copy. Outlining that both are autonomous rights, Stefan Brink and Daniel Joos, 'Reichweite und Grenzen des Auskunftsanspruchs und des Rechts auf Kopie' (2019) Zeitschrift für Datenschutz 483, 434; Bäcker (n. 28) Art. 15 para. 39; dissenting, Philipp Zikesch and Thorsten Sörup, 'Der Auskunftsanspruch nach Art. 15 DSGVO' (2019) Zeitschrift für Datenschutz 239, 239–240; Dix (n. 28) Art. 15 para. 28.

35 Rather, it serves as a security for transparency and law enforcement: Boris P. Paal, in Boris P. Paal and Daniel A. Pauly (eds), *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz* (2nd edn, Beck 2018) Art. 15 para. 3; Bäcker (n. 28) Art. 15 para. 5; Margot E. Kaminski, 'Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability' (2019) 92 Southern California Law Review 1529, 1587.

36 The GDPR does not put the data subject's legal position in concrete terms, cf. Angela Sobolciakova, 'Right of Access under GDPR and Copyright' (2018) 12 Masaryk University Journal of Law and Technology 221, 226–227.

activities, ie information of the supervisory authority or a request for erasure. This right of use against private parties is derived not only indirectly from the purpose of Article 15 GDPR to enable control that needs to be effective but also from Article 6 (1) lit. f GDPR: The interests of the data controller cannot override the interests of the data subject in the case of a violation.

2. *Right to data portability, Article 20 GDPR*

The GDPR does not include many innovative regulatory tools in comparison to the DPD, but Article 20 GDPR certainly is one. As this provision will be the core of another paper in this volume, this paper will only look at the provision from the standpoint of access to data from the special perspective of data protection.

Article 20 GDPR is a clear sign that data protection is increasingly including a consumer law perspective and also competition law aspects.[37] Article 20 GDPR reacts to the special qualities of many service providers as part of a larger network economy in which the economy of scale and scope prevents functioning competition.[38] Although this creates information asymmetry and a lack of control by actors other than the data subject and thus refers to some of the concerns of data protection law, the regulation

37 Cf. Article 29 Data Protection Working Party, WP 242 rev. 01, (2017) 4 <http://ec.europa.eu/newsroom/document.cfm?doc_id=44099> accessed 27 July 2020; Inge Graef, Martin Husovec and Nadezhda Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2018) 19 German Law Journal 1359, 1375; Helena Ursic, 'Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control' (2018) 15 SCRIPTed (Journal) 42, 44.

38 Lucio Scudiero, 'Bringing Your Data Everywhere: A Legal Reading of the Right to Portability' (2017) 3 European Data Protection Law Review 119, 119. See the resolution of the German National Data Protection Conference, stating the role of the data portability right in strengthening consumers' positions and limiting market-dominating positions: 'Entschließung Marktmacht und informationelle Selbstbestimmung, 88. Konferenz der Datenschutzbeaugten des Bundes und der Länder, 08./09. Oktober 2014', <www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/88DSK_Marktmacht.html?nn=5217228> accessed 27 July 2020. The right to data portability was originally targeted to counteract so-called 'lock-in effects', especially in the context of social networking platforms; Dix (n. 28) Art. 20 para. 1; Gerrit Hornung, 'Eine Datenschutz-Grundverordnung für Europa? Licht und Schatten im Kommissionsentwurf vom 25. Januar 2012' (2012) Zeitschrift für Datenschutz 99, 103.

of a failing market order are not the prime interests of data protection.[39] Article 20 GDPR now illustrates that data protection law is becoming more and more a tool for other regulatory aspirations, as well, predominant among them consumer protection law and competition law.[40]

Under Article 20 GDPR, the data subject may request personal data present with a data controller to be presented to him or her in such a way that the data subject may transfer this data to another data controller. Article 20 (2) GDPR clarifies that the data subject may also request a direct transfer from the data controller to another party and need not undergo the effort of becoming a mediator of services.

Thus, consumers are enabled to switch to another service provider with minimal outlay and without loss of data. From an economic view obstacles to market access are reduced, hence conditions of competition should be ensured.[41] The right to data portability, which includes access and transfer services, aims to safeguard the data subject's control over transmission between processors and to extend possibilities of self-determined decision-

39 Cf. Article 29 Data Protection Working Party, WP 242 rev. 01, (2017) 4 <http://ec.europa.eu/newsroom/document.cfm?doc_id=44099> accessed 27 July 2020.

40 For the latter cf. only the decision of the German antitrust agency (*Bundeskartellamt*) against Facebook of February 2019; Bundeskartellamt, 'Bundeskartellamt prohibits Facebook from combining user data from different sources' (6 February 2019) <www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html> accessed 27 July 2020; as well as the two consecutive court decisions, Düsseldorf Higher Regional Court, 26 August 2019, VI Kart 1/19 (V), (2019) Multimediarecht 742; German Federal Supreme Court, 23 June 2020, KVR-69/19, <https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2020/2020080.html?nn=10690868> accessed 4 August 2020 (press release), in the end upholding the decision. Thus, data protection violations were used as a shoehorn for competition law impact. See for comments on the antitrust authority's decision in the literature, Christina Etteldorf, 'Data Protection from a Different Perspective: German Competition Authority Targets Facebook's Data Usage' (2019) 5 European Data Protection Law Review 238; Irene Lorenzo-Rego, 'The Perspective of the Bundeskartellamt in the Evaluation of Facebook's Behaviour: Prior Considerations and Possible Impact' (2019) 3 European Competition and Regulatory Law Review 100; Christoph Becher, 'A Closer Look at the FCO's Facebook Decision' (2019) 3 European Competition and Regulatory Law Review 116.

41 Michael Strubel, 'Anwendungsbereich des Rechts auf Datenübertragbarkeit. Auslegung des Art. 20 DS-GVO unter Berücksichtigung der Guidelines der Article 29-Datenschutzgruppe' (2017) Zeitschrift für Datenschutz 355, 355.

making;[42] simultaneously it is geared towards the goal of regulating market monopoly.[43]

It should be noted that access to data under Article 20 GDPR is limited to data which has been processed on the basis of either consent or a contractual relationship (Article 20 (1) lit. a GDPR).

The exact impact of Article 20 GDPR is still unclear in regard to the scope of data that is covered. It can be argued that only data which the data subject has actively submitted to the data controller or knows that is being processed is captured by the provision in order not to have Article 20 GDPR become a super-right for any type of access to any type of data including evaluation or analysis data.[44]

III. Right to access of data by others than the data subject

Data protection law does protect data and it assures controllability, but it does not hinder data processing. Rather, as any technology regulatory law, it aims at avoiding the pitfalls of digitalisation. On the other hand, this means data protection law is not preventing data processing that follows certain procedures, restricts an overarching impact and remains within the boundaries of the GDPR. Similarly, access of data is not something that the GDPR explicitly forbids but rather restricts in the interest of the data subject and common goals.

---

42 Improving the data subject's control of its personal data is mentioned in Recital 68 sentence 1 GDPR. See also Article 29 Data Protection Working Party, WP 242 rev. 01, (2017) 6 <http://ec.europa.eu/newsroom/document.cfm?doc_id=44099> accessed 27 July 2020; Ursic (n. 37) 44, 58–60; Graef, Husovec and Purtova (n. 37) 1365–1366.

43 Cf. Peter Schantz, 'Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht?' (2016) Neue Juristische Wochenschrift 1841, 1845; Ursic (n. 37) 58–59; cf. Graef, Husovec and Purtova (n. 37) 1365, 1369.

44 Dix (n. 28) Art. 20 para. 8; Tobias Herbst, in Jürgen Kühling and Benedikt Buchner (eds), *Datenschutzgrundverordnung Kommentar* (C.H. Beck 2017) Art. 20 No. 11; cf. Article 29 Data Protection Working Party, WP 242 rev. 01, (2017) 10–11 <http://ec.europa.eu/newsroom/document.cfm?doc_id=44099> accessed 27 July 2020; Scudiero (n. 38) 123; Heike Schweitzer, 'Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung' (2019) Gewerblicher Rechtsschutz und Urheberrecht 569, 574. Giving an overview on differing views, Kai von Lewinski, in Stefan Brink and Heinrich A. Wolff (eds), *Beck'scher Online-Kommentar Datenschutzrecht* (C.H.Beck 2020) Art. 20 paras 37–48.

Consequently, the GDPR includes a number of provisions under which access to data can be obtained by parties other than the data subject. They shall – in an overview – be the content of this section. It should be noted that some of these provisions within the GDPR are not formulated as a direct right which can be exercised, but are often more subtly included in other provisions that deal with data processing as such. It should not be forgotten that data access is a type of data processing, and as such some of the provisions may yield data access in a much broader sense than typically associated with the data protection legal regime.

1. Consent or legal ground as basis for data processing, Article 6 (1) GDPR

Considering this data access as data processing the first and most important way of gaining access to data protected under the GDPR would be to adhere to the standards of the GDPR on data processing.

Most importantly, the GDPR contains a number of legitimate grounds on which any type of data processing and thus also access to data can be enabled. Within the more specific provisions of Article 6 GDPR, a number of interests are weighted on a general level, taking into account special situations and special circumstances of typical data processing such as contractual or legal obligations or also life-threatening situations. Article 6 (1) lit. f GDPR, finally, opens desirable data processing for a more individualised balancing test, at least between private data controllers.

It should be noted that this generalisation of balancing of interests inherent in Article 6 (1) GDPR takes into account interests on the side of the data processor and potential further third parties who would profit from the data processing and also interests on the side of the data subject and potential further third parties which are affected by data processing.[45] This needs mentioning because the wording in Article 6 (1) GDPR is not always precise. For example, Article 6 (1) lit. f GDPR mentions on the one hand 'interests pursued by the controller or by a third party' and on the other hand 'interests […] of the data subject'. Article 1 (1) GDPR, however, and the aforementioned general purpose of the GDPR, make clear

45 Cf. Peter Schantz, in Stefan Brink and Heinrich A. Wolff (eds), *Beck'scher Online-Kommentar Datenschutzrecht* (C.H.Beck 2020) Art. 1 para. 7. Specific to Art. 6 lit. f GDPR, Schantz (n. 11) Art. 6 paras 98–99, 101–102. A number of interests to be included are identified in Indra Spiecker gen. Döhmann, 'A new framework for information markets: Google Spain' (2015) Common Market Law Review 1033, 1046 et seq.

that data processing not only has effects on the data subject but also on third parties, who are judged on the basis of information gathered from individuals.[46] Thus, on both sides of the scale not only the interests of the parties involved directly, but also the effects on the whole, have to be integrated. This explains why the data protection legal regime is not restricted to certain elements within the information cycle but covers all steps and also integrates effects going beyond individual legal interests and rights and thus offers a comprehensive solution.

The GDPR points out manifold reasons, beyond a balancing of interests in the individual case (typical of this is Artice 6 (1) lit. f GDPR), for granting access. Here, some little-regarded interests shall be pointed out, in particular as they are used as an argument why an extensive data access regime is necessary. The GDPR opens personal data to these purposes so the need for additional access rights is not necessarily pressing.

Foremost, one should mention Article 6 (1) lit. d GDPR which allows for processing necessary 'in order to protect the vital interests of the data subject or of another natural person'. This covers a number of catastrophic, pandemic or life-threatening situations in which data processing assists in curing or at least relieving imminent dangers. Even if Article 9 (1) GDPR is considered to be an additional threshold to health-related data,[47] in a number of cases the clause of Article 9 (2) lit. c GDPR covers even the processing of special data and consent will always be possible according to Article 9 (2) lit. c and 9 (2) lit. a GDPR.

Likewise granting very wide access to data are the provisions of Article 6 (1) lit. c and lit. e GDPR when the purpose of the data processing can be subsumed under the goal of furthering the common good. While the meaning of Article 6 (1) lit. c and e GDPR is often confined to the opening

46 Cf. Schantz (n. 11) Art. 6 para.102; Joshua A. Fairfield and Christoph Engel, 'Privacy as a Public Good' (2015) 65 Duke Law Journal 385, 396–406.

47 Cf. Recital 51 sentence 5; Thomas Petri, in Spiros Simitis, Gerrit Hornung and Indra Spiecker gen. Döhmann (eds), *Datenschutzrecht. DSGVO mit BDSG* (Nomos 2019) Art. 9 No. 24; Marion Albers and Raoul-Darius Veit, in Stefan Brink and Heinrich A. Wolff (eds), *Beck'scher Online-Kommentar Datenschutzrecht* (C.H.Beck 2020) Art. 20 paras 37–48; Thilo Weichert, in Jürgen Kühling and Benedikt Buchner (eds), *Datenschutzgrundverordnung Kommentar* (C.H. Beck 2017) Art. 9 No. 4; contradicting this, Frenzel (n. 16) Art. 9 No. 18; Alexander Schiff, in Eugen Ehmann and Martin Selmayr (eds), *DS-GVO Kommentar* (C.H. Beck 2017) Art. 9 No. 9.

clause for member state public interest laws it contains,[48] its importance initially rests in making data protection law applicable for all public interest causes. Thus, although data access in the public interest has to keep in mind the principle of proportionality and may not overburden data protection interests, it nevertheless can be an important reason why data processing is possible.

A similarly hidden door opener to wide access of data is the legitimation clause of Article 6 (1) lit. c GDPR, according to which a legal obligation may cause the access to data. As the legal obligation has to be enacted either by member-state or Union law, there has to be an overriding public interest in this data access.[49]

Thus, under this clause, a number of data accesses in the public interest can be legitimised, and considering the special interests in member states or the Union, very specific interests can be served.

It should be stated, however, that public interests cannot be freely construed and enacted without restrictions but are limited themselves. The principle of proportionality[50] has already been mentioned. Also, they need to have a constitutional or other foundation within member state law, and they may not be construed to violate the core principles of EU law, in particular Articles 7 and 8 of the EU Charter protecting the interests of data, communication and privacy. Thus, ethical or other normative standards, which are sometimes voiced to enable free data access, are not sufficient if they do not have a legal foundation. This is especially true for arguments such as a duty under a principle of solidarity which is raised as a reason for

48 Art. 6 (6 (2) and (3) GDPR contain opening clauses in regard to data processing covered by lit. c. While there is some debate over the relationship and scope of the opening clause(s) – cf. Alexander Roßnagel, in Spiros Simitis, Gerrit Hornung and Indra Spiecker gen. Döhmann (eds), *Datenschutzrecht. DSGVO mit BDSG* (Nomos 2019) Art. 6 No. 16–21; Albers and Veit (n. 47) Art. 6 No. 35; Julian Wagner and Alexander Benecke, 'National Legislation within the Framework of the GDPR' (2016) 2 European Data Protection Law Review 353, 354–355 –, its function as gateway for European or national legislation concerning data processing by 'public bodies' is emphasised consistently; cf. Roßnagel (ibid.) Art. 6 para. 52; Benedikt Buchner and Jürgen Kühling, in Jürgen Kühling and Benedikt Buchner (eds), *Datenschutzgrundverordnung Kommentar* (C.H. Beck 2017) Art. 6 No. 83; Wagner and Benecke (ibid) 354.

49 Cf. Roßnagel (n. 48) Art. 6 No. 1 para. 53.

50 Art. 6 (6 (3), fourth sentence GDPR. It should be noted that every legal obligation governing the processing of personal data restricts the freedom under Art. 8 of the EU Charter of Fundamental Rights. Art. 52 (1) second sentence of the Charter requires its accordance with the principle of proportionality. See Roßnagel (n. 48) Art. 6 No. 35.

disclosure and access to information, e.g. in discussions on the legality and desirability of data donations. Even in public health care systems, solidarity is restricted to certain legal forms; in Germany, for instance, solidarity can only be an argument in regard to the financial contribution within the health care system but not in regard to the behaviour of patients and citizens.[51]

2. *Limitation of purpose and extension of purpose*

There are a number of general principles within data protection law; some are listed in Article 5 (1) GDPR.

a) The strict binding of data processing to a specific purpose

Under the DPD, the limitation of purpose was a stronghold of data protection principles. Under the GDPR, a similar and even more explicit formulation can be found in Article 5 (1) lit. b GDPR.

The purpose limitation works two ways:[52] It first binds every gathering of personal data to a 'specified, explicit and legitimate' purpose. Thus, the collection (and storage) of data for no specific reason is unlawful under the GDPR.[53] In a second step, the purpose limitation binds every consecutive step following the original gathering of data to this exact same original

51 Cf Sec. 1 German Social Code (*Sozialgesetzbuch*) Part V. See in regard to health insurance as a community of solidarity and the incompatibility of a behaviour-based health insurance system with solidarity the German Ethic Board's statement, Deutscher Ethikrat, 'Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung' (2018) 11, 230–237, <www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-big-data-und-gesundheit.pdf> accessed 1 August 2020; Executive Summary: <www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/englisch/opinion-big-data-and-health-summary.pdf> accessed 27 July 2020.

52 For a more detailed approach cf. Maximilian von Grafenstein, *The Principle of Purpose Limitation in Data Protection Laws* (Nomos 2018) 425 et seq.

53 Roßnagel (n. 48) Art. 5 No. 72; Schantz (n. 45) Art. 5 No. 13; cf. Zarsky (n. 11) 1006. In regard to purpose under the DPD, Article 29 Data Protection Working Party, WP 203 (2013) 15 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203en.pdf> accessed 27 July 2020.

purpose.[54] This is important to note, as a common misunderstanding[55] believes a legitimation to be sufficient only for the first step of data processing, which would then justify all further processing of this data, e.g. the transfer of it to other parties.[56] This is, however, not the case under the GDPR.

In consequence, a situation is created by which the data subject may control the flow of his or her data to the first controller and the more precise circumstances of processing. The purpose itself can be broader or more narrow depending on the weight of infringement: The more infringing the data processing potentially is, the more precisely must the purpose be defined in order to allow a proper assessment.[57]

However, the GDPR contains two big exceptions from the strict principle of binding purpose which allow for further accessing of data despite the boundaries from the purpose limitation. Both are integrated into Article 5 (1) lit. b GDPR. The first one allows for secondary purposes for which data can be processed, so-called compatible purposes, and the second one allows for different entities and different purposes and reacts to the inter-

---

54 Herbst (n. 44) Art. 5 No. 38. Further issues of admissibility arise just in cases of consecutive processing for another purpose (compatible/incompatible): Herbst (ibid.) Art. 5 No. 22–24; Schantz (n. 45) Art. 5 No. 18–19; Roßnagel (n. 48) Art. 5 No. 92–93, 96–102; with respect to the DPD, see Article 29 Data Protection Working Party, WP 203 (2013) 12 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203en.pdf> accessed 27 July 2020; cf. von Grafenstein (n. 52) 34.

55 Part of this misunderstanding arises from an unclear distinction between consecutive data processing for the original purpose and consecutive data processing for a different, albeit potentially compatible purpose.

56 On the question of purpose-compatible further processing, Roßnagel (n. 48) Art. 5 No. 97–99; Lukas Feiler, Nikolaus Forgo and Michaela Weigl, *The EU General Data Protection Regulation (GDPR): A Commentary* (Globe Law and Business Ltd 2018) Art. 6 No. 14; Jürgen Kühling and Mario Martini, 'Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?' (2016) 27 Europäische Zeitschrift für Wirtschaftsrecht 448, 451. For instance, in US law, the US Federal Information Privacy Law (esp. FRCA) basically legitimises data processing for a wide range of purposes, exempting processing for employment purposes or when medical data is contained, where consent by an opt-in mechanism is required; Paul M. Schwartz and Karl-Nikolaus Peifer, 'Transatlantic Data Privacy Law' (2017) 106 Georgetown Law Journal 115, 153.

57 Schantz (n. 45) Art. 5 No. 15; with respect to the DPD: Article 29 Data Protection Working Party, WP 203 (2013) 15–16 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203en.pdf> accessed 27 July 2020.

ests of 'archiving purposes in the public interest, scientific or historical research purposes or statistical purposes' within the meaning and the boundaries of Article 89 GDPR when these are in accordance with the original purpose.

b) Compatible other purposes

The GDPR – as did the DPD – distinguishes in principle two types of purposes: One type is the original purpose, which may allow for a number of consecutive and parallel instances of data processing once data has been legally obtained under this purpose if further steps are necessary to achieve this purpose. The second type contains all other purposes that may occur with the data which has been obtained under another purpose. This other purpose-oriented data processing is not justified under the original legitimation of the data processing. As a consequence, any data processing for such an 'other purpose' would be unlawful if it could not be justified by itself, and this would require a complete new testing.

The GDPR now opens up another venue by a fiction: According to Article 5 (1) lit. b GDPR's difficult terminology, there exists a 'compatible purpose'. This is, in the above typology, a different purpose from the original one.[58] However, the legal fiction declares such compatible purposes to be covered by the original purpose and thus legal under the same legal grounds and adherence to procedural standards.[59] A change of purpose is thus legally harmless.

Article 6 (4) GDPR gives guidelines as to which factors should be taken into account in order to assess whether a new purpose is compatible, ie the context and the relationship between data subject and data controller (Ar-

58 Schantz (n. 45) Art. 5 Nr 18; Herbst (n. 44) Art. 5 No. 24, 42. Dissenting, Roßnagel (n. 48) Art. 5 No. 97.

59 Further processing for a compatible purpose fulfilling GDPR requirements (e.g. Art. 6 (6 (1) GDPR) is lawful, whereas consecutive processing for an incompatible purpose is unlawful per se. See also Schantz (n. 45) Art. 5 No. 23; Herbst (n. 45) Art. 5 No. 24, 28–29, 47–49; Jessica Bell and others, 'Balancing Data Subjects' Rights and Public Interest Research' (2019) 5 European Data Protection Law Review 43, 48; cf. the difference between the final version and the wording of Art. 5 lit. b GDPR in the Commission proposal interpreted by Article 29 Data Protection Working Party, WP 203 (2013) 36 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203en.pdf> accessed 31 August 2020. Dissenting, Roßnagel (n. 48) Art. 5 No. 96–99.

ticle 6 (4) lit. b GDPR), or the consequences of the new purpose-oriented data processing in comparison to the original intended consequences.

In the end, the establishment of compatible other purposes enlarges the possibilities under which data can be accessed because a transfer of data to another entity and another data controller may well be in accordance with the new purpose. Once legally obtained, data may then be continuously used for other purposes, as well. The new controller, however, should take care to inform itself about the restrictions of the original data processing, as those restrictions still apply under the new purpose.[60] This also covers the event that the original purpose is fulfilled. In this case, the justification for the compatible purpose also ceases to apply.

c) Archiving, Research and Statistics as privileged purposes

The second exception is also rooted in Article 5 (1) lit. b GDPR itself. It reacts to a special conflict of interests between the privacy interests of a data subject and the interests in continuous use of personal data for archiving, research and statistics.[61]

All three of these purposes are declared to be compatible purposes per se; further limitations are not expressed. In particular, Article 6 (4) GDPR does not apply and thus no individual balancing of interests takes place; the legitimation for the original processing is extended to the processings for these purposes.

The GDPR recognises this flaw and refers to Article 89 GDPR, according to which any processing for these purposes 'shall be subject to appropriate safeguards' (Article 89 (1) GDPR). These include the requirement to anonymise as early as possible (Article 89 (1), last sentence, GDPR).

This provision in Article 5 (1) lit. b GDPR answers concerns from the side of these interests, in particular research interests, which are often raised when claiming that a comprehensive legal regime to free access of

60 Cf. Roßnagel (n. 48) Art. 5 No. 93; Herbst (n. 45) Art. 5 No. 23; Frenzel (n. 16) Art. 5 No. 29.

61 Alexander Roßnagel, 'Datenschutz in der Forschung' (2019) Zeitschrift für Datenschutz 157, 159; Thilo Weichert, 'Die Forschungsprivilegierung in der DSGVO' (2020) Zeitschrift für Datenschutz 18, 18–19. Disagreement remains on whether the ground for privileged status is that these purposes are more highly valued, Weichert (ibid.) 21, or that these purposes are not connected to the data subject, Frenzel (n. 16) Art. 5 No. 32; Roßnagel (n. 48) Art. 5 No. 104. Taking both aspects into account, Herbst (n. 45) Art. 5 para. 52.

data has to be established. Frequently, it is argued in the interest of research and scientific purposes, based on the assumption that data protection in this regard blocks access and processing, that the data protection regime should be abandoned.[62] These assumptions, however, do not show a consideration for the purposes of the GDPR and they do not reflect the GDPR's standing towards research and scientific interests properly. These purposes are privileged under the GDPR already, and this privilege allows for wide access to existing personal data. Thus, a further research exemption or a further regulatory impact on research data is not necessary as such. Rather, one can ask why there seems to be a desire for almost limitless access to personal data.

Any legal regime could make use of the opening clauses in Article 89 (2) GDPR under which the member states (or EU law) may provide for derogations from central rights of the data subject and thus encroach even further on data subjects' rights than the privilege itself does. This is the case because the GDPR does not provide any obvious restriction on the terminology or the exact purposes of research and science.[63] So any type of science – as obscure and controversial as it may be – could claim the privilege of Article 89 GDPR.[64]

Considering the wide impact of statistical and scientific data processing, a completely unlimited privileging would make the GDPR devoid of application in an area where the risks of automated decision-making and of wide use of personal data that it is intended to mitigate are particularly present. The development, and often the application of Big Data, artificial intelligence, ubiquitous computing, direct marketing, profiling, tracking and scoring would all fall under statistical and/or research purposes and

62 E.g. Amy Kristin Sanders, 'The GDPR One Year Later: Protecting Privacy or Preventing Access to Information' (2019) 93 Tulane Law Review 1229. Dissenting, Kim Leonard Smouter-Umans, 'GDPR and Research: Is the GDPR Eventually Going to Be Good or Bad for Research?' (2018) 2 International Journal for the Data Protection Officer, Privacy Officer & Privacy Counsel 29; Mike Hintze, 'Science and Privacy: Data Protection Laws and Their Impact on Research' (2019) 14 Washington Journal of Law, Technology & Arts 103, 121.

63 See Recital 159, sentences 2–3.

64 Cf. Carolyn Eichler, in Stefan Brink and Heinrich A. Wolff (eds), *Beck'scher Online-Kommentar Datenschutzrecht* (C.H.Beck 2020) Art. 89 paras 3, 7; Alexander Roßnagel, 'Datenschutz in der Forschung' (2019) Zeitschrift für Datenschutz 157, 159; Benedikt Buchner and Marie-Theres Tinnefeld, in Kühling and Buchner, *Datenschutz-Grundverordnung* (n. 28) Art. 89 No. 13. Contradicting this, Johannes Caspar, in Simitis, Hornung and Spiecker gen. Döhmann, *Datenschutzrecht* (n. 2) Art. 89 No. 25; Weichert (n. 61) 20–21.

thus be widely exempted from the bindings of the purpose limitation and many other restrictions of the GDPR.[65] Therefore, restrictions of the purposes of research for data access have to be derived from the inherent meaning and structure of the GDPR itself.

The context of the exceptions help in construing a meaningful description of research and of statistics. That this is the goal of the GDPR itself, rather than unlimited access and data processing for these purposes, can be seen in the wording and the recitals. Archiving, the first of the three special purposes, is restricted by the wording 'public interest'. Also, Recital 162, sentence 5, GDPR clarifies that statistical data may only be aggregated data. The existence of Articles 7 and 8 of the EU Charter of Fundamental Rights requires an interpretation which leaves ample room for the general goals of the GDPR.[66]

Without being able to go further into detail in this paper, the seemingly wide research clause has to be read as research in the public interest. This does not prevent private research from profiting from Articles 89 and 5 (1) lit. b GDPR, as Recital 50 clarifies. But it does exclude a completely commercialised research interested only in commercial use and the own interest of the researching institution.[67] Public interest can be demonstrated by other tools than public research, e.g. by being publicly funded, by being made publicly available (e.g. by patents, licences for use) and by being published and transparent. Thus, any research which aims at remaining a trade and business secret is not considered to be a compatible purpose, just as private archiving or individualised statistical evaluation is not covered.

In the end, this interpretation allows access to data for research purposes in the common interest. It also enables data protection interests and research interests to be aligned.

---

65 Similar, Johannes Caspar, in Simitis, Hornung and Spiecker gen. Döhmann, *Datenschutzrecht* (n. 2) Art. 89, No. 17; Benedikt Buchner and Marie-Theres Tinnefeld, in Stefan Brink and Heinrich A. Wolff (eds), *Beck'scher Online-Kommentar Datenschutzrecht* (C.H.Beck 2020) Art. 89 para. 12; Weichert (n. 61) 20–21. Although arguing that the purpose limitation principle hinders big data uses significantly, Tal Z. Zarsky assumes that commercial big data analyses cannot be included in statistical purposes; Zarsky (n. 11) 1105–1007.

66 Cf. Johannes Caspar, in Simitis, Hornung and Spiecker gen. Döhmann, *Datenschutzrecht.* (n. 2) Art. 15 No. 32 et seq.

67 Ibid. Art. 15 No. 16; Weichert (n. 61) 20–21.

3. *Freedom of expression, media, press and journalistic purposes, Article 85 (1) GDPR*

Similarly, Article 85 (1) GDPR requires member states to establish a regulatory regime which enables freedom of expression as well as the institutionalised human rights of the media from both an institutionalised and a personal ('journalistic purposes') perspective.

4. *Transparency and freedom of information, Article 85 (1) GDPR*

Article 5 (1) lit. b GDPR, with its extension of the purpose limitation, privileges research, archiving and statistics in a particular way. However, in Article 85 (1) GDPR, the explicit necessity to reconcile data protection interests and interests in transparency and freedom of information is mentioned and left to member state law.

E. Guidelines for a regulatory regime in conformance with data protection

Having thus sketched the general framework of the GDPR on how personal data can be assessed, it becomes clear that data protection does not exclude access to data. Rather, it aims at creating access to data in a way that is socially and personally desirable and which – as the purpose limitation illustrates – is limited and controllable. Thus, the GDPR restricts access to data and creates an individualised approach without banning it or being unfriendly towards data processing. Rather, this approach is able to take into account some of the background noise of what data can positively and negatively achieve in the decisions being drafted on the basis of these.

The insights on a meta-level should not be forgotten when analysing the data protection regime as a potential starting point for a wide data access regime.

I. Proactive versus reactive regime

Data protection law as such and the GDPR in all its specificity are technology laws,[68] functioning according to the insights on how to regulate technologies whose development and effects are not yet fully known or indeed predictable. This is very much true for digitalisation and information technology: The tremendous speed in which this technology evolves, the huge investments by private and public actors, the new ubiquity of information technology and data processing, the difficulty of assessing the results of data in decisions and the technology's psychological, cognitive and educational effects are just a few very obvious examples of the unknowns in this multi-actor, complex field.

Experiences from technology law and the understanding of state decision-making under conditions of uncertainty teach us in circumstances such as these to use a proactive, preventive concept of regulation combined with close monitoring and high flexibility and with clear models and structures.[69] Risk prevention, and not security management, has to be the guiding principle.

II. Irreversible and uncontrollable consequences versus liability and damages

Data protection law pays close attention to the understanding that data rights violations are not damages that can easily be controlled for and compensated. As any loss of data means uncontrollable access to this data and potential further use and distribution including recombination with other data, the characteristic of information and privacy as common goods[70] have to be reflected in any regulatory regime. Typical regulatory concepts

68 Cf. on the term 'technology law', Milos Vec, *Kurze Geschichte des Technikrechts* (Springer 2011) 3–91, 4–8; in regard to computer law, Thomas Dreier and Oliver Meyer-Brandt, 'Computerrecht' in Martin Schule and Rainer Schröder (eds), *Handbuch des Technikrechts* (2nd edn, Springer 2003) 823; and data security, Hannes Federrath and Andreas Pfitzmann, 'Datensicherheit' in Schule and Schröder (ibid) 857; in regard to the relationship between technology and data protection law, Hornung and Spiecker gen. Döhmann (n. 2) Einleitung paras 244–249; declaring the aspect of information law a technology law, Michael Kloepfer, *Informationsrecht* (C.H. Beck 2002) § 1 para. 4.

69 See Indra Spiecker gen. Döhmann, *Staatliche Entscheidungen unter Unsicherheit* (Mohr Siebeck 2021, forthcoming).

70 See at C. below.

like absolute liability without culpability and easy compensation[71] do not function in conditions of such great uncertainty.

Understanding this already requires a careful defining of meaningful access to data, as the price for any later corrections has to be paid by the data subjects without being able to receive just compensation because data breaches can hardly ever be fully retracted, certainly not under conditions of professional information technology evaluation and exploitation. Data protection rights violations cannot be cancelled, and they cannot be undone.

III. Specific, controlled, anti-discrimination interests versus overall transparency and access

Transparency and free access to information for each and all sound intriguing. However, they leave out of consideration that information technology is not available for all, and that the need for information depends on the decision in which it is to be incorporated. Information can well be used for purposes which violate common understandings in society, such as anti-discrimination, equality before the law, or fair chances. The purpose and the precise interest determine whether or not it is socially, economically, legally, ethically, internationally and normatively desirable to share data, and if so, under which conditions. Thus, unlimited access to personal data and transparency without any requirement as to purpose do not serve the common interest but the interest of a select few.

F. Conclusion and Outlook

We have lived in a knowledge society long enough to understand the importance of data and also the difficulties in detecting data in decisions and controlling the flow of data once it has been started. Surprisingly, our regulatory impetus to prevent negative impact on society overall and to create a fair division of data is not reacting strongly to this: We are generous in sharing data and making available the backbone of productivity –

71 See Spiecker gen. Döhmann (n. 69).

for free. Numerous freedom of information regulatory impulses tell this story forcefully.[72]

Uncontrollability of the input of data in the output of decisions requires a three-step-test: Both the input of data, with its processing e.g. by recombination, and the outcome of the decision have to be controlled.

Data protection law approaches all three steps from a particular, personality and human rights perspective and thus offers answers to pressing questions. It also gives important guidelines for the necessary weighing of interests between the protection of data and access and distribution of data beyond personal data.

The GDPR does not address the pressing issue of the gains and the added value within the data lifecycle. It is not an instrument creating economic or social distributive justice, nor does it attribute economic value. It explicitly refrains from creating property rights, and it explicitly contradicts the notion of data being foremost an economic asset. But it is an instrument to strengthen democratic values such as liberty, freedom of decision and autonomy.

Access to data is always a decision on third parties without their inclusion, their participation or their knowledge. Modern information technology often has little interest in the individual and its individuality, which makes individual control and countermeasures even more difficult. A data-protection-friendly regulatory regime to access of data will take these third-party-effects into account and builds the limitations to data use into it.

In any decision of the legislature on whom to grant access to data the decision on the use of this data is always incorporated. Data protection's interest in binding data processing to a cause and a purpose relies on basic functionalities in situations of power. Insights into the foundations of state control can assist in finding the proper legal standards. Among these standards is the core of all rationality: If there is a legitimate reason which can be openly discussed, there is ground for data access, but data access with-

72 See, for example, Thomas Dreier and others (eds), *Informationen der Öffentlichen Hand – Zugang und Nutzung* (Nomos 2016); Spiecker gen. Döhmann (n. 8); Kloepfer (n. 68), especially § 4 paras 12–14; Jean Nicolas Druey, *Information als Gegenstand des Rechts – Entwurf einer Grundlegung* (Schulthess 1995); Herbert Burkert, 'Public Sector Information: Towards a More Comprehensive Approach in Information Law' (1992) 3 (1) Journal of Law Information and Science 47; Herbert Burkert, *Informationszugang und Datenschutz: ein kanadisches Beispiel* (Nomos 1992). Cf. in regard to consistency of regulatory instruments like the right to data portability, Graef, Husovec and Purtova (n. 37), proposing a comprehensive legal code concerning access to public information.

out clear purpose cannot claim legitimacy. This, due to the special characteristic of data, is a ground to start from.

In the end, all we know about data, about data processing and about decision-making and its control calls for a data-protection-inspired regulatory regime of data access, and that is in dubio pro data protection – including trade and business secrets!