Prof. Dr. Martin Nettesheim University of Tübingen Law School

Data Protection in Contractual Relationships (Art. 6 (1) (b) GDPR)

April 24th, 2023

Abstract

The General Data Protection Regulation (GDPR) sets forth that a justification is required for a company (the “controller”) to process personal data. The list of justification grounds in Art. 6(1) GDPR is exhaustive. Art. 6(1)(b) GDPR provides that the controller acts justifiably if the processing of personal data is necessary for the performance of a contract to which the data subject is party. The use of this legal justification ground makes recourse to Art. 6(1)(f) GDPR (legitimate interests) or Art. 6(1)(a) GDPR (consent) unnecessary. This leads to the accusation from data protection authorities and members of the data protection community that companies relying on Art. 6 (1) (b) GDPR could undermine data protection. Companies are accused of trying to circumvent the purportedly "proper" and "correct" standards of data protection. Behind this is the notion that data protection consent is the "gold standard" of effective data protection. The following article challenges this view. It is based on the thesis that effective data protection in contractual relationships can and must be realized above all through an appropriate design of the contractual relationships. A consent requirement downstream of the conclusion of the contract does not strengthen the digital autonomy of the data subjects, but ultimately contributes to its weakening. The level of protection envisaged by Article 8 CFR cannot be achieved by constantly increasing the number of consent requirements in the digital world - this only leads to "consent fatigue". The article describes in detail which specific requirements arise from this for the understanding of Art. 6(1)(b) GDPR.

Table of Content

I. Subject, Scope and Research Question*

The General Data Protection Regulation (GDPR)[1] sets forth that a justification is required for a company (the "controller"[2]) to process personal data. The list of justification grounds in Art. 6 (1) GDPR is exhaustive. Art. 6 (1) (b) GDPR provides that the controller acts justifiably if the processing of personal data is necessary for the performance of a contract to which the data subject is party.[3] The use of this legal justification ground makes recourse to Art. 6 (1) (f) GDPR (legitimate interests) or Art. 6 (1) (a) GDPR (consent) unnecessary. This leads to the accusation from data protection authorities and members of the data protection community that companies relying on Art. 6 (1) (b) GDPR could undermine data protection. Companies are accused of trying to circumvent the purportedly "proper" and "correct" standards of data protection. Some data

---

* This study is based on preliminary work by the author (Verfassungsblog.de, October 18, 2022 (https://verfassungsblog.de/dig-aut-contr-rel/); EU Law Live Weekend Edition No 129, February 2023 (https://issuu.com/eulawlive/docs/weekend_edition_129). It was inspired and supported by the Computer and Communications Industry Association (CCIA).

[1] Official Journal of the EU (OJ) 2016, L 119 p. 1. See, e.g., *Spiecker Döhmann/Papakōnstantinu/Hornung, et al.,* General Data Protection Regulation. Article-by-Article Commentary, 1 ed. 2023; *Hornung/Papakōnstantinu/Spicker,* European General Data Protection Regulation. Article-by-Article Commentary, 2022; *Krzysztofek/Behlert/Paszkowski,* GDPR personal data protection in the European Union, 2021; *Feiler/Forgó/Nebel,* The EU General Data Protection Regulation (GDPR): a commentary, 2 ed. 2021; *Vrabec,* Data subject rights under the GDPR – with a commentary through the lens of the data-driven economy, 2021; *Lynskey,* The Foundations of EU Data Protection Law, 2015. Important German publications on the subject: *Wolff/Brink/Albers,* Datenschutzrecht. DS-GVO, BDSG, Grundlagen, bereichsspezifischer Datenschutz: Kommentar, 2. ed. 2022; *Sydow,* DS-GVO, BDSG Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: Handkommentar, 3 ed. 2022; *Gola,* Datenschutz-Grundverordnung VO (EU) 2016/679 –Bundesdatenschutzgesetz. Kommentar, 3 ed. 2022; *Paal/Pauly/Ernst,* Datenschutz-Grundverordnung - Bundesdatenschutzgesetz, 3. ed. 2021.

[2] See Article 4 (7) GDPR: "controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law".

[3] Art. 6 (1) (b) GDPR also sets forth that the processing shall be lawful "in order to take steps at the request of the data subject prior to entering into a contract".

protection activists are talking about a "bypass" of EU data protection standards.[4] The argument that can be heard again and again is that if Art. 6 (1) (b) GDPR allowed data processing beyond the scope of what is technically indispensable for the performance of a contract (e.g., data identifying the contracting subject, his or her address, credit card information to process payments and ship goods bought online), companies would be undermining the alleged consent requirement[5] by providing for certain data processing in the contract. It is further claimed that this would degrade the meaning of Art. 6 (1) (a) GDPR and an erosion of EU data protection standards.[6]

This position that consent is a superior legal basis is explicitly or implicitly shared by many data protection authorities. In 2019, the European Data Protection Board (EDPB) used it as the underlying understanding for the development of its guidelines on the interpretation of Art. 6 (1) (b) GDPR.[7] In these guidelines, the scope of Art. 6 (1) (b) GDPR is interpreted in an overtly restrictive manner. It is also implicitly reflected in a Binding Decision issued by the EDPB on December 5, 2022.[8] A similar view is expressed in an Opinion presented by Advocate General *Rantos* in October 2022.[9] He seems to be of the opinion that the data subject is always in a better position if he or she consents to data processing. Conversely, the same data processing based on a contractual agreement would always put the data subject at a disadvantage. For him, it is

---

[4] See, e.g., the view of NGO noyb: https://noyb.eu/en/irish-dpc-greenlights-facebooks-gdpr-bypass.

[5] It must be noted that Art. 6(1)(a) GDPR and 6(1)(b) GDPR are not the only two options. Legitimate interest, for example, is also a viable option for many companies, including those providing personalized online services described throughout.

[6] See *Riehm,* Freie Widerrufbarkeit der Einwilligung und Struktur der Obligation - Daten als Gegenleistung? in: Pertot (eds.), Rechte an Daten, ed. 2000, p. 185.

[7] *European Data Protection Board*, Guidelines 2/2019 on the processing of personal data under Art. 6 (1) (b) GDPR in the context of the provision of online services to data subjects, 8 October 2019, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

[8] *ibid.*, Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR), 5 December 2022, https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-32022-dispute-submitted_en.

[9] Opinion of Advocate General Rantos, 20 September 2022, C-252/21, Meta Platforms Inc./Bundeskartellamt, EU:C:2022:704.

therefore obvious to keep the scope of application of Art. 6 (1) (b) GDPR narrow and to rely primarily on the data subject's consent to process personal data (Art. 6 (1) (a) GDPR).

The supporters of this view see themselves obliged to restrict the explicit wording of Art. 6 (1) (b) by means of rather daring constructions and interpretations. Occasionally, they even try to marginalise contracts as a legitimate ground for processing, alleging that its use may be unfair and unjust both in terms of business ethos and legal policy. One has the impression, however, that these actors approach Art. 6 (1) (b) GDPR predominantly with a preconceived notions of legitimate data processing, without considering the purpose of the nature of data protection and its relationship with other fundamental rights. This then results in knee-jerk reflexes and defensive posturing in order to prevent controllers from using this provision. There is often no careful holistic consideration of what the right to data protection envisaged in Art. 8 (1) of the Charter on Fundamental Rights of the EU (CFR) actually entails.[10] It is striking to see the lack of consideration to EU and Member States contract law as an appropriate vehicle to protect personal data. Furthermore, the potential advantages or drawbacks of placing too much emphasis on consent, and whether this aligns with individuals' expression of their digital autonomy, are not subjected to careful analysis or debate. Digital autonomy should not and cannot be limited and restricted merely to the decision of the data subject to release digitally encoded information (or the underlying digital symbol sets) via the granting of consent and, if necessary, to withdraw it by revoking it. Simply limiting the exercise of digital autonomy to the act of granting and, if needed, revoking consent would be too simplistic both in terms of data protection theory and in practicality.

In the meantime, more thoughtful observers are beginning to have doubts about the extent to which obtaining more and more consent rights actually improves individuals' digital autonomy in the emerging digital society. With the exponential growth of consent boxes in recent years, there is no denying that consent is routinely given without thoughtful deliberation of the outcomes and advantages of the choice. This is especially

[10] In the following, the provision of Art. 16 (1) TFEU, which is identical to Art. 8 (1) CFR, will not be cited.

true in a situation in which the consent requirements are regularly exercised mechanically and without in-depth rational consideration of the consequences and benefits of the decision. In the meantime, an open and interesting discussion has broken out at the level of data protection theory about what the goal of effective protection of personal data must be and what follows operationally from this. It has become clear that there is a wide divergence of views.[11] Some authors are calling for the creation of an EU "data market regulation"[12]. Others call for a deeper discussion about what a good life in a digital world can look like.[13] In this context, it should be clear that ultimately everyone must develop and realize their own ideas here and that governmental paternalism is inappropriate in a liberal community. These discussions have now also reached the theory and doctrinal construction of the GDPR. One sees the need to think more deeply, perhaps even anew, about other grounds for justifying the processing of personal data under Art. 6 (1) GDPR, beyond Art. 6 (1) (a) GDPR. These efforts have now reached the Court of Justice of the EU (CJEU): In Case C-300/21, Advocate General *Campos Sánchez-Bordona* made statements on the underlying values and goals of data protection theory that are highly relevant for the interpretation of Art. 6 (1) (b) GDPR.[14] The Advocate General openly questioned the widespread understanding of data protection as "control".

At the same time, it is easy to see that many data protection players do not want to face up to this discussion. They cling to their old ideas and ingrained preconceptions. It is not always clear whether this unwillingness is due to lack of interest in data protection theory or ignorance of contract law realities. There is some evidence to suggest that institutional and disciplinary interests are also at stake: while the interpretation and

---

[11] *Cohen*, Harv. L. Rev. 2013 (126), 1904; *Mulligan/Koopman/Doty*, Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 2016 (374), ; *Gstrein/Beaulieu*, Philos Technol 2022 (35), 3. As to different views about a data protection "theory of harm": *Solove/Citron*, Tex. L. Rev. 2018 (96), 737; *Citron,* The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age, 2022.
[12] *Peitz/Schweitzer*, NJW 2018 275; *Schweitzer*, GRUR 2019 569; *Steinrötter*, Recht digital 2021 (1), 480.
[13] *Cohen,* Configuring the Networked Self, 2012; *Cohen*, Theoretical Inquiries in Law 2019 (20), 1.
[14] Opinion of Advocate General Campos Sánchez-Bordona, 6 October 2022, C-300/21, UI/Österreichische Post, EU:C:2022:756.

application of Art. 6 (1) (a) GDPR is entirely in the hands of data protection authorities and the data protection community, the application of Art. 6 (1) (b) GDPR ought to bring contract law experts into play. The data protection community loses part of its decision-making competence and may find itself exposed to competition that it must distrust, if only because EU and Member State contract law and its interpretation are based on an independent legal culture distinct from the prevalent data protection doctrine. The price for fending off contract law experts from this discussion is high for is high, however: data protection authorities try to compensate for weaknesses in contract law by affording excessive and misplaced priority to Art. 6 (1) (a) of the GDPR. They fail to recognise that in doing so they are reducing the data subject's expression of his or her digital autonomy into a single, blunt form: "notice and consent".[15]

The CJEU is currently dealing with the question of whether the view developed by the EDPB and shared by many data protection activists is in line with EU law. In the *Meta Platforms v. Bundeskartellamt* case, the referring Higher Regional Court in Düsseldorf raised, among other things, questions regarding the interpretation of Art. 6 (1) (b) GDPR.[16] As mentioned, Advocate General *Rantos* submitted his opinion on 20 September 2020.[17] The decision of the CJEU is expected in the near future. The CJEU must also deal with the scope of Art. 6 (1) (b) GDPR in a reference procedure initiated by the Austrian Supreme Court.[18]

The following article attempts to determine the position of the provision of Art. 6 (1) (b) GDPR in EU data protection law. The article is explicitly not guided by the idea that "notice and consent" alone serves data subjects and the expression of their autonomy in the digital world. It also rejects the notion that 21st century data protection law should still rely decisively on the principle of "data scarcity." This is the idea that every form of data processing is fundamentally questionable and that the aim should be to achieve a

[15] For a precise doctrinal analysis of the content requirement, see *Leitner,* Das Rechtsinstitut der Einwilligung im Datenschutzrecht im Lichte der DS-GVO, 2021.
[16] OLG Düsseldorf, 24 March 2021, Kart 2/19 (V).
[17] See Opinion of Advocate General Rantos, 20 September 2022, C-252/21, Meta Platforms Inc./Bundeskartellamt, EU:C:2022:704.
[18] The proceedings are registered by the CJEU under No. C-446/21.

situation in which personal data is not processed to the greatest possible extent.[19] Anyone who reads Art. 5 GDPR closely will see that the European legislator has not codified this principle. The goal of the GDPR is not to establish rules for the past but rather to set up a suitable legal structure that accommodates the political, socio-cultural, and economic progression towards a digital society in the 21st century. It does not make sense to interpret the provisions of the GDPR against the realities of the emerging societal and economic structures. Actually, this should also be clear to the members of the data protection community: five years after the GDPR came into force, large parts of the population do not feel that they have been truly empowered by the GDPR. Rather, fatigue effects triggered by the myopic use of the "notice and consent" principle can be seen. By interpreting the provisions of the GDPR in light of the realities of a modern digital society, this article responds not least to accusations that the GDPR reflects an outdated or obsolete data protection philosophy.[20] Instead, a forward-looking and contextualized interpretation of Art. 6 (1) (b) of the GDPR[21] makes it possible to keep pace with the developments of Europe's digital society while fully respecting individuals' digital autonomy and all their other fundamental rights.

The political and legal dispute about the interpretation of Art. 6 (1) (b) GDPR mainly revolves around three business models and the accompanying contractual relationships between a data processing company and an individual. First, there may be contracts that

---

[19] Until a few years ago, the question of how to avoid data collection was a weighty academic topic (see, e.g., *Weiß/Reisener*, ZInsO 2017 (20), 416). In the meantime, the discussion has turned around: People are discussing how to eliminate the problems of data scarcity: *Ladeur*, DuD 2016 (40), 360; *Brillowski/Overhage/Tegetmeyer-Kleine, et al.,* Overcoming Data Scarcity in the Quality Control of Safety-Critical Fibre-Reinforced Composites by means of Transfer and Curriculum Learning in: Herberger/ Hübner (eds.), Proceedings of the Conference on Production Systems and Logistics, ed. 2022, p. 83.

[20] See, e.g., *Leistner/Antoine/Sagstetter,* Big Data Rahmenbedingungen im europäischen Datenschutz- und Immaterialgüterrecht und übergreifende Reformperspektive, 2021, p. 401: "In designing the GDPR, instead of responding to technological and societal developments, in many cases the EDPB relied on decades-old principles and tenets that are only partially supportive of today's practice." (My Translation).

[21] With regard to a flexible interpretation of the GDPR, allowing for diversity, see *Veit,* Einheit und Vielfalt im europäischen Datenschutzrecht, 2023.

enable the controller to process data as the main service; such contracts may be concluded for altruistic reasons, but may also be driven by an economic interest. Second, the contract may provide that the controller is allowed to process personal data in order to personalise its main service.[22] Third, the contract may provide that the processing of data is enabled as a contribution to the consideration of the contract. It is conceivable that the contractual authorisation of data processing and the resulting creation of personal profiles reduces the actual monetary price to be paid by the data subject (e.g., in the case of insurance services). It is also conceivable that a service can be offered free of charge because the profile is used to display personalized advertising (such as behavioral advertising). This opens up a wide range of possibilities - from the reduction of the monetary price actually envisaged, to the development of "freemium" models, to the provision of offers financed completely by advertising.

The wording of Art. 6 (1) (b) GDPR does not provide for any restrictions on the right of companies and individuals to conclude contracts on the use of data or contracts about the provision of services that require the use of data.[23] The legal question this paper explores is whether there are systematic, teleological, or other legal reasons to adopt a restrictive (reductive) reading of Art. 6 (1) (b). On the part of many data protection authorities, the general view is that this is the case. On the one hand, it is argued that certain contracts (and the business models which rely on those contracts) as such must be excluded entirely from the scope of application of Art. 6 (1) (b) GDPR. The EDPB took this view in Binding Decision 3/2022 that business models which finance free services via behavioral advertising can have no place in Art. 6 (1) (b) GDPR. The EDPB argued in the abstract: It made no empirical analysis of the effects of behavioral advertising on the data subjects, nor did it allow for any differentiations. At least from the point of view of data protection theory, it would be conceivable to consider the composition, age and education of the clientele, the preferences of the clientele, the type and effect of the advertising, etc. The EDPB claimed that the business model *as such* had to be rejected. On the other hand, many data protection authorities argue that the necessity test

[22] Personalization of the offering can be observed not only among retailers in the digital economy, but also among service providers (e.g., search engines, social networks).
[23] In the legal literature, it is disputed whether contracts that provide for digital services in exchange for personalized advertising can be based on Article 6 (1) (b) of the GDPR.

provided for in Art. 6 (1) (b) GDPR must not refer to the contract actually concluded; the point of reference must be a (possibly idealized and hypothetical) contract that a consumer with the same perspectives and biases as the DPAs "ideal consumer" would or should have concluded.[24]

To sum up: The following article aims to expand the discussion about Art. 6 (1) (b) GDPR by questioning certain assumptions of data protection theory, such as the notion that data protection is best achieved through consent requirements and the understanding that the justification ground of contractual agreement is by nature and in all cases inferior. In a first step, it will be shown that the GDPR aims to establish a regime that is both empowering and protective. On the one hand, the GDPR is about contributing to economic and social integration as a consequence of a functioning internal market. On the other hand, it is about preserving an adequate level of protection for the data subject. The GDPR has dual functionality (see II. below). For the interpretation and application of provisions such as Art. 6 (1) GDPR, it is therefore crucial to understand the essence of the protection sought in Art. 8 (1) CFR is (see III. below). The interpretation of the justification grounds of Art. 6 (1) GDPR must also not be pursued in introverted isolation, but must take into account the primary law environment, especially the relevance and meaning of all relevant EU fundamental rights. This forces the conclusion that Art. 6 (1) (b) GDPR must be understood literally and does not allow for a restrictive interpretation (see IV. below). From this, doctrinal conclusions can then be drawn for the interpretation of Art. 6 (1) (b) GDPR (see V. below). The article builds on two blog posts by the author.[25]

[24] The EDPB speaks in Guidelines 2/2019, para. 32, of the standard of "reasonable view of the data subject when concluding the contract".
[25] *Nettesheim*, Digital Autonomy in Contractual Relationships (Verfassungsblog, 18 Oktober 2022) <https://verfassungsblog.de/dig-aut-contr-rel/>; *ibid.*, EU Law Live 2023 (129), 3.

II. The GDPR as an instrument of enabling and protection

The GDPR simultaneously serves the purpose of enabling the use of data and the purpose of introducing appropriate data protection. The GDPR serves a dual-function . It takes up the regulatory mandate that was established by the treaty-maker in Art. 16 (2) TFEU, i.e. the requirement to achieve the "free movement of data" and the protection of individuals are mentioned with equal priority. As a consequence, the GDPR is already misconstrued in its basic approach if it is only understood as an instrument to prevent or suppress the use of (personal) data to the greatest possible extent.

1. Dual functionality of the GDPR: Freedom of data flows and data protection

The GDPR has two intertwined regulatory objectives.[26] Art. 1 (1) GDPR, which in this respect implements Art. 16 (2) TFEU, indicates that the subject matter and objective of the Regulation is not only "the protection of natural persons with regard to the processing of personal data". The equally important second objective of the Regulation is to establish rules "on the free flow of such data". This two-pillar structure of the GDPR is already expressed in the title of the regulation; it is also reflected in the further paragraphs of Art. 1 GDPR. Here, on the one hand, the protective aim and concern of the GDPR is specified by establishing a reference to the fundamental rights and freedoms of the data subjects (Art. 1 (2) GDPR). On the other hand, the importance of the "free movement of personal data within the Union" is also emphasised (Art. 1 (3) GDPR). This wording would be misunderstood if it referred only to the flow of data across Member State borders. Unlike the EU fundamental freedoms, EU secondary law

[26] *Sattler,* Personenbezug als Hindernis des Datenhandels in: Pertot (eds.)*,* Rechte and Daten, ed. 2020, p. 49: „With the General Data Protection Regulation (GDPR), the European legislator has responded to the ubiquitous processing of personal data. In the public debate, the focus is currently predominantly on the protection of personal data and the privacy of data subjects. In this respect, there is a risk that the second regulatory purpose of the GDPR will be pushed into the background. Recital 2 p. 2 and Art. 1 I 2, III GDPR already emphasize that the GDPR should at the same time promote the free movement of personal data in the internal market. This dichotomy of comprehensive protection of personal data and adaptation of the legal framework for intra-European data traffic is a challenge." (my translation).

measures to order markets and protect consumers always apply to purely domestic situations, unless they indicate a divergent decision by the European legislator. The European Court of Justice recently stated this explicitly for the Services Directive.[27] The GDPR does not indicate that it intends to address this issue differently. There is no sensible reason to assume that the GDPR is concerned with the cross-border flow of data,[28] but at the same time wants to exclude the flow of data within the Member States from its scope. On the contrary, provisions such as Art. 20 GDPR (right to data portability) make it clear that it deals with both cross-border situations and purely domestic situations. It is true that the European legislator was and is motivated by the need to eliminate differences in the level of data protection between EU Member States (recital 9 of the GDPR). However, the choice of an EU regulation as the legislative instrument makes it clear that both the protective and the liberalizing elements of the GDPR are not only concerned with situations of cross-border data processing.[29] The free flow of personal data is considered so important that data protection concerns cannot justify a general restriction or prohibition in principle.

This two-pillar structure of the GDPR is also described in the recitals. Recital 4 states that the processing of personal data should be "in the service of mankind". Here, the GDPR rejects a one-sided perspective according to which combating and restricting the processing of personal data is above all else. Rather, it soberly states, "The right to protection of personal data is not an unrestricted right; it must be seen in light of its social

---

[27] CJEU, 30 January 2018, C-360/15 and C-31/16, College van Burgemeester et al., EU:C:2018:44, with regard to chapter III of the Directive 2006/123/EC.
[28] With regard to third country data traffic: *Drechsler*, PinG 2022 (10), 24; *Fazlioglu,* The United States and the EU's general data protection regulation in: Cortez (eds.)*,* Data protection around the world, ed. 2021, p. 231; *Gerhalter,* Internationale Datentransfers im Lichte der DSGVO und der DSRL-PJ, 2021; *European Academies*, International sharing of personal health data for research, EASAC policy report 41, 2021, https://easac.eu/fileadmin/PDF_s/reports_statements/Health_Data/2021_ALLEA_EASAC_FEAM_Policy-Report_International_Sharing_Health_Data_en.pdf.
[29] *European Commission*, 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) (SEC(2012) 72 final), 2012, https://www.europarl.europa.eu/cmsdata/59702/att_20130508ATT65856-1873079025799224642.pdf.

function and weighed against other fundamental rights in compliance with the principle of proportionality." The twofold objective of the GDPR was already present in the genesis of the GDPR. The EU Commission had spoken of the goal of strengthening the data economy when it presented the first draft of a data protection regulation.[30] In the initial proposal, a reference to the value the digital economy was included.[31] Accordingly, the provisions of the GDPR have a dual function.

It is also recognised in the case law of the CJEU and in academic literature that there is a dual objective behind the provisions of Union law on data protection, which requires a balance between the concern for the efficient use and free movement of data on the one hand and the requirement for an adequate level of protection on the other. [32] In the

[30] See Reding, Viviane, The upcoming data protection reform for the European Union, International Data Protection Law 2011 (1), 3 et seq.; Reding, Viviane, The European data protection framework for the twenty-first century, International Data Protection Law 2012 (2), 119 et seq.; Reding, Viviane, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age, Speech 22 January 2012, https://ec.europa.eu/commission/presscorner/api/files/document/print/en/speech_12_26/SPEECH_12_26_EN.pdf; see also European Commission, EU - Communication Comprehensive approach on personal data protection in the EU, COM/2010*/0609* final.

[31] *ibid.*, Proposal for a Regulation of the European Parliament and 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) (COM/2012/011 final), 2012, https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf, p. 2: „This is why it is time to build a stronger and more coherent data protection framework in the EU, backed by strong enforcement that will allow the digital economy to develop across the internal market, put individuals in control of their own data and reinforce legal and practical certainty for economic operators and public authorities."). It is interesting to see that the aim of building a digital economy is mentioned in the first place.

[32] Advocate General Tizzano, 14 November 2002, C-465/00, C-138/01 and C-139/01, Österreichischer Rundfunk et. al., EU:C:2002:662, para.53; Advocate General Tizzano, 19 September 2002, C-101/01, Lindqvist, EU:C:2002:513, para. 42; in agreement: *Lynskey,* The Foundations of EU Data Protection Law, 2015., p. 60; for a plurality of purposes, taking into account the interests of data processors and the internal market reference: *Klement*, JZ 2017 (72), 161 (162).

academic literature, it is said that the goal of establishing a functioning internal data market and the goal of an adequate level of data protection are of equal importance. [33]

It is thus implicit in the provisions of the GDPR that its goal is to contribute to the emergence of a digital society in which the economic value of data can be realized, however without falling below a level of data protection that complies with the requirements of Art. 8 CFR.[34] The GDPR does not oppose the creation of economic value from data. Rather, by implication, generating economic wealth from data is one of their goals, on the premise that an adequate level of protection is not undercut.

On the basis of this understanding, guided by Art. 16 (2) TFEU and Art. 1 GDPR, the provisions of the GDPR fit seamlessly into the broader political context. The institutions of the European Union have long been engaged in legally facilitating and promoting the upcoming digital transformation of European society. This is not just about securing a level of European prosperity that enables natural persons in the EU to live a good life in autonomous freedom. It is also about unlocking the potential of the digitisation of governmental governance structures and the societal environment for the individual's realization of their conception of a good life. Entrepreneurial freedom is mentioned in the fourth recital of the GDPR. In more recent legislative proposals, the importance of the free movement of data is reiterated. For example, in recital 10 of Regulation (EU) 2018/1807[35] on a framework for the free flow of non-personal data in the EU ("Free-flow Regulation"), the EU legislator emphasises that "Regulation (EU) 2016/679 provides that Member States shall neither restrict nor prohibit the free flow of personal data within the Union for reasons connected with the protection of individuals

[33] *Hacker*, DGRI-Jahrbuch 2021 (2019/2020), 281. Hacker emphasizes that the assessment that ensuring the free flow of personal data is the "main objective" of the DSRL can be found above all in the older CJEU judgments. He points to CJEU, 20. May 2003, C-465/00, C-138/01 and C-139/01, Österreichischer Rundfunk et al., EU:C:2003:294, para.70, and CJEU, 9 March 2010, C-518/07, Commission/Germany, EU:C:2010:125, para. 20.

[34] Obviously, the balance between the two goals must be found on a situation-specific basis in each case; in this regard, EU fundamental rights provide important normative guidelines.

[35] Regulation (EU) 2018/1807 of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ 2018 L 303/59.

with regard to the processing of personal data. This Regulation establishes the same principle of free movement within the Union for non-personal data, except where a restriction or prohibition is justified on grounds of public security. Regulation (EU) 2016/679 and this Regulation form a coherent set of rules aimed at the free movement of different types of data. Moreover, this Regulation does not require that different types of data be stored separately."

In fact, the legislator of the GDPR opted for a regulatory approach that is also inherent in general EU consumer protection law. Here, too, it is a question of simultaneously realising market openness, economic efficiency and an appropriate level of protection. The CJEU has emphasised that EU consumer contract law seeks to strike a balance between a high level of consumer protection and the economic freedom of market players. In the April 7, 2022 judgement, it emphasised the need to "ensure, in interpreting the provisions of Directive 2011/83, a balance between a high level of consumer protection and the competitiveness of undertakings, as is apparent from the fourth recital in the preamble to that directive, while respecting the entrepreneurial freedom of the contractor as guaranteed by Art. 16 of the Charter of Fundamental Rights."[36] (para. 31).[37] This right to balance different concerns is clearly also included in the GDPR.

So far, however, this dual function of the GDPR has not really been sufficiently developed, both in practical application and in the academic discussion. While the CJEU, for example in "Google Spain",[38] recognises the need to interpret European data protection law in light of conflicting fundamental rights, including the individual freedoms of the controller, and does not attempt to deny the liberalising and enabling dimension of the regulation in principle, the goal of establishing data markets simply goes unnoticed in many EDPS and EDPB documents. This also applies to documents that explicitly deal with the position of data processing companies in the market. For instance, in the already mentioned Guideline 2/2019, the normative principle of free flow of data is not given a single word. In the academic discussion, the picture is mixed. In some academic

[36] CJEU, 7 April 2022, C-249/21, Fuhrmann-2-GmBH, :EU:C:2022:269, para. 31, with reference to CJEU, 10 July 2019, C-649/17, Amazon EU, EU:C:2019:576, para. 44.
[37] Similar approach in: CJEU, 5 May 2022, C-179/21, Victorinox, EU:C:2022:353.
[38] CJEU, 13 May 2014, C-131/12, Google Spain, EU:C:2014:317.

publications on the GDPR, the dual function of the GDPR is indeed addressed in analyses of Art. 1 GDPR. However, when examining other provisions, it is then regularly lost sight of. This is especially true for analyses of Art. 6 (1) GDPR: here, it has not yet been possible to incorporate the dual function of the GDPR into the interpretation and application of the different grounds of justification in a structured and appropriate manner.

One can only speculate about the reasons why the GDPR's decision in favour of value creation based on free data markets is often not taken note of in data protection discussions. It may be because it does not fit into the basic ideological understanding of the discussants. But it may also be due to the view that the establishment of free data markets undermines data protection as understood in terms of "personality" rights.[39] In particular, contributions from the German-speaking data protection world continue to be strongly influenced by a specific construction of the German constitution developed by the German Federal Constitutional Court in the 1980s. These contributions openly or implicitly attempt to "Germanize" the GDPR. The specific context in which the German Federal Constitutional Court developed its construction at the time is not seen, or is deliberately eliminated. The orientation towards a certain data protection philosophy is so strong that it is supposed to take precedence over the explicit order in Art. 16 (2) TFEU and in the stipulations of Art. 1 GDPR set forth by the EU legislator. As a result, this leads to interpretations and applications that can only view data protection one-sidedly from a reductive protection perspective, which can easily turn into a siloed approach.

These efforts to reduce the meaning and content of the GDPR must be rejected. The GDPR must not be reduced to the isolationist according to which the GDPR merely focuses on the protection of individuals' data. Such a view would clearly contradict both

[39] The term and the concept behind it are highly ambiguous. This is all the more true when it is linked to the idea of human dignity (see, e.g., *Floridi*, Philosophy & Technology 2016 (29), 307). It seems as if those who invoke the "personality function" of data protection primarily want to ward off a commercialization of personal data. However, no justification is given for why this contradicts the essence of human personality, especially if it is done voluntarily. Rather, it seems to be a matter of protecting a certain ethical image of the human being. These images, however, are of a highly particularistic nature.

Art. 1 (1) GDPR and the general purpose of the regulation. The interpretation of any provision of the GDPR (including Art. 6 GDPR) must be guided by the twofold objective of the European legislator to simultaneously protect individuals' data and to further the free movement of data.

2. Market regulation for personal data in compliance with the protection standard pursuant to Art. 8 (1) CFR

The GDPR is an instrument of market regulation law insofar as it regulates legal relationships in dealing with personal data. Data are means of storage, transmission and processing of information.[40] Data protection is concerned with sets of symbols from which information can be obtained on a semiotic, syntactic and semantic level.[41] The scope of application of the GDPR is defined by a semantic criterion (identifiability of a person). Symbol sets are only relevant in terms of data protection law insofar as they enable the generation of "information relating to an identified or identifiable natural person" (Art. 4 (1) GDPR). The GDPR does not regulate the generation and use of digital symbol sets per se, but only if they have a (potential) information content relating to a natural person. As Art. 4 (1) GDPR makes clear, the GDPR can only be meaningfully understood if it is seen as part of a legal *information order* in which the relevant fundamental rights are sufficiently realised.

The interpretation of the GDPR must therefore be guided by the goal of contributing to the establishment of an *information order* that is both effective and normatively appropriate. To reiterate, this includes a sufficient level of protection (Art. 8 (1) CFR). Individual provisions of the GDPR must not be removed from this context and isolated. However, the basic structures of a digital data economy, in which it is generally recognised that personal data (can) be commercialised, have yet to be described in terms of data protection law. The tendency to characterise the commercialisation of data as unethical or immoral per se (often, indeed, against the preferences of data subjects who decide otherwise) finds no support in EU law. It is almost paradoxical when, on the one

[40] See *Zech,* Information als Schutzgegenstand, 2012.
[41] On the various mappings of data, information, and knowledge: *Zins*, Journal of the American Society for Information Science and Technology 2007 (58), 479.

hand, it is emphasis ed that economic value creation in late-modern European societies takes place primarily on the basis of information - and, on the other hand, the position is taken that personal information is to be treated as *res extra commercium* when it is digitally encoded. As is well known, the EU legislator sees this differently: Directive 770/2019/EU[42] provides for a special consumer protection right for contracts for digital content, and this also applies when the consumer "pays" with data.[43] I will come back to that later. Even if an explicit formulation to this effect has been deleted from the text of that directive: the substance remains the same.[44] There is no point in turning a blind eye to this. And it is even more pointless to pursue an interpretation of the GDPR that is fundamentally opposed to these developments.

Probably the greatest legal, political and socio-cultural achievement of the GDPR is to have established that the initial collection and all further processing of personal information requires a specific justification (Art. 6 GDPR). However, this principle would be misunderstood if it were interpreted to mean that the conclusion of agreements on the economic use of data should be prohibited as a matter of principle, or even just reined in by regulation. Art. 6 (1) (b) GDPR makes it clear that the contract (in addition to consent) is a hierarchically equivalent instrument for overcoming the statutory restriction

[42] Directive (EU) 770/2019 of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, OJ 2019 L 136/1.
[43] The EU legislator rightly assumes that there is no need for special (consumer) protection if there is no contract at all or no (monetary or data-related) consideration. However, undertakings which contractually undertake to provide a "digital product" is subject to specific obligations. A consequence of the (limited) protective purpose is that Directive 770/2019 does not apply if the entrepreneur only collects data in order to be able to perform the contract. The Directive does not specify which forms of processing can be contractually agreed and thus justified under Art. 6(1)(b) GDPR. It only regulates what applies in the case of action according to Art. 6(1)(a) (cf. e.g. § 327q German Civil Code (BGB)).
[44] See Directive (EU) 770/2019, recital 24: "Digital content or digital services are often supplied also where the consumer does not pay a price but provides personal data to the trader. Such business models are used in different forms in a considerable part of the market. While fully recognising that the protection of personal data is a fundamental right and that therefore personal data cannot be considered as a commodity, this Directive should ensure that consumers are, in the context of such business models, entitled to contractual remedies."

on processing. This is also reflected in Art. 8 (2) CFR, which does not give consent a special status of legitimacy .

The GDPR would therefore be misconstrued if it were to be understood as a lever with which action could be taken in a fundamental way against the emerging "information market structures" and the actors involved, especially companies processing data. Recent EU legislation makes it clear that data and information markets are to be systematically expanded - both for non-personal data and for personal data. These markets should be efficiently organised and at the same time provide an adequate level of protection for personal data in accordance with the requirements of Art. 8 (1) CFR.[45] It is not surprising that conflicts of interest and normative disputes arise in this context. There is no difference in information markets than in other markets.

The creation and design of a "information market order" in which the allocation and use of digitally encoded information is regulated in an expedient, effective and normatively appropriate manner is rather presuppositional because there is a lack of reference standards or direct points of connection. The emergence of a digital society has no models. How information is allocated here, who can dispose of or access it and how, and what fair compensation should look like, raises new decision-making problems that have never had to be answered before. The necessity of a context-specific development of (sub-)elements of a digital information order[46] suggests to orientate on corresponding

[45] See, e.g. *European Commission*, A European Strategy of Data (COM/2020/66 final), 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066. The analysis of the legislative acts of the EU institutions gives a good picture of how they understand the protective content of Art. 8 CFR. See, e.g. Regulation (EU) 2018/1807 of 14 November 2018 on a framework for the free flow of non-personal data in the EU, OJ 2018 L 303/59; Regulation (EU) 2022/868 of 30 May 2022 on European Data governance, OJ 2022 L 152/1; Proposal for a Regulation on harmonized rules on fair access to and use of data (Data Act), COM/2022/68 final (critical evaluation: *Kerber*, GRUR International 2022 (72), 120).

[46] So *Nissenbaum,* A contextual approach to privacy online in: Savirimuthu (eds.)*,* The library of essays on law and privacy. Part 3: Security and privacy, ed. 2015, p. 32 et seq. See also *Schafer,* Of wicked wizards and indigo jackals: Legal regulation of privacy and identity in cultural comparative perspective in: Buchner/ Petri (eds.)*,* Informationelle Menschenrechte und digitale Gesellschaft, ed. 2022, p. 27 et seq.

contexts in the analog world. Even if it can be observed in the meantime that individual provisions of EU law are turning to the topic of establishing "information markets", the ultimate structures to be aimed at are rather unclear on a theoretical level and politically. If an informational practice can be regarded as both effective and appropriate in the analog world, it is in any case worth considering whether it should not also be made possible in digital spaces.[47] In many areas, however, there are no patterns of orientation to which one could refer.

3. Necessity of interpreting Art. 6 (1) GDPR in light of its dual function

Legal practice and academia are thus faced with the task of developing an interpretation of the provisions of the GDPR that is appropriate to the dual function of the GDPR. This also applies to Art. 6 (1) GDPR. A myopic approach that makes one of the legal bases absolute, declares it to be decisive for all or even just the primary ground, or attempts to marginalise other grounds, is inadmissible in terms of legal methodology and inappropriate in terms of legal policy. At the same time, each of the justifications must be tailored to contribute to the establishment of effective and normatively adequate data markets and to ensure an appropriate level of protection there. This requires a context-dependent approach. When it comes to the relationship between the state and its citizens, different values must be applied than in horizontal relationships between private companies and individuals; this is reflected, for example, in Art. 6 (1) (e) GDPR. In cases involving the allocation of information and the handling of information in contractual relationships, different values must be applied than in cases where third parties (outside of contractual relationships) access personal data. Even within contractual relationships, data protection law sits within a broader regulatory context, as it is only one element of an encompassing system of market regulation law. This system includes general contract law with its consumer protection content,[48] competition law, and other

[47] This is one of the thesis of *Nissenbaum,* A contextual approach to privacy online in: Savirimuthu (eds.), The library of essays on law and privacy. Part 3: Security and privacy, ed. 2015, p. 32 et seq.
[48] In this context, a distinction must be made between contracts that make the processing of data the (main) subject matter of the contract, contracts that specify data as a

regulatory rules (e.g. the Digital Services Act). Data protection law is market regulation law and a regulatory instrument under economic law - it must be aligned with other applicable legal instruments, in particular with private contract law.[49]

The literature of information philosophy and information sociology has long recognised that the allocation of information and the ordering of access to or the transferability of information within different social relations and with regard to the different types and contents of information (also within the group of personal information) must be decided in its actual context. There would be no need to emphasise it here if the tendency to an isolationist approach were not repeatedly apparent in legal discussions on data protection law. It is not inaccurate to speak of a "siloed mentality" that amounts to protecting data while ignoring the concrete societal, economic and political context. In many cases, data protection positions are one-sidedly oriented toward the ideals of the 1970s, invoke the ideal of a world in which natural persons can return to informational anonymity at any time, and therefore place consent (which can be revoked at any time) at the centre of the legal protection of human autonomy in the digital society.[50] This ideal may have had its justification vis-à-vis the data-collecting state of the late 20th century: Liberal state theory is based on the premise that the state should, in principle, stay out of natural persons' lives. Even then, however, it was inappropriate for describing the horizontal social relationships of natural persons in society. Even more so in the digital society of the 21st century, it can no longer serve as a normative model for the legal structure of the legal status of natural persons in their relationships with fellow citizens and companies.

4. The GDPR as Market Regulation Law: Equal Value of Contract and Consent

The above considerations were aimed at elaborating that the discussion on data protection theory and data protection law must open up to the insight that data protection law is about the regulation of information markets. The GDPR sees itself as a regulatory

consideration, and contracts that cover data as a mere ancillary service. EU consumer contract law does not extend to contracts that cover data only as an ancillary service.

[49] The courts regularly assume (at least in Germany) that the use of search engines (e.g. Google) or the use of a social network (e.g. Facebook) is on a contractual basis.

[50] See, e.g., *Beaulieu/Leonelli,* Data and Society: A Critical Introduction, 2021.

instrument with which digitally encoded information can be managed effectively and in a normatively appropriate manner, i.e. in compliance with the level of protection set forth in Art. 8 (1) CFR. The GDPR opposes the idea of the public domain of personal data (in other words: information about individuals): without justification, the processing of personal data is prohibited. It then establishes a nuanced system of information use: Art. 5 (1) GDPR obliges lawfulness, transparency and fairness. Art. 5 (2) and (3) GDPR obliges the determination of a specific, explicit and legitimate data processing purpose and prohibits the collection of data that is not necessary for purposeful processing. The GDPR cannot, however, be understood as intending to make the processing of personal data generally scarce or to push it back.

When enacting the GDPR, the EU legislator decided to place the contract (Art. 6 (1) (b) GDPR) and consent (Art. 6 (1) (a) GDPR) on an equal footing as instruments of market regulation. This is based on legal policy insights according to which open data markets (Art. 16 (2) TFEU) will not function without contractual agreements. At the same time, the EU legislator has been guided by the insight that the autonomy of natural persons can be realised particularly well in contracts. This does not mean that a Wild West mentality should prevail in the markets envisaged by Art. 16 (2) TFEU or that the law of the strongest should apply (nor does GDPR facilitate that). The EU legislator made the decision to place contract and consent on an equal footing in the knowledge that Member State contract law will ensure fairness and justice. For this very reason, however, it is impermissible to interpret Art. 6 (1) (b) GDPR in a reductive or restrictive manner or even to marginalise it.

The market regulation element of the GDPR breaks down into three sub-areas. First, Art. 6 (1) GDPR shows that market actors operate in a framework that incorporates mandatory EU or Member State law (Art. 6 (1) (c) GDPR) and the realisation of public interest objectives (Art. 6 (1) (e) GDPR). In these cases, the data processing is legitimized by EU law, without regard to the will or the specific and concrete interests of the data subject. On a second level, there is Art. 6 (1) (b) GDPR and Art. 6 (1) (a) GDPR, which aim to give effect to the legal or quasi-legal will of the data subject. On a third level, there are then those provisions that declare the specific and concrete interests of

the persons involved to be decisive (Art. 6 (1) (d) GDPR on vital interests of the data subject or another person; Art. 6 (1) (f) GDPR on overriding interests of the controller or a third party). The GDPR thus makes it clear that it is not wedded to a one-sided ideology that bases the management of digitally encoded information solely on the formal subjective will of the data subjects as expressed by explicit consent. Material interests count. However, in cases where the data subjects have expressed their will under contractual law, there is no reason to base the order directly on interests. There is no reason to give more weight to the expression of an individual's will under Art. 6 (1) (a) GDPR than to his or her will expressed by concluding a contract under Art. 6 (1) (b) GDPR . From the point of view of data protection theory, Art. 6 (1) (b) GDPR takes precedence over the justification grounds of Art. 6 (1) (d) GDPR and Art. 6 (1) (f) GDPR

III. The Construction of Data Protection: Right to arbitrary control or right to unharmed digital sociality?

1. Data protection law as part of an information order

In the 21st century, one of the significant challenges for the legal system is to establish rules that operate alongside the existing laws protecting goods and the freedoms of individuals.[51] An order for the allocation of public or private goods and the handling of these goods has always existed. Likewise, there has long been an order for the assignment and allocation of competences and freedoms of action. A *general order for information* does not yet exist. There is yet to be a comprehensive set of laws and regulations that govern the use and handling of digital information in various social fields. The emergence of an information society, in which digitally encoded information (i.e. data) is becoming ubiquitous and the number of social fields in which no information is generated will continue to decline, makes it necessary to create such a corpus of laws and regulations that is both general and sufficiently concrete. There are individual pockets in modern law where rights about information are conceived (e.g. intellectual property law). Beyond these islands, the questions of how to assign rights about information in a way that is both effective and fair have not really been answered or resolved. This requires a legal and political discussion which is still in its infancy today, as evidenced by the debate that has broken out in many social fields about appropriate standards for the assignment of information. The EU is in the process of creating regulations on the allocation and use of information in a whole series of legal acts.[52] The regulatory regime governing Europe's digital society is expected to be as multi-layered and complex as the laws and regulations governing goods and individuals' freedom in the physical world.

Data protection law is an important element of an effective and appropriate channel to govern the use of digitally encoded personal information. However, it would be overestimating its possibilities if it claimed to be able to establish the legal order for the entire

[51] See the analysis of *Klement,* JZ 2017 (72), 161.
[52] For an overview: https://www.europarl.europa.eu/factsheets/en/sheet/64/eine-digitale-agenda-fur-europa.

digital society on its own. Such a claim, however, can be observed among some data protectionists. They believe they can solve the problem with (apparently) simple principles. Some do this by treating information, or the personal data behind it, as a commodity that can be assigned property-like or ownership-like assets ("My data belongs to me"). These proposals obviously borrow from principles of goods allocation. The others try to make information the subject of individual freedom and work towards subjecting information (and the data behind it) to subjective free will ("I have a right to control my data"). Both approaches reveal the extent to which the paradigms of the non-digital world ("ownership" or "control") are used to meet the challenge. Neither approach does justice to the task of developing an appropriate legal order for digitally encoded personal information, because information is not a commodity and cannot be made the subject of freedoms and competencies without context and further differentiation.

The difficulties that exist in formulating appropriate standards of allocation, freedoms and responsibility in the area of digitally encoded information are expressed in the wording of Art. 8 (1) CFR. The authors of the Charter of Fundamental Rights clearly indicate that they do not intend a property-like attribution of personal information.[53] Nor did they establish a right to control personal information. Instead, Art. 8 (1) CFR states that every person has "the right to the protection of personal data concerning him or her." What this protection should look like in detail is not specified. The first sentence of Art. 8 (2) CFR only stipulates that the processing of data may only be carried out "fairly for specified purposes" and "with the consent of the person concerned or some other legitimate basis laid down by law". The provision thus leaves largely open what

[53] The Drafters of the Charter of Fundamental Rights of the European Union do not refer to the idea of "data as property" in their explanations (see: Explanations relating to the Charter of Fundamental Rights, 2007/C 303/02, OJ 2007 C 303/17, Explanation to Article 8. This idea was also of no relevance in the deliberations of the drafting convention. The discussion about "data ownership" cannot be reproduced here (see, e.g., *Bauer/Fuhr/Heynike, et al.,* Risikofeststellung Dateneigentum in: Datenschutz (eds.), Dateneigentum und Datenhandel. DatenDebatten Band 3, ed. 2018, p. 15; *Amstutz*, AcP 2018 (218), 438; *Hummel/Braun/Dabrock*, Philosophy & Technology 2021 (34), 545; *Black*, Ind. L. Rev. 2022 (54), 305; *Cofone*, Cardozo L. Rev. 2021 (43), 501; *Jurcys/Donewald/Fenwick, et al.*, Harvard Journal of Law & Technology Digest 2021 3; *Thouvenin*, JIPITEC 2021 (12), 246.

function data protection has in the context of a digital society, and what its form and essence are.

A meaningful interpretation of Art. 6 (1) GDPR will only succeed if it is first clarified what the "protection" envisaged by Art. 8 (1) CFR should look like. Like any secondary law, the provisions of the GDPR must be read in light of EU primary law. None of the provisions of the GDPR may be interpreted in a way that falls short of the level of protection envisaged by Art. 8 (1) CFR. This also applies to the interpretation and application of Art. 6 (1) GDPR. However, the other elements and provisions of EU primary law, such as the regulatory mandate of Article 16 (2) TFEU and the liberal fundamental rights and freedoms of the persons concerned, must also be taken into account.

In the following, the widespread thesis that data protection must mean “data control” will first be described and criticised (see 2. below). Subsequently, a more adequate model of appropriate data protection will be presented, which is linked to the sociality of human life in social communities. The model ties in with recital 4 of the GDPR, according to which data protection must be viewed "in light of its function in society" and be balanced against other fundamental rights, in accordance with the principle of proportionality (see 3. below).

2. Data protection as "control": Protection of the informational free will

At the heart of the "control theory" that continues to be widespread in data protection communities is the view that data protection aims to give natural persons the broadest possible "control" over the personal data that concerns them. This view has left its mark on the GDPR; it can be based in particular on recital 7 of the GDPR ("Natural persons should have control over their own data."). It is also influencing the work of the data protection authorities in the EU. Under this theory, consent under Art. 8 (2) CFR and Art. 6 (1) (a) GDPR becomes the primary ground for processing personal data, and all other grounds recognised under the Art. 8 (2) CFR and Art. 6(1) GDPR are deemed secondary.

a) Focus of data protection on information control

At the heart of the "control theory" is the view that data protection law must establish and confer rights upon the data subject that give comprehensive control options over the use of personal information by third parties. The fundamental right to data protection under Art. 8 (1) CFR is therefore understood as conferring on the data subjects a legal status that is primarily constituted by a right to oppose the use of his or her personal information by the state or other private actors. From the point of view of fundamental rights theory, Art. 8 (1) CFR must thus be understood as creating subjective rights, the purpose and nature of which is the empowerment of subjective free will. However, the aim and expression of this right are not actions of the data subject, but the suppression of the actions of others. Art. 8 CFR is interpreted as a right to exercise freedom of choice for or against a controller and third party's data processing, rather than a right to control one's own actions. From this perspective, data protection law is thus about introducing a specific form of informational power in informational relationships, whereby the optimal legal implementation of the fundamental right to data protection is achieved by creating "notice and consent" rules to the greatest possible extent, enabling the data subject to assert which of his or her personal data is processed and used by whom. Data protection by consent is declared to be the fundamental characteristic of effective data protection; the extension and multiplication of "notice and consent" requirements is considered to be the silver bullet of informational empowerment of the data subject. As a consequence, consent as a ground for processing recognised in the first sentence of Art. 8 (2) CFR is given normative primacy over other legal bases .

This basic position is currently held by the European Data Protection Board (EDPB), for example. The EDPB argues that data processing that is not based on "notice and consent" *deprives* the data subject of his or her rights. The EDPB seems to assume that processing on the basis of consent is, from the point of view of legal legitimacy, of the highest order; all other processing seems to be subordinate in the EDPB's view. A similar basic position can also be found in the opinion of Advocate General *Rantos*, who also seems to assume that the effectiveness of data protection is primarily expressed in the number of "notice and consent" activities. Some members of the data protection

community go so far as to see consent as an inherent and quasi-natural right of the individual, which itself overrides the entire wording of Article 8 (2) CFR. For this position to hold, the right to accept or reject the processing of personal data personal data seems drawn from natural law, which belongs to the individual *qua* human being. Typically, those who subscribe to this view will argue that data processing which has already been contractually agreed upon be further justified with an additional "notice and consent" layer . This, however, is not the view of the drafters of the EU Charter of Fundamental Rights or the GDPR. They have ensured that the controller has at his disposal various means of justification for the processing of personal data, which are hierarchically similar and of equal legitimacy. Recently, the efforts to cope with the developments of the digital society by imposing ever new and additional legal requirements have been described as a form of "Kabuki theatre"[54].

b) Individualism, data minimisation, anonymity

If the fundamental right to data protection, and the information order that is to be build upon it, are reconstructed entirely or predominantly from the perspective of the individual's right to control his or her personal data, this implies that the essence of data protection is allowing individuals to exercise their own subjective free will. Self-determination under data protection law means retaining control over digitally encoded information, and that the data subject is able at any time to force controllers and third parties to delete the information concerning him or her. This understanding of self-determination implies the right of the data subject to be able to disengage from informational contexts at any time and to return to a sphere of informational isolation. The idea of self-determination under this data protection philosophy is thus reconstructed in individualistic and isolationist terms.

[54] *Cohen,* Between truth and power the legal constructions of informational capitalism, 2019, p. 59: "… the lawyerly emphasis on such things as disclosure, privacy dashboards, and competition over terms becomes a form of Kabuki theater that distracts both users and regulators from what is really going on."

Often, this understanding of the nature of data protection is combined with a substantive statement: the less data about a person is in the hands of controllers and third parties, the better (principle of data scarcity).[55] This postulate is not logically connected with the notion of data protection through the empowerment of free will, but it regularly goes hand in hand with it. An individualistic, freedom-oriented ideal then takes on an isolationist character. According to this view, the ideal state of affairs in terms of data protection law is only achieved when controllers, processors and third parties have as little personal data as possible.

c) Weaknesses and deficits

The basic position described above has considerable weaknesses and deficits from the perspective of fundamental rights theory.[56] If data protection is understood as a concern that can be constructed from the isolated individual, it is a matter of subjective free will - and thus of an (apparent) empowerment of the individual. The construction is based on the construction of civil liberties, but then focuses on controlling the actions of third parties. However, the allocation of information in social relations between natural or legal persons cannot be unilaterally made solely the subject of one parties' mercurial free will. In such relationships, when one side has or wants to gain information about the other, it is always a matter of social relations involving two or more actors. Regardless of whether provided data, observed data, derived data or inferred data is at issue:[57] Information is always relational. Any understanding of data protection that seeks to grant the data subject informational dominion over third parties does not do justice to the nature of information. Moreover, this conception of data protection law and its focus on "notice and consent" instruments is individualistic, solely exclusionary and negatory,

[55] See text at footnote 19 above.
[56] These weaknesses have repeatedly been discussed. See, e.g., *Solove,* The meaning and value of privacy in: Roessler/ Mokrosinska (eds.), Social Dimensions of Privacy: Interdisciplinary Perspectives, ed. 2015, p. 71; *Pearce*, Inf. Commun. Technol. Law 2018 (27), 133.
[57] See *Organisation for Economic Cooperation and Development. Working Party on Security and Privacy in the Digital Economy*, Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking, 21 May 2014, https://one.oecd.org/document/DSTI/ICCP/REG(2014)3/en/pdf.

and does not provide any real power of negotiation. It certainly does not provide comprehensive digital autonomy. And it does not reflect questions of justice and fairness.[58] In the German language context, it is often referred to as a "personality rights approach". Ultimately, however, this is wrong: the legal protection of free will, subjective in informational relationships, is not about protection of the human "personality", at least not in a meaningful and informed sense.

The approach described above is also deficient in the sense that it construes effective data protection without taking into consideration the broader context and the concrete socio-informational environment. The individual is seen as an isolated nomad - without taking into account his or her social position and without considering the fact that the individual's social environment and the individual himself or herself may have legitimate interests in having controllers and third parties provide information to the individual.

Another weakness of the approach described above is that it forces unjust exaggerations and distortions.[59] Anyone who understands the individual right to data protection as a quasi-natural right of the individual assumes that this right cannot be waived and that data cannot therefore become the subject of economic activity. The literature speaks of a "fundamental rights approach" that implies "that 'data protection automatically trumped other interests and could not be traded-off for economic benefits.'"[60] Data protection tailored to isolated subjective free will thus become the highest-ranking super fundamental right that is supposed to supersede all other interests. This is a strange contrast to the wording of the Charter of Fundamental Rights, where the right to data protection (Art. 8 (1) CRF) is not only one of many other fundamental rights, but is also designed in a special way: It is to be implemented by the EU legislature and thus gives lawmakers wide discretion to design its implementation. The extreme radicalisation of this position is reached when, on the one hand, it is claimed that natural persons have a comprehensive right of control over the personal data concerning them and, on the other

[58] *Braun/Hummel*, Cell Patterns 2022 (3), 1 et seq.
[59] *Ferretti*, Common Market Law Review 2014 (51), 843 (852).
[60] *Ausloos/Mahieu/Veale*, JIPITEC 2019 (10), 283 (306).

hand, it is asserted that all personal data are goods that are "extra commercium" and therefore cannot be commercialised.[61] According to this view, all personal data should be treated as goods that cannot be traded in the market.[62] Only in very rare instances can we find laws which regulate such goods (e.g. human body parts etc.).[63] Whoever applies this approach for all personal data in the sense of the GDPR shows an uncompromising radicalism that can only seem alienating in the 21st century. Anyone who thinks historically will also recognise that it will not be possible to sustain this position. On this point, data protection law is about to reach a dead end.

---

[61] See *European Data Protection Supervisor*, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, 17 March 2017, https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf ("The EDPS reaffirms that he welcomes the intention of the Commission to protect consumers even in cases where they did not pay a price for the digital content received. However, as explained, one should avoid treating personal data as a commodity as any other, for reasons mentioned above."); *European Data Protection Board*, Statement 05/2021 on the Data Governance Act in light of the legislative developments, 19 May 2021, https://edpb.europa.eu/system/files/2021-05/edpb_statementondga_19052021_en_0.pdf , p. 4: "Indeed, considering that data protection is a fundamental right guaranteed by Article 8 of the Charter, and taking into account that one of the main purposes of the GDPR is to provide data subjects with control over personal data relating to them, the EDPB reiterates that personal data cannot be considered as a "tradeable commodity". An important consequence of this is that, even if the data subject can agree to the processing of his or her personal data, he or she cannot waive his or her fundamental rights."; *European Data Protection Board - European Data Protection Supervisor*, Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), 4 May 2022, https://edpb.europa.eu/system/files/2022-05/edpb-edps_joint_opinion_22022_on_data_act_proposal_en.pdf, para. 15: " The EDPB and the EDPS are concerned that the Proposal in its current text would extensively push a development towards "commodification" of personal data, whereby personal data are seen as a mere tradeable commodity. This would not only undermine the very concept of human dignity and the human-centric approach the EU wants to uphold in its Data Strategy, but it would also risk undermining the rights to privacy and data protection as fundamental right." The attempt to mix the question of the commercialization of data with the question of the possibility of waiving fundamental rights must be surprising.

[62] For a description of the current discussion, see *Nolin*, Journal of Information, Communication and Ethics in Society 2019 (18), 54; *Fierens/Ooms*, Personal data as a commodity: is the door open for small-scale data processing? (KU Leuven CiTiP 4 August 2022) <https://www.law.kuleuven.be/citip/blog/personal-data-as-a-commodity-is-the-door-open-for-small-scale-data-processing/>.

[63] For an ethical examination of the limits of markets: *Sandel,* What money can't buy. The moral limits of markets, 2013.

As has already been said, this conception of data protection law is led by many data protectionists on the basis of the theory of natural law. Natural persons are supposed to be entitled to data protection control by virtue of their mankind. There is not enough space here to explore in depth the question of why such quasi-naturalistic attributions can be observed in data protection law - a modern fundamental right - while in other areas there has long been a shift to a functionalist interpretation of fundamental rights. The presumption is that it is a rather clumsy and desperate attempt to eliminate supposed weaknesses of the fundamental right to data protection by recourse to a rock-solid construction in human nature; allegedly. The theory of Natural Law applied to data protection might nonetheless be relevant for safeguarding some limited sensitive information like genetic data of a person. But it becomes disproportionate when it is extended to all "personal data" in the sense of Art. 4 (1) GDPR. One cannot have both at the same time: an enormously broad scope of protection extended to all personal data, and a legal construction that is based on a natural law understanding and does not allow for trade-offs.

3. Data protection and digital sociality: the function of data protection in society as a whole

The essence of data protection can only be meaningfully described if one assumes that natural persons live in social communities that are constituted by each actor having knowledge about other actors. This is true for the realm of non-digital relationships; there is no reason to see it differently for relationships in which digital information is held at the ready. The information order of the digital society must reflect the fact that information about natural persons is regularly relational in nature: It enables one side to form a picture of the other side. In social relationships, it is the prima facie right of each side to form a picture of the other side. In these relationships, no one can claim to have comprehensive control over the other side's informational knowledge. For centuries, the law has protected spatial spheres in which natural persons can exercise control, including informational control ("spatial privacy").[64] In detail, constitutional law and human rights documents provide for different protection of “spatial privacy”. For example, the 4th Amendment of the U.S. Constitution differs in protection from Article 12 UDHR or

[64] See, e.g., *Solove*, U. Pa. L. Rev. 2006 (154), 477.

Article 10 ECHR. All documents have in common that they actually provide for control of the holder of fundamental rights in the premises considered to be “private”. On the other hand, as far as life outside these spaces is concerned, it is a social fact and the expression of normative standards that the social counterpart can gain information about the person. This was and is true of life in the non-digital community; it must therefore also apply to natural persons' lives on digital social platforms and on the websites of service providers. Outside the spaces protected by (spatial) privacy, no human being can meaningfully claim to gain comprehensive control over the image that the other side forms about him. This is also true when it comes to digitally encoded information. To the extent that users of digital services go to websites or download apps, they are traversing through other peoples' property (servers) which must necessarily affect their expectation of privacy. When a data subject uses a social network, he or she is moving in a space that a private company has built. Anyone who sees this differently wants to ascribe to human beings a claim to dominance over the other side, which runs counter to any form of sociality.

For this view, data protection cannot be understood as the protection of subjective freedom of will, even at a principled level. Rather, this view assumes that data protection must guarantee informational conditions that correspond to the functional information needs and the justified normative protection expectations of the socially interacting actors. These conditions include that the individual human being suffers no "harm" from the collection and use of personal information by a third party (principle of non-harm). This view ties in with recital 4 of the GDPR, which states that the right to protection of personal information must be "seen in the light of its social function." It is therefore "not an unrestricted right". According to this view, the essence and function of data protection cannot be inferred solely from the individual and its will. Rather, data protection must be understood as part of the information order in society as a whole and must gain its meaning from this perspective.

a) Data privacy as an integral part of an information order

In the course of the 21st century, essential structures of the social sphere will undergo fundamental change. Today, it is clear that there are socio-cultural structures within

which human beings' life will be "datafied" in a fundamental way and thus rewritten. Digital technologies make it possible to open up new social spaces; they open up new possibilities for communication and action and thus create the socio-technical environment for new ways of life. The emerging structures will change the way we live in much the same way as the abundant availability of energy and the spread of machines did in the industrial age more than a century ago.

Information is at the centre of the emerging digital society. The functional requirements for effective and normatively appropriate information management have changed fundamentally in the course of the digitization of more and more areas of life. From the point of view of law, a central political concern in the coming decades must be the creation of an efficient and normatively appropriate information order. Deciding what an information order of the 21st century should look like is first and foremost a political question that must be decided in democratic procedures. Politics decides in an environment that is shaped by historical lines of development, by conventions, by socio-cultural patterns of meaning, but also by values, interests and visions of the future. The novelty and peculiarities of digital social structures make it sometimes questionable to adhere to the standards of the past. On the other hand, as far as these standards embody principles, values and socio-cultural patterns that we want to protect in our trajectory, they deserve to be used in the development of the new digital information order. In a pluralistic society, such values, interests and socio-cultural patterns diverge significantly among the members of the political community. This applies not only to the area of privacy: Here, highly particular views can be observed about what is to be assigned to the area of privacy and is therefore worthy of protection. It applies to the same extent to the handling of (personal) information. The cost benefit calculations in this regard differ widely among human beings. It is by no means the case that digitization as such and the services and business models made available on the market are a cause for concern for everyone. Even though it has become popular to describe the emerging digital society in dystopian terms, almost everyone accepts the new services voluntarily. They obviously see a benefit in this that outweighs any possible disadvantages. In any case, the dystopian formulations and horror scenarios developed by some political actors are obviously self-serving; in some cases, they are also developed against the manifested interests and

views of natural persons. It is exceedingly paradoxical that a world whose benefits are voluntarily sought by a large majority of natural persons has for some years been described as a dystopian hell by others. Obviously, these descriptions are semantic artifice with which the data protectionists understand themselves to be in a position to help and protect, or paternalize, the data subjects, depending on one's view. In some cases, natural persons who use (and want to use) the allegedly dangerous services are dismissed as unreasonable, or at any rate as unenlightened. The problem of such semantic and socio-cultural argumentation strategies is particularly obvious when certain services and business models are condemned across the board without any consideration of the specific details.

Any form of legal data protection (like the comparable concept of legally protected "spatial privacy") can only gain its proper meaning and adequate function in specific social relations.[65] There is no way to talk about appropriate "spatial privacy" in a supra-temporal way or without reference to a specific socio-cultural context. Nor can notions of data protection be ahistorical or deculturalized. Rather, concepts of privacy and data protection are relational, contextual, socio-culturally encoded, and must be thought of in concrete spatial or informational terms. In legal terms, this means that the decision as to whether a particular digitally coded piece of information is assigned to a person must always take into account the interests and values of the data-processing counterpart (relationality). The legitimacy and value of the mutual claims in an information order can only be determined with a view to specific socio-cultural and socio-political situations (contextuality). What is to be regarded as an impermissible encroachment on the "right to informational self-determination" is subject to historical changes and can change over time (historicity). The decision whether and how to assign rights to information (or to the underlying data) must be guided by a variety of aims, purposes and functional considerations (teleological functionality). In this context, it is not only the goals, purposes, and interests of the personally affected individual that are important, but also the concerns of third parties and the public interest. The interests of the controller, third parties and the general public must be given equal weight, as recital 4 of the GDPR emphasizes. The individual's interest in secrecy or control must therefore be set against other

[65] *Cohen,* Theoretical Inquiries in Law 2019 (20), 1.

legitimate goals and interests (efficiency and prosperity; security, protection and health; individual benefit and convenience, etc.). The respective social views on the respective rights and powers in an information order are primarily encoded in social views and norms. They can be codified by the legislator in positive law - and thus also changed legislatively. With the enactment of the GDPR, for example, the EU legislator has determined that personal data must not be conceived of as an "almende"[66] and that the processing of personal data is not "public domain" but requires a specific justification. The notion of who has what rights and powers in an information order that is both effective and fair are strongly influenced by legislation.

The legal architecture of a digital society that enables natural persons to live a good life in freedom and prosperity must be multi-layered and complex. There are no *a priori* rules about how information should be managed in human society. Thus there are also no *a priori* rules about who should have which rights to a certain piece of information. This is already true for spatial spheres, where "privacy" standards are subject to political contestation and are therefore in fluidity. Spatial areas that were considered the object of "privacy" protection a few decades ago have lost this qualification. On the other hand, existing spaces were given new and additional protection through new safeguards, for example against illegal electronic spying. These observations are even more true for the information order of the public sphere and of digital spaces established by private companies. The information order of these areas must be able to accommodate and process conflicting interests - it cannot be constructed from only one perspective (such as the perspective of the subjective free will of individuals). It will not be possible to realize it even at the outset if individual goals, values or interests are made absolute or if specific elements are taken out of context. For the law, the challenge is to define a normative framework that allocates appropriate space to the various interests, each of which is justified in its own right.

---

[66] Data as „almende" have repeatedly been discussed with regard to non-personal data (see *Bertschek/Bonin/Kühling, et al.*, Entwicklung eines Konzepts zur Datenallmende. Erstellt im Auftrag des Bundesministeriums für Arbeit und Soziales <https://www.bmas.de/SharedDocs/Downloads/DE/Publikationen/Forschungsberichte/fb-581-entwicklung-eines-konzepts-zur-datenallmende.pdf?__blob=publicationFile&v=2>).

As a consequence, data protection cannot be pursued in isolation, but must be understood as part of an information management system that allocates information and information generation possibilities.[67] The allocation can be based, for example, on the act of scripting (symbolization of the data),[68] the reference of the data to an individual person, economic usage interests, public welfare concerns and the like. It is all about valuations that do not follow from the nature or the essence of a data or a data set. Rather, the allocation decisions must be made functionally and justified normatively.[69] The judgment as to how to design a data protection regime that is at the same time efficient, normatively appropriate, and politically wise can therefore only be made with a view to the goals and values that the information order as a whole is supposed to satisfy.

If data protection law is understood as the law of information management, it is not difficult to see where the challenge lies in the interpretation of the GDPR: It is about developing an order of the data economy that allocates competences, freedoms and rights to information in a way that is compatible with our ideas of an efficient and just model of society (Art. 2 TEU). The allocation to be made in this context concerns, on the one hand, information extraction possibilities; on the other hand, it is about the allocation of information that has already been generated, including the related possibilities of use.[70] To emphasize it clearly: An information order which understands human beings as socially integrated persons cannot do without duties and prohibitions, rights and competences, also in dealing with information. Just as it classifies certain spheres as "private" and then establishes rights of control and exclusionary rights for the private sphere, it can also provide for "control" of the data subject in certain public spaces. However, it is crucial, firstly, that the decision on information management must always (also) be

---

[67] See above III. 3.
[68] According to *Zech,* Daten als Wirtschaftsgut – Überlegungen zu einem „Recht des Datenerzeugers“ in: Wimmers/ Metzger (eds.), DGRI Jahrbuch, ed. 2015, p. 1, the act of scripting should determine the allocation of data.
[69] See *Thouvenin/Weber/Früh,* Data ownership: Taking stock and mapping the issues in: Dehmer/ Emmert-Streib (eds.), Frontiers in Data Science, ed. 2017, p. 111, 123 et seq.
[70] Even if the immediate point of reference is data, the starting point for data protection law is always the semantic information. This is because the decision as to whether something is personal data can only be made at the semantic level.

thought of from the perspective of society. Secondly, contextual differentiations are required in order to do justice to the diversity of the respective situations. The GDPR must not be interpreted from a siloed perspective, but must be read in its overall societal context. There cannot be a general right to “control” of personal information in the public sphere.

b) The basic structure of the GDPR

Effective data protection means contributing to the basic conditions that a person must have in order to lead a good or successful life in the digital society. The starting point for thinking about effective data protection must therefore be natural persons' lives in the digital society. The authors of the GDPR were clearly aware of these interrelationships. As already mentioned, they emphasize in recital 4: "The right to protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights in accordance with the principle of proportionality." This formulation combines a number of statements that are on different levels. Some concern the nature and function of data protection, others the legal status of the subjective right. The decisive point is the following: The attempt to tear the EU data protection regime out of its larger contexts and subject it to a siloed treatment is explicitly rejected. The EU legislator makes it clear that an information order (and the data protection scheme contained therein) can never be developed exclusively from the perspective of the isolated individual, but must always be developed from the concept of human sociality. Data protection is ascribed a "social function" from which it must be interpreted. It is exceedingly striking that this basic decision of the EU legislator has never played a role in the work of the EDPB, which is entirely driven by the idea of informational free will. It is not clear whether it is overlooked or deliberately suppressed.

The CJEU's jurisprudence also reflects the view that the function and place of data protection can only be developed from the perspective of society as a whole. In its judgment of January 12, 2023, the CJEU states that "the right to the protection of personal

data - as is clear from the fourth recital of the GDPR - is not an absolute right."[71] Indeed, as the CJEU essentially reiterated in its judgment of 16 July 2020[72], that right must be seen in the light of its social function and weighed against other fundamental rights in compliance with the principle of proportionality." A similar view was already found in the judgment of July 16, 2020.

The notion that data protection can be reduced to "control" or is in any case substantially realized through "control" is now also being rejected in the EU institutions. Advocate General *Campos Sánchez-Bordona* recently explicitly opposed the idea that data protection amounts to granting data subjects "control" over their personal data to the greatest possible extent.[73] In his opinion, the assessment that appropriate data protection cannot be reduced to "control powers" but requires the creation of an environment in which data subjects can assert their digital autonomy, is reflected.

The EU legislator and the CJEU have thus made it clear that the question of the legal efficiency of a data protection regime cannot be determined "from within the individual". They make it clear that this can only be done against the background of well-founded views about a good or successful life of the individual in the social community. Data protection law must process individualistic and community-oriented, as well as personality-oriented and economic value orientations, interests and preferences of natural persons on an equal footing. One must think of data protection and its function from the perspective of society; this does not preclude thinking of digital sociality from the perspective of a data protection model that empowers and emancipates the individual. It is time for data protection authorities and control-focused data protectionists to apply recent data protection theory to their interpretation of Art. 8 CFR and Art. 6 GDPR.

Data management regulations such as the GDPR set out normative guidelines and rules that are based on values about how natural persons can and should live a good life in the

[71] CJEU, 12 January 2023, C-154/21, RW/Österreichische Post AG, EU:C:2023:3, para. 47.
[72] CJEU, 16 July 2020, C 311/18, Facebook Ireland and Schrems, EU:C:2020:559, para. 172.
[73] See footnote 14 above.

digital world (individual perspective). They also always formulate an ideal of the sociality of a person in the digital community (societal perspective). The drafters of the GDPR recognized the need to always read the law simultaneously from an overall societal *and* an individualistic perspective - unlike some of the current exegesis. They have also seen that data protection law will only be able to develop an appropriate overall picture if it understands performance expectations ("action structure") and factual allocations ("possession structure") in context. In concrete terms, this means that it does not make sense to assign digitally encoded information to the data subject for arbitrary disposal if there is no question that the state and the digital companies will only be able to fulfill the performance expectations placed on them by making considerable use of personal information.

c) Socially integrated and self-determined life in a digital society

The concept of self-determination (under data protection law) can thus not be understood in an individualistic-isolationist way. Self-determination must be understood (in general, but also in contexts relevant to data protection law) as the ability to lead a life that is both autonomous and integrated in a social community with others. Accordingly, the measure of self-determination is not the ability to prevent others from obtaining information about one's own person and to destroy the available information. Rather, "digital autonomy" means being able to live in a socio-technical ("digital") environment in which the necessary and sufficient conditions exist to realize an autonomously developed life plan. Obviously, the standards in this regard are highly dependent on the respective socio-cultural views at a certain moment in time.

However, certain structural aspects can be identified. This includes precautions to ensure that the processes of preference formation can take place in a sufficiently independent manner and are not exposed to inappropriate external influences (manipulation, pressure[74]) ("internal autonomy"). In addition, external conditions must be in place for the formed preferences to be realized ("external autonomy"). Moreover, this also means

[74] See *Hacker*, European Law Journal 2021 (Version Online), 1.

that conditions must exist in which processes of reflexive identity formation can take place.[75] It is one of the generally agreed insights of fundamental rights theory today that elements of social interaction and self-reflection are combined in these processes. Identity formation does not happen in a vacuum.[76] Heteronomy is the human condition. As a consequence, the fact that third parties have (and use) personal information does not cause any impairment *per se* - it is even a prerequisite for a socially integrated life, which necessarily includes an economic dimension and the interaction with commercial undertakings.[77] To see in this an unspecified potential for risk or danger, to which one reacts by establishing property-like rights of control in favour of the other side, seems paranoid. It cannot therefore amount to a fundamental claim to be able to control the image that others have of the person. Whoever claims to be able to determine in a social relationship what the other knows (or is allowed to know) about him, claims his subjugation.[78]

To develop and realize one's own life plan requires more, and other, than atomistic isolation. A successful life can only be led as a member of a community that is at the same

[75] Some authors summarize the various elements in a single term (e.g. "personality formation" etc.) In Germany, the Federal Constitutional Court has created a "general right of personality", which includes a wide variety of sub-positions (see: *Federal Constitutional Court,* Decisions of the Federal Constitutional Court. Volume 6: General right of personality, 1. Auflage 2022). However, it makes sense to distinguish between self-determined action, autonomy and identity formation.
[76] *Shoemaker*, Ethics of Information Technology 2010 (12), 3.
[77] Digital autonomy thus does not mean the empowerment to live in informational isolation or digital autarky.
[78] The "right to informational self-determination" developed by the German Federal Constitutional Court (Decisions of the Federal Constitutional Court, Vol.65, p. 1) can be applied coherently in the relationship between citizens and the state. In horizontal relations between private individuals, on the other hand, there can be no prima facie right of one side to be able to control (by analogy with property) the information obtained by the other side (see, e.g., *Solove,* Understanding Privacy, 2009). Some authors in Germany try to overcome the theoretical incoherence of a "right to informational self-determination" by admitting that the right is clearly "overshooting" its possibilities; at the same time, they claim that the construction can be saved in legal practice by engaging in balancing. The construction developed by the Federal Constitutional Court empowers courts to adjudicate all matters relating to the handling of digitally encoded information and gives them comprehensive supervisory powers - but at the price of blurring the difference between constitutional law and political decision.

time stimulating, inspiring and criticizing, in which one is confronted with the values, interests, systems of meaning and actions of others. Social interaction (including the resulting conflicts, impositions and restrictions) is as important as the provision of spaces of retreat ("spatial privacy"). The idea that one could ideally live in the emerging digital world without confrontation with the counterpart who has information about the other is based on a misunderstood atomistic individualism. The normative ideal of a life in which governmental authorities in principle have no information about the citizen (according to the data protection philosophy of the 1970s and 1980s) cannot simply be transferred to the horizontal relationships of the human being to his socio-cultural and economic environment. It is inconceivable to develop the normative ideal of a good life in which this environment has no information about a person, or at least the available information is beyond that person's control. Just as knowledge and information about natural persons exist in offline contexts, the basic normality of knowledge about natural persons must also be assumed in online contexts.[79]

Any information order (and its data protection dimension) must take as its starting point the relational quality of information from actors about other actors. What appears to be appropriate or even acceptable here is socially contextualized and changeable. Without contextualization, no appropriate standards can be formed. It thus depends on the type of information and the measure of information that third parties have at their disposal in order to be able to make a judgment as to whether the existence of information in the hands of the "other" is a matter of empowering or of impairing the individual subject. It also depends on the actions that are (expectedly or actually) taken on the basis of the information. In a close personal relationship, the appropriate level of information is inherently different than in commercial contractual relationships. Again, the situation is different when it comes to the behaviour on the part of third parties who analyse the actions of the data subject outside of a contractual relationship. Data protection theory has

[79] It must be emphasized that people must have spaces of retreat in order to find themselves (for example, *DeBrabander,* Life after privacy reclaiming democracy in a surveillance society, 2020 pp. 97 et seq.). These spaces of retreat must also be protected in the digital world, for example by prohibiting surreptitious intrusion, snooping or other illegitimate acquisition of information. However, this protection of privacy in the digital world is not the issue here. People who are socially active in the digital world (e.g., by using digital services) are not in a private space.

to take note of the fact that assessments now diverge widely as to whether third party knowledge is enabling or impairing. The extent to which views diverge can be seen, for example, in the differences of opinion that exist on the question of what can (or even should) be posted on a network and what it makes sense to keep to oneself. Even individual views have changed over time. The same applies to the offers provided as part of digital services: While some see personalized offers made in the knowledge of their preferences and interests as an enrichment because they amount to a pre-ordering and facilitate choice, others see this as an intrusion and interference with their claim to "privacy." The law must recognize this plurality of opinions; there is no way to define a "normal level" for data protection law. The data protection authorities' attempt to speak for "the people" seems a bit strange against the backdrop of the plurality of human views and the variety of conceptions of the good life in today's society. In none of its statements has the EDPB ever indicated that it is aware that it is making decisions in a pluralistic world. Rather, it seems to want to speak and decide for a completely homogeneous mass of human beings.

Digital autonomy thus requires the guarantee and safeguarding of conditions within which it is possible for natural persons to develop and implement their individual idea of the good life. Natural persons must be given the legal means to find recognition and empowerment as autonomous subjects in all areas of life. Those who see data protection law only as an instrument to enable natural persons to remain in digital anonymity will not be able to realize the emancipatory character of this legal instrument. Natural persons must also be given the opportunity for self-determination in the market. They must be empowered to dispose of their data autonomously in contractual relationships, depending on their individual value orientation, interest structure and order of preference. Anyone who sees the world of the data economy only from the perspective of individualistic-isolationist possibilities for withdrawal, is ultimately curtailing human autonomy - and not strengthening it. An "empowerment" that leads to socio-cultural isolation and cannot be used in an economically meaningful way does not bring about emancipation. EU data protection law is not based on a theory of normative individualism, which can be secured primarily by giving natural persons the right to suppress personal information (informational withdrawal from the social sphere). As a consequence, the ideal

of self-determination under data protection law will attribute a fundamental value, both in terms of data protection theory and legal legitimacy, to contractual agreements between the data subject and third parties about the use of personal data, the conditions of this use, and the benefits resulting from the use.

In any case, the above considerations should have made it clear that it would be a simplistic misunderstanding to believe that "one-size-fits-all" solutions are available in data protection law. This applies in particular to the idea that consent rights would optimize natural persons' self-determination under data protection law always and in all situations. The conclusion to be drawn is that the instrument of the contract must be seen as an important instrument for realizing digital autonomy in the digital space as well. However, a libertarian formalism that regards every contractual agreement as conducive to autonomy simply because it is based on the consent of both sides would be misguided. In view of specific data collection and use contexts, it is always necessary to clarify whether a contract is an expression of “material” contractual autonomy. As will be shown in the next chapter of this study, “material” autonomy will only be realized if the law provides for protective safeguards that make this possible. There has to be an appropriate legal response to concrete risks and dangers. In this context, contract law and data protection law should not be viewed in isolation, but rather in their interrelatedness.[80]

The above considerations were aimed to provide insights into data protection theory. First, it has been argued that the instrument of data protection must be understood as a component of an overall social information order. It has also been argued that the essence and function of data protection lies in guaranteeing certain conditions of social life for natural persons in the digital society. Data protection aims to make a good life in the digital society possible, but must also serve to protect against “digital harm”. In positive legal terms, this means that there is no reasonable reason to assume that the "notice and consent" principle of Art. 6 (1) (a) GDPR has a special or prominent place in the

[80] This systematic finding should not be confused with the question of whether a particular institution (data protection authorities, courts, etc.) has the legal authority to also use contract law when interpreting provisions of the GDPR.

system of justification grounds. Rather, the contract under Art. 6 (1) (b) GDPR is at the centre of the enabling (and emancipating) function of data protection.

IV. Data protection in contractual relationships: Art. 6 (1) (b) GDPR

The time of the 1970s and 1980s, when data protection was realized in the fight against an excessive "hunger for data" of governmental institutions, is long gone. In a society where digitality has become ubiquitous, very different and peculiar challenges arise. The challenge is to realize an architecture of digital spaces (and the markets built into them) that adequately accommodates a variety of concerns simultaneously: private autonomy that enables a good and self-determined life in a digital society; an effective market design that ensures a smooth operation and prevents abuse; entrepreneurial freedom that brings innovation and creates wealth; and fair allocation of the value embodied in data. As to the empowerment of the data subjects, the challenge will only be met by approaches that appropriately combine concern for non-economic interests, values and orientation patterns of the individual ("personality"), for economic interests (e.g. through property rights), and for socio-cultural and political interests of the data subjects. It is simply pointless to try to reduce the human being to one dimension in data protection law. Art. 6 (1) of the GDPR cannot be meaningfully interpreted if one (myopically) declares the atomistically conceived data subject and his free will to be the interpretative guideline. The legal challenge can only be met by recognizing the necessity of a superordinate approach in which (civil) society, the market, and the individual find their place.

The considerations set out under II. and III. should give rise to increased reflection on the legal framework conditions that enable the data subject to comprehensively realize his or her interests. This requires a comparative assessment of the various control instruments: contract, consent, weighing of interests, direct legal duties, and prohibitions.[81] Each of these instruments has a specific efficiency. Depending on the legal policy objective, each instrument has specific advantages and disadvantages. From the perspective of the data subject, too, the empowering and protective effects of the individual

[81] The many years of discussion on data ownership (cf. footnote 53 above) have shown that ownership constructions cannot cope with the problem of appropriate management of data in a digital society. Introducing ownership of digitally encoded information (or of the digital code itself) would not adequately solve the attribution problems.

instruments are not identical.[82] In particular, the empowerment and emancipative value of the instruments differs.

The theoretical, conceptional and general considerations under II. and III. make it possible to interpret Art. 6 (1) (b) GDPR in a way that is not burdened by unfounded presumptions. In the following, it will be explained that the provision has the same hierarchical rank in the system of justification grounds as Art. 6 (1) (a) GDPR (see 1. below). Digital contracts under Art. 6 (1) (b) GDPR allow the data subject to exercise digital self-determination in the exercise of private autonomy (see 2. below). A literal understanding of Art. 6 (1) (b) GDPR optimizes fundamental rights (see 3. below). The level of protection provided by Art. 8 (1) of the GDPR is also fully complied with under this understanding of Art. 6 (1) (b) GDPR (see 4. below).

1. Hierarchical position of Art. 6 (1) (b) GDPR in the system of justification grounds

Art. 8 (2) CFR stipulates that the processing of personal data requires a specific grounds of justification . The provision makes it clear that there may be other grounds for justification besides consent (which is explicitly mentioned). It indicates that they are of equal importance. Art. 8 (2) CFR thus makes it clear, firstly, that the protective level envisioned by Art. 8 (1) CFR is not only satisfied exclusively or primarily by means of consent requirements. Secondly, the provision makes it clear that the European legislator can implement the protection requirement set forth in Art. 8 (1) CFR in a different way than through the classic data protection consent ("notice and consent").

[82] It does not make sense to construct a conflict between a consideration oriented to personality and a consideration oriented to property interests (see *Peukert,* Güterzuordnung als Rechtsprinzip, 2013 , p. 4: "The prevailing opinion in the literature agrees and consistently concludes a (limited) transferability and attachability of asset components of the personal right corresponding to copyright. Thus, these unwritten rights have all the characteristics of copyright, which is recognized to constitute constitutionally protected property." (my translation).

This equivalence is reflected in the GDPR: In Art. 6 (1) GDPR, a total of six grounds for justification are placed next to each other, without establishing a legal hierarchy or an explicit or implicit normative precedence. The understanding that the justification grounds are hierarchically of equal rank also corresponds to the understanding of the EU legislator.[83] Even the data protection authorities claim to share this view, at least in their abstract doctrinal statements about the provision (if not as to their underlying data protection teleology).[84] It is also not questioned in academic literature. Art. 6 (1) GDPR thus does not contain an internal hierarchy of the grounds according to which data processing on the basis of lit. a) would be "better" (whatever is meant by this) than processing on the basis of lit. b) or lit. f). Against this background, there is no reason to generally reduce the scope of application of Art. 6 (1) (b) GDPR or to define it as narrowly as possible. Any reductive reading of Art. 6 (1) (b) GDPR runs counter to the primary law understanding of EU data protection law set forth in Art. 8 (2) CRF.

2. Optimizing digital autonomy through contractual agreements

By way of teleological interpretation, it can be shown that the self-determination of both the data subject and the controller can be realized particularly effectively by means of contractual agreements. Only on a very superficial view does “consent” appear to be an effective instrument for empowering the data subject in contractual relationships. This also applies if contract and (downstream) consent are combined. If the executability of a contract depends on one side having to give (downstream) consent that can be revoked at any time, that side will have limited bargaining power. The right to revoke consent at any time (Art. 7 (3) GDPR) deprives the data subject of the possibility of effectively entering into binding contracts. The will *and* ability to enter into a genuine contractual commitment strengthens digital bargaining power. Efforts to establish autonomy under

[83] *European Commission*, Amended Proposal for a Council Directive on the potection of individuals with regard to the processing of personal data and on the free movement of such data, , 15 October 1992, (COM(92) 422 final (SYN 287), http://aei.pitt.edu/10375/1/10375.pdf, p. 17.
[84] *European Data Protection Board*, Guidelines 8/2020 on the targeting of social media users, Version 2.0, 13 April 2021, https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf, para. 48.

data protection law primarily via a consent requirement (revocable at any time) in Art. 6 (1) (a) GDPR ultimately result in an situation, in which data subjects are deprived of the possibility of self-binding (and thus an essential component of private autonomy). Arguably the side providing the service also has limited bargaining options: They must craft the contract and performance in a manner that allows for their counter-party to unilaterally terminate one of the conditions of the contract at any time. It must therefore be repeated at this point that in contractual relations, the application of Art. 6 (1) (a) is an empowerment only on a superficial view. In such relations, the application of Art. 6 (1) (a) means a devil's gift. Effectively, the negotiating power is weakened.

There is no reason for this. It can be shown that Art. 6 (1) (b) GDPR opens up sufficient space for the contracting parties to be able to conclude mutually beneficial contractual agreements about digital services including the use of data. It can also be shown that contract law ensures that such agreements contain a fair (synallagmatic) exchange of benefits. In particular, contract law works against the superior negotiating power of digital companies by providing special protections in favour of consumers and by controlling the terms of service. There is no need to add the requirement of consent in contractual relationships governed by effective contract law. As a result, it can be shown that the justification grounds of Art. 6 (1) (b) GDPR has normative priority over the justification grounds of Art. 6 (1) (a) and (f) GDPR.

a) Contract, realization of preferences and bargaining power

The conclusion of a contract is an expression of the use of human freedom and is therefore of central importance for liberal thinking about the state and society.[85] No other coordination instrument is equally suited to enable natural persons to realize their ideas of the good life. Contracts are the best means by which natural persons can fulfil their different individual preferences. The transaction costs involved are low. Contracts

[85] The conclusion of a contract enables the self-determination of the individual ("realization of autonomy"); contract law creates the legal and factual freedom ("autonomy of action").

stabilize legal relations and create efficiency. EU law is based on the view that human autonomy in social relations can be optimized by concluding contracts.

aa) Contracts as expression of self-determination

Contracts are an expression of a self-determined life in the digital society. They are therefore also the optimal instrument for establishing digital autonomy (in the sense developed above). The idea of contractual "privacy self-management"[86] is not an underdeveloped form of data protection, but its logical perfection. The contract also enables natural persons to decide for themselves which data they want to release for processing, which form of personalization of the service they consider useful and which they do not, or whether and how they want to consent to the processing of data on the other side, for example in order to receive a digital service free of (monetary) charge. Even in case of contracts of adhesion, the undertaking setting the terms of the contract will incorporate the normal interests and hypothetical will of its customers it wishes to retain into the contract design. Contracts create "data sovereignty" - understood as genuine authority to determine, dispose of and shape one's own data. They are instruments of emancipation and empowerment of the individual and enable self-determined informational freedom.[87] It is not easy for an unbiased observer to understand why we live in a world in which contracts are considered the ideal form of self-determination in market relations, but this is not supposed to be the case with regard to the handling of personal data.

EU law is based on the fundamental axiom that natural persons should, in principle, be able to pursue their personal and economic interests freely in the market (Article 26 (2) TFEU). Both on the level of primary law and in countless instruments of secondary law, it is committed to the idea of human self-determination through the conclusion of contracts. The EU Commission is currently undertaking a public consultation on “Digital

[86] *Solove*, Harv. L. Rev. 2013 (123), 1880.
[87] *Bunnenberg,* Privates Datenschutzrecht –Über Privatautonomie im Datenschutzrecht – unter besonderer Berücksichtigung der Einwilligung und ihrer vertraglichen Kopplung nach Art. 7 Abs. 4 DS-GVO, 2020, p. 85 with further references; *Buchner,* Informed consent in Germany in: Vansweevelt/ Glover-Thomas (eds.), Informed consent and health: a global analysis, ed. 2020, p. 216 (133, 176, 183).

Fairness – Fitness Check on EU Consumer Law".[88] This shows that EU contract law is permanently updated to ensure the fairness of contracts in the digital society. Only in the area of data protection law do individual EU actors within the data protection community take a different view, albeit without providing any viable justification. The vague assertion that in the digital society a model of contractual data self-determination is fundamentally unsuitable for taking account of legitimate personal concerns or economic interests is sometimes put forward, but has never been substantiated. There is also no reason for data protection authorities to assess the value of such contracts over the will of the parties concerned.[89]

It has already been mentioned that such contracts provide the data subjects with a bargaining power that does not exist if the data processing takes place on the basis of Art. 6 (1) (a) GDPR.[90] It is an old insight that a data subject can negotiate more favourable conditions if the company does not have to reckon with the fact that consent given under Art. 6 (1) (a) GDPR can be revoked (at any time), thus nullifying a fundamental condition for the performance of the contract. In a contractual relationship in which data processing has been made the subject of a binding contractual exchange relationship, the cost-benefit calculation, both of the data subject and the digital enterprise, will be different than in a relationship in which the data subject gives consent to data processing - and can revoke it at any time. The abstract statement that the latter is necessarily more advantageous or appropriate for the data subject is wrong in any case - it depends on the preferences of the data subject, the subject of the contractual agreement, the alternative services provided by the company, and the other circumstances of the case such as the negotiating power.[91] It cannot be argued that binding contractual agreements, in which the agreement to data processing is part of a synallagmatically

[88] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en.
[89] It is not for the EU institutions to determine how the value and consideration of the benefits in such a contract are assessed. In the modern age, there are no longer any "objective" standards by which the officials of an administrative authority can decide what the value of a given consideration is. Insofar as no harm to the individual can be observed and demonstrated, this is blunt paternalism.
[90] See Section IV. 2. at the beginning.
[91] This has been subject to a debate in Germany: *Riesenhuber*, Recht der Arbeit 2011 (64), 257 (258); *Sattler*, JZ 2017 (72), 1036 (1042).

agreed exchange of benefits, are necessarily worse for the data subject than a revocable right of consent. Adopting this view on a principled level implies that one cannot meaningfully discuss the relationship between Art. 6 (1) (b) GDPR and Art. 6 (1) (a) GDPR even at the outset.

bb) Ensuring substantive contractual autonomy

Digital autonomy can only develop in contractual relationships if it is ensured that the conditions for genuine self-determination are met. Genuine digital autonomy will only be manifested if certain framework conditions are in place (guarantee of "substantive" or "material" contractual autonomy[92]), and certain market failure reasons are sufficiently taken into account (information deficits, limited rationality). Ensuring these conditions is the task of contract law and cannot be handled by data processing law.

There is not the space here to describe these conditions in detail. However, they should be mentioned briefly. Most importantly, the data subject must have the individual capacity to develop first and second order preferences. It must also be ensured that these preferences have been formulated in a sufficiently independent process based on critical reflection. Undue interference with the process of preference formation, e.g. through manipulation, must thus be avoided.[93] However, undue idealization is unwarranted. It is inevitable that certain "behavioral biases" will influence preference formation; the idea of "homo economicus" is a constructive ideal. Moreover, there are good policy reasons to assume that the law must ensure that existing biases are not further reinforced in contract negotiations. It must also be ensured that the influence of other phenomena of market failure is reduced. This applies in particular to information asymmetries and information deficits.[94] Liberal contract law theory also points out that contracts can only

[92] See, e.g., *Bunnenberg,* Privates Datenschutzrecht, 2020.
[93] *Hacker,* Nudging and Autonomy – A Philosophical and Legal Appraisal in: Micklitz/Sibony/ Esposito (eds.), Handbook of Research Methods in Consumer Law, ed. 2017, p. 77 (243).
[94] Such deficiencies may concern the questions: What is done with the data? What insights can be gained from it? What are they worth?

fulfil their function if certain external conditions are met (no undue imbalance in bargaining power; procedural and substantive fairness, etc.).

Data protection law is neither structurally adequate nor efficient in fulfilling these regulatory tasks. Obviously, an absolute requirement of consent is not necessary or proportionate to address these concerns. On the other hand, contract law may contain the necessary provisions to counteract any problems of free self-determination, both in the case of freely negotiated contracts and in the case of contracts of adhesion. It is the task of contract law to establish the necessary protective standards in this regard. If necessary, the additional use of regulatory instruments under public law or the application of competition law is required. Again, however, these are not problems particular to the digital society; these problems also arise in the non-digital world and are successfully dealt with there. There is no fundamental reason to reject the realization of digital autonomy through the conclusion of contracts in the digital world simply because regulatory or control necessities arise in specific situations.[95]

It is clear in any case that any (potential or actual) deficits of contract law cannot be eliminated by reducing the scope of application of Art. 6 (1) (b) GDPR and granting data subjects a right of consent under Art. 6 (1) (a) GDPR.[96] In particular, there is no reason to believe that phenomena of market failure that call into question the value of a digital contract do not also arise when it comes to granting or refusing consent. In other words, deficiencies in the area of digital contracts cannot be addressed by additionally granting data subjects a right of consent under Art. 6 (1) (a) GDPR. Some data

[95] *Möslein/Beise,* Datensouveränität als Privatautonomie in: Augsberg/ Gehring (eds.), Datensouveränität – Positionen zur Debatte, ed. 2022, p. 103.

[96] The EDPB's "Binding decision" 3/2022 (see footnote 8 above) confirms this vividly: The EDPB repeatedly complains about the (alleged) lack of transparency of the contract between digital companies and users. It does not address the question of whether the alleged lack of information of the users would really be clarified if they still have to consent after the conclusion of the contract according to Art. 6 (1) (a) DSGVO. There is no reason for the general assumption that the contractual obligations to inform and specify do not have the same scope as the data protection obligations with regard to consent. It would require concrete investigation whether this is so in the specific case. However, the EDPB has not done this.

protection experts, however, fundamentally reject the contract as an instrument for realizing digital autonomy: It is claimed that the data processor unilaterally dictates the terms and conditions.[97] However, formulation of general terms and conditions does not mean that the contract is not backed by the mutual assessment of the contracting partners that the conditions are fair and the relationship between performance and consideration is balanced.[98]

cc) Limitations of digital contractual autonomy

Of course, there are limits to the use of contract law as a means for realizing digital autonomy. Obviously, there may be risks and threats in both the non-digital and digital social spheres that are so difficult for natural persons to recognize or so weighty that the law must intervene through outright prohibitions. In these cases, (digital) autonomy is eliminated - if necessary also in the well-understood self-interest of those affected. It is not entirely inconceivable that in a liberal information order based on contractual relations, prohibitions must also be resorted to. It does not seem impossible that the disclosure of certain personal information (or the underlying data) could damage an individual's ability to lead a good life so severely that it would be normatively wrong to allow room for autonomy. However, none of the practices or business models discussed here even remotely raises such a need for regulation through prohibitions under public law or contractual law.[99] This also applies to the financing of monetarily free digital services

---

[97] *Article 29 Working Party*, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217), 9 April 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf, pp. 16–17: The justification ground "contract" "must be interpreted strictly and does not cover situations where the processing is not genuinely necessary for the performance of a contract, but rather unilaterally imposed on the data subject by the controller".

[98] A look at general contract law shows, moreover, that it is highly unusual to link the conclusion of a contract with a downstream requirement for consent. A fortiori, contract codes do not provide for either party to be granted a free right of withdrawal at any time, which would make further performance of the contract impossible. If such rights were really necessary to secure the individual's substantive autonomy, they would certainly have been realized long ago in a world that relies very heavily on the idea of consumer protection. Once again, data protection law exceptionalism is evident here.

[99] The GDPR also contains special rules for the processing of particularly sensitive data (Art. 9 GDPR).

through behavioral advertising. If one were to assume that there is a particular risk as to the effects of behavioral advertising, it would be contradictory to require and permit consent under Art. 6 (1) (a) GDPR. If such a risk were to exist, the legislator would be called upon to outlaw the practice. The EU legislator has made it clear in the context of the creation of the Digital Services Act that behavioural advertising does not in principle give rise to any need for prohibition.

dd) Inappropriateness of data protection exceptionalism

Digital contract law can thus strengthen the autonomy of individuals in a way that the "consent" requirement never will. This is true, as I said, not only in the case of freely negotiated contracts, but also in the case of contracts of adhesion, which will never reflect only the interests of one side.[100] Nevertheless, it can be observed In the discussion on data protection law that the reaction to this is the introduction of a condescending and patronizing image of the human being. However, it is normatively and analytically inappropriate to simply stylize natural persons as passive beings helplessly in the hands of overpowering and predatory large corporations. There is no justification for fundamentally ruling out the possibility that a contract is a suitable means of realizing private autonomy, realizing individual preferences, creating efficiency, and stabilizing socio-economic relationships in the emerging digital society. Doing so fundamentally calls the modern liberal economic order into question. Data privacy "exceptionalism," which denies the functional and normative value of digital contracts per se, is ultimately an attack on the foundations of the Western social order. In a market economy, at any rate,

[100] It is interesting to observe that some data protection experts seem to reject the notion that contracts may serve as an instrument for realizing digital autonomy on a fundamental level: they claim that the data processor "unilaterally dictates" the conditions (see, e.g., *European Data Protection Board*, Guidelines 2/2019 on the processing of personal data under Art. 6 (1) (b) GDPR in the context of the provision of online services to data subjects, 8 October 2019, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf). Such statements mainly show prejudice. They are also based on an error in thinking: the formulation of general terms and conditions does not mean that the contract is not based on the mutual assessment of the contracting partners, that the conditions are not fair, and the relationship between performance and consideration is unbalanced.

one should prima facie rely on contractual agreements unless there are sufficiently good reasons to make divergent allocations by creating special legal positions or granting special (exclusionary) rights.

In summary: The digital autonomy of the data subject can be optimized by entering into contracts with digital economy companies that provide for processing under Art. 6 (1) (b) GDPR. Such contracts enable data subjects to realize their first and second order preferences better than the right of consent under Art. 6 (1) (a) GDPR can. Digital contracts empower natural persons. There is also no reason for data protection authorities to assess the value of such contracts over the will of the parties concerned. In contrast, an official assessment of the value of contractual services by data protection authorities disempowers the contractual parties. Finally, if the conclusion of a contract is followed by a consent requirement pursuant to Art. 6 (1) (a) of the GDPR, this only *appears* to empower the data subject. The fact that consent can be revoked at any time ultimately has the effect of weakening the subject's negotiating power and digital autonomy.

This makes it clear that data protection law must be thought of through the lens of contract law: if and to the extent that an agreement on business services and digital content and data has been concluded between a company and the data subject that is appropriate under contract law and corresponds to the interests of the parties involved, there is no reason for data protection law to correct this agreement - not even by constructing additional consent requirements that place the possibility of any implementation of the contract in the hands of one of the two contracting parties.

b) EU Regulations to safeguard substantive contractual autonomy

The above considerations would be open to attack if they were based solely on a libertarian and formalistic philosophy on the value of the contract. They gain their persuasiveness above all from the fact that the contract law of the EU and of EU member states ensures, in an almost incalculable number of provisions, that the conditions for the use of digital autonomy by contract are safeguarded (e.g. transparency and information; balancing of power imbalances; prevention of the use of harmful clauses, etc.). It can be shown that the conditions for “material” contractual autonomy are more than

satisfied through a large body of contractual law. If deficits seem to appear, the EU institutions do not hesitate to react. In this context, the EU legislator has fulfilled its treaty obligation (Art. 12 TFEU).

For reasons of space, only very few comments can be made here. Directive 770/2019 provides for specific consumer protection provisions for contracts that have digital services as their subject matter. This applies both to the service offered and to the legal consequences in the event of poor performance.[101] The precautions of the directive also apply if the services are not provided in return for monetary payment, but in return for the provision of data or consent to the use of data. In contrast, the provisions of the directive do not apply if the transfer or use of data does not go beyond what is absolutely necessary for the performance of the contract. In terms of legal policy, this is based on the consideration that the special consumer protection regulations regarding contractual obligations should not apply to providers who only collect the absolutely necessary data (name, address, etc.).

The provisions of Directive 770/2019 are of direct relevance for the interpretation of Art. 6 (1) (b) GDPR. It is not only clear from the provisions of the directive that EU law permits the conclusion of contracts that provide for the collection of data that goes beyond what is technically necessary and thus treats data as consideration. It can also be inferred from Directive 770/2019 that, in the opinion of the EU legislator, contracts that comply with the conditions provided for therein satisfy the requirements to be met with regard to "material" private autonomy, at least as far as the content of the directive goes. In terms of data protection law, it would be inadmissible to call into question the values of the EU legislator and the practical effectiveness of the directive by not including such contracts under Art. 6 (1) (b) GDPR. The EU legislator indicates that it wants to ensure fairness in contracts - and this not by adding an additional data protection regime under Art. 6 (1) (a) GDPR to the contract. If one were to see this differently, one would have to claim (and demonstrate) that EU consumer protection law is not achieving its goal

[101] The Directive does state (recital 24) that it does not take a position on the normative question of whether data can be regarded as consideration. Economically, politically and practically, however, this is precisely what is recognized (*Schmitz,* Die Digitalisierung der gesetzlichen Formen, 2022).

properly and that the EU legislator has done a poor job. It would be contradictory to want to strengthen the digital economy in the EU by expanding digital consumer protection law and thus stimulate growth, while at the same time depriving consumers of their contractual autonomy under data protection law by making the performance of contracts dependent on consent pursuant to Art. 6 (1) (a) GDPR.

For reasons of space, it should only be noted here that the provisions of the Digital Markets Act[102] are also relevant for the interpretation of Art. 6 (l) (b) GDPR. The limitation of market power and the detailed regulation of (contractual) conduct provided for therein also contribute to the fact that data protection law should recognize and respect the exercise of digital autonomy in contracts pursuant to Art. 6 (1) (b) GDPR - and not attempt to obstruct what has been agreed.

Furthermore, EU law on protection against unfair terms in consumer contracts[103] and Member State consumer contract law ensure that substantive private autonomy comes into play in digital contracts. The processing of data can only be provided for in contracts that are transparent and fair according to contract law categories (Art. 12 TFEU). Otherwise, they would already not come into existence, could be challenged or would be incompatible with the law on general terms and conditions. It is contradictory for data protectionists to devote enormous energy to subjecting processing that has just been contractually agreed to an additional consent requirement (under data protection law), and thus to apply a parallel or cumulative order, instead of using legal policy to ensure that any deficits and problems in the world of digital contracts are remedied by changing contract law.

The above considerations make it clear that an interpretation of the clauses in Art. 6 (1) GDPR is only legally appropriate and meaningful if the respective context is taken into account. The interpretation of legal provisions outside of the patterns of meaning in which they and their application are embedded leads, in the best case, to meaningless

[102] Regulation (EU) 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act), OJ 2022 L 265/1.
[103] Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ 1993 L 95/29, as amended by Directive (EU) 2019/2161.

random results; and in the worst case, it leads to bad law. Subjective believes and options are no substitute for a contextualized interpretation of Art. 6 (1) GDPR supported by normative principles. It is extremely striking that data protection authorities refuse to read a provision such as Art. 6 (1) (b) GDPR in a systematic context with the contract law provisions of EU and EU Member State law. By enacting RL 770/2019, the EU legislator has clearly legitimized the business models reliant on behavioural advertising.[104] By adopting the Digital Services Act, it has clarified that behavioral advertising is, in principle, normal and legitimate market practice. It has also expressed its view that the protective concerns of EU law are to be fulfilled through the contractual safeguards of consumer law (and not through the subsequent implementation of data protection consent requirements). Data protection theory that closes their eyes to this does not lead to enlightenment, but remains (deliberately) in the dark.

c) No reason or authority for "choice-requiring paternalism"

This observation is drawn from legal and economic considerations.

The attempt by individual data protection authorities to add a consent requirement under Art. 6 (1) (a) of the GDPR to a binding contract which parties have already concluded can be understood as an attempt to tightly control how one may express his or her digital autonomy, or lack thereof. In behavioral economic terms, one could speak of a form

[104] See, e.g., *Fries,* Data as counter-performance in B2B contracts in: Lohsse/Schulze/Staudenmayer (eds.), Data as counter-performance – contract law 2.0?, ed. 2020, p. 253; *Mischau*, GRUR International 2020 (69), 233; *Linardatos,* Autonome und vernetzte Aktanten im Zivilrecht, 2021, pp. 506-559; *Riehm,* Freie Widerrufbarkeit der Einwilligung und Struktur der Obligation – Daten als Gegenleistung? in: Pertot (eds.), Rechte an Daten, ed. 2020, p. 175; *Scheibenpflug,* Personenbezogene Daten als Gegenleistung – Ein Beitrag Zur Rechtlichen Einordnung Datengetriebener Austauschverhaltnisse, 2022; *Wendehorst,* Of Elephants in the Room and Paper Tigers How to Reconcile Data Protection and the Data Economy in: Lohsse/Schulze/Staudenmayer (eds.), Trading Data in the Digital Economy – Legal Concepts and Tools, ed. 2017, p. 327. See also *Langhanke,* Daten als Leistung – Eine rechtsvergleichende Untersuchung zu Deutschland, Österreich und der Schweiz, 2018.

of "nudging" in form of "required active choosing".[105] In the practice of the EDPB, it can be observed that the application of Art. 6 (1) (b) GDPR is to be excluded via questionable legal-doctrinal constructions[106] in order to bring about (aside from the conclusion of the contract) an (additional) consent requirement under Art. 6 (1) (a) GDPR. However, from a "law and economic" point of view, very predominant reasons speak against the construction of such a decision architecture.

What reasons could there be for wanting to establish an additional consent requirement for data processing beyond the effective conclusion of the contract? In terms of substance, at any rate, such an additional consent requirement does not establish any protective element that is not already the subject of contract law. In principle, contract law will establish similar standards with regard to transparency and information, with regard to self-determination and rationality etc. as the provisions of the GDPR on consent (Art. 4 (11), Art. 7 GDPR). Procedurally, however, there is a behavioral economics effect. If there is a time span between the conclusion of the contract and the subsequent consent, the data subject will be in the position to change his or her mind after the contract has been concluded but before the consent has been given. In such a case, the data subject might rethink his or her decision, change his or her mind and can make it impossible to execute the contract that has already been concluded by refusing to give his or her consent. [107] It is also conceivable that the data subject may change his mind after giving consent, revoke his consent and thus prevent further performance of the contract. From the point of view of behavioral economics, it is possible to speak of the necessity of an "active" consent action by the data subject . Instruments of "required active choosing" cause the person to make a renewed decision after conclusion of the contract. The necessity of having to decide again can be a reason to improve the information base, to deal with one's own biases and correct them, or to change one's own preferences.

---

[105] *Hacker,* Nudging and Autonomy – A Philosophical and Legal Appraisal in: Micklitz/Sibony/ Esposito (eds.), Handbook of Research Methods in Consumer Law, ed. 2017, p. 77 (489).
[106] See chapter V. below.
[107] See, e.g., *Esposito*, European Journal of Risk Regulation 2015 (6), 331 (329); *Rebonato,* Taking Liberties – A Critical Examination of Libertarian Paternalism, 2012, p. 202; *Hansen/Jespersen*, European Journal of Risk Regulation 2013 (4), 3 (18); *Baldwin*, The Modern Law Review 2014 (77), 831 (835).

There are good reasons why instruments of "required active choosing" do not play a significant role in consumer contract law both in the EU and the EU member states (unlike rights of withdrawal). In practice, it can be observed that natural persons hardly ever use the time between the conclusion of the contract and the additionally needed second decision to actually improve their information base. There is also no reason and regularly not enough time for them to work on correcting "biases". Anyone who has concluded a transparent and fair contract for a digital service, which also provides for consent to data processing, will, in most cases, be in a position to assess whether the conclusion of the contract is based on exogenous or endogenous preference deficits and biases. In terms of behavioral economics, instruments of "required active choosing" primarily favor human inertia: Some natural persons do not make the required renewed active decision out of indifference, carelessness or other factors - with the consequence that the contract already concluded cannot then be executed.

In terms of data protection theory and data protection law, there is no reason to interpret Art. 6 (1) (b) GDPR in such a way that consent under Art. 6 (1) (a) GDPR is applied as a downstream instrument of "required active choosing" (after the conclusion of a binding contract). This construction is of no use at all if the contract is concluded and the data protection consent is given at the same time - procedural-intertemporal behavioral economic effects are then already excluded in principle. But even if the conclusion of the contract and the subsequent declaration of consent do not coincide, no benefit can be identified. Typically, the data subjects do not attempt to obtain information during this period that would allow them to make a better decision. Nor do they rationally correct preference deficits. Downstream competition (*post contractum*, but *ante consentum*) is also not observed. It is true, however, that such a decision architecture makes room for inertia.[108] The available behavioral economic studies also show in this regard that the use of such a right of withdrawal is rarely an expression and consequence of the elimination of information deficits or the correction of "biases". More often, it is simply a

[108] Moreover, if a consent requirement is established *post contractum*, the data subject can make the execution of the contract impossible later on by revoking the consent (Art. 7(3) first sentence GDPR.

matter of preference changes. It cannot be denied that this is an empowerment of the data subject, in the sense of acting arbitrarily. However, it was pointed out above that this has to be paid for with a reduction in bargaining power. In another publication, I pointed out that a legal architecture that relies entirely on allowing natural persons to change preferences arbitrarily ultimately infantilizes human beings.

A downstream consent requirement also imposes significant transaction costs: it is not enough that a contract has been made, and it is not enough that the related contract documents have been studied. The subsequent use of an instrument of "required active choosing" leads to the need for yet another (quasi-legal) act. The inflationary use of instruments of "required active choosing" leads to a blunting that can damage the instrument. The cognitive demand placed on humans by such instruments is high; they must not be used unless there is sufficient reason to do so. Especially in cases where a transparent and fair contract has been concluded between the data subject and the company, such a tool does more harm than good.[109]

In terms of “law and economics”, another objection can be formulated. It makes no sense whatsoever to provide as a default rule the non-implementability of the contract in the event that the data subject resists the expectation to make another decision on consent after the conclusion of the effective contract. If Art. 6 (1) (a) GDPR is applied in contractual relationships, the requirements of Art. 7 GDPR amount to such a default rule. This may be in line with the political wishes of those data protectionists who fundamentally reject the developments of the digital economy and see every non-performable contract as a gain. However, it does not correspond to the observation that digital autonomy has already been reflected in the effectively concluded contract. The legal protection of mere inertia is of no value here.

As a result, this leads to the following conclusions: Even from a “law and economics” point of view, there is no reason under data protection law to add an additional consent requirement to the conclusion of a transparent and fair contract for the provision of a digital service. Obviously, the EU legislator could have provided that any processing of

[109] With regard to “consent fatigue”, see, e.g., *Wein*, Economies 2022 (10), 1 et seq.

data, even in contractual relationships, still requires additional consent. However, knowing the legal-economic dubiousness of such a step, it knowingly did not do so. Art. 8 (2) CFR does not explicitly provide for this either. There is no legitimate possibility to overrule this decision of the EU legislator through means of enforcer interpretation. Insofar as an effective contract has been concluded, the requirements of Art. 6 (1) (b) GDPR as well as those of Art. 8 (1) CFR have been met. Anyone who wants to exclude the application of Art. 6 (1) (b) GDPR only in order to provide data subjects with an additional consent requirement (Art. 6 (1) (a) GDPR) after the conclusion of a binding contract must accept the accusation of "choice-requiring paternalism," to use a formulation by *Cass Sunstein*.[110]

d) No danger of unlimited commercialization

Finally, I would like to make a comment on legal policy. Concerns that personal information could be commercialized without limits seem to lay behind the reluctance of some data protection authorities to validate the right of data subjects to conclude contracts allowing for the processing of personal data (e.g. for services financed by behavioural advertising). Opponents of any form of commercialization of data seem to be dominated by the concern that everything could start to slide - to the point of the spread of data markets in which all personal information (regardless of its sensitivity) is regarded only as a commodity.

This concern about the boundless commercialization of the personal cannot be brushed aside lightly. It is not entirely unjustified and must be taken seriously. However, the concern must be addressed through appropriate means and must not be taken out of perspective. Data protection law cannot take seriously concerns used as an opportunity to deny natural persons the right to autonomous contractual self-determination altogether. This would obviously lead to disproportionate results (Art. 5 (3) TEU). In other words, a justified concern must also not lead to throwing out the baby with the bathwater. As important as it is to position contract law and data protection law against

[110] *Sunstein*, Duke L.J. 2014 (64), 1; *ibid.*, Journal of Behavioral Economics for Policy 2017 (1), 11.

developments in which personal information becomes the commercialized object of unregulated transactions in the marketplace, it is inappropriate to axiomatically deprive autonomously acting natural persons of any possibility of entering the market with data. In the non-digital world, the idealistic idea that any "alienation" of the data subject can be prevented by legally prohibiting others from using personal data at any time has never been accepted. In the digital society, there is no room for this either. In the non-digital world, whoever has information about another person is also not just a "trustee" who has to exercise this information in the interest of the person concerned. There is no reason why this should be the case in principle or even always in the digital world.[111] Concerns about undesirable developments should not lead us to adopt a myopic view that loses sight of the overall context and sees the world only through the lens of data protection law dystopias.

3. Optimization of fundamental rights values and legal positions

From a fundamental rights perspective, too, decisive objections can be formulated against the attempt to interpret Art. 6 (1) (b) GDPR restrictively. The exercise of digital autonomy through contracts within the meaning of Art. 6 (1) (b) GDPR leads to an optimization of fundamental rights values and fundamental rights legal positions that cannot be achieved in this way under Art. 6 (1) (a) GDPR. This applies both to the fundamental rights of the company and to the fundamental rights of the data subject.

a) Necessity of taking all affected fundamental rights into account - inadmissibility of a silo-ed approach under data protection law

The CJEU has consistently held that provisions such as Art. 6 (1) GDPR must be interpreted in accordance with fundamental rights. In concrete terms, this means that a fundamental rights cost-benefit balance must be drawn up for various possible interpretations of the legal provision in question. In this way, it can be determined which of the possible interpretations optimizes the goods protected by fundamental rights and is therefore preferable from an interpretative point of view. There can be no "precedence"

[111] See *Wendehorst/Schwamberger/Grinzinger,* Datentreuhand – wie hilfreich sind sachenrechtliche Konzepte? in: Pertot (eds.)*,* Rechte an Daten, ed. 2020, p. 103.

of specific fundamental rights here: All rights in the EU Charter of Fundamental Rights have the same rank and status. Even if this is sometimes claimed otherwise in data protection circles: There is no reason to give priority to the fundamental right in Art. 8 (1) CFR over the freedoms of companies and individuals, even more so because this provision (only) requires an adequate level of protection.[112] In terms of fundamental rights theory, it is necessary that the level of protection sought by Art. 8 (1) CFR is not undercut - above this level of protection, only the rights of freedom can determine the interpretative decision in question.

Obviously, the interpretation of provisions such as Art. 6 (1) GDPR in conformity with fundamental rights cannot succeed properly even at the outset if only select fundamental rights are taken into account . Such a selective approach is diametrically opposed to the case law of the CJEU. Nevertheless, it corresponds to a common approach of the EDPB.[113] In the 2019 guidelines, no fundamental right apart from Art. 8 CFR is mentioned at all. In the Binding Decision 3/2022 the EDPB states that "[t]he GDPR develops the fundamental right to the protection of personal data found in Art. 8(1) of the EU

[112] It is predominantly assumed that the various fundamental rights have the same rank and that practical concordance must therefore be established (*Lynskey,* The Foundations of EU Data Protection Law, 2015., p. 62*;* for the discussion in Germany, for example: *Buchner*, in: *Kühling/Buchner,* Datenschutz-Grundverordnung BDSG. Kommentar, 4 ed. 2023, commentary on Art. 1 GDPR, para. 1 et seq.; *Pötters*, in: *Gola,* Datenschutz-Grundverordnung VO (EU) 2016/679 –Bundesdatenschutzgesetz. Kommentar, 3 ed. 2022., commentary on Art. 1 GDPR, para. 5; *Klement,* JZ 2017 (72), 161 (164); for the primacy of the fundamental right to data protection: *Hornung/Spiecker gen. Döhmann*, in: *Simitis/Hornung/Spiecker Döhmann, et al.,* Datenschutzrecht DSGVO mit BDSG, 1. Auflage 2019, commentary on Art. 1 GDPR, para. 28; *Clifford/Graef/Valcke*, German Law Journal 2019 (20), 679 (709).

[113] See *European Data Protection Board*, Guidelines 2/2019 on the processing of personal data under Art. 6 (1) (b) GDPR in the context of the provision of online services to data subjects, 8 October 2019, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf and *ibid.*, Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR), 5 December 2022, https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-32022-dispute-submitted_en.

Charter of Fundamental Rights and Art. 16 (2) of the TFEU".[114] The EDPB also points out the need to interpret the GDPR in a manner consistent with primary law.[115] However, the EDPB never seems to engage in this conformity exercise: it does not elaborate on what specific purposes, values, and protected interests in Art. 8 CFR are affected by the practice of placing behavioral advertisements. It then also does not explain to what extent these purposes, values, and interests are sufficiently impaired that use of Art. 6 (1) (b) GDPR must be ruled out. It is not sufficient to proclaim trivial generalities - the decision should have been an opportunity to deal more precisely with the specific meaning of Art. 8 CFR and then, against this background, to draw conclusions for the interpretation of Art. 6 (1) (b) GDPR. Further, the EDPB does not mention, let alone consider, other fundamental rights in its interpretation of Art. 6 (1) (b) GDPR. Art. 16 CFR is simply overlooked - or considered irrelevant. The freedom rights of the data subjects, which include the right to enter into contracts for services involving the processing of personal data, are also missing. The EDPB ultimately refrains from an interpretation of Art. 6 (1) GDPR in conformity with primary law. Rather, it presents its secondary law understanding of Art. 6 (1) (b) GDPR as an implementation of Art. 8 CFR without alternatives. This is a very serious deficiency. It can also already be observed in its 2019 guidelines on Article 6(1)(b) GDPR.[116]

The attempts to eliminate the relevance of EU fundamental rights apart from Art. 8 CFR are not limited to the EDPB. In the academic discussion, efforts can also be observed to completely block discussions about how Art. 6(1) GDPR could be structured in a way that complies with all relevant fundamental rights. Some observers try to avoid a

---

[114] *ibid.*, Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR), 5 December 2022, https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-32022-dispute-submitted_en, para. 101, first sentence.
[115] Ibid., para. 101, second sentence.
[116] *European Data Protection Board*, Guidelines 2/2019 on the processing of personal data under Art. 6 (1) (b) GDPR in the context of the provision of online services to data subjects, 8 October 2019, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf.

discussion by referring to an alleged "fundamental rights nature of data".[117] The formulation is already linguistically strange, because the collection and processing of data is limited by fundamental rights, but this does not change its quality. Money and money demands are protected by Art. 17 CFR - yet no one would speak of the "fundamental rights nature of money". The protection mandate expressed in Art. 8 (1) CFR does not exempt from the necessity to deal with the relevance and weight of other fundamental rights. Others seem to imply that Art. 8 CFR reigns supreme within the Charter. Such flaws, both from the point of view of fundamental rights theory and methodology, are to be avoided. The interpretation of Art. 6 (1) GDPR must take into account all relevant fundamental rights guarantees.

b) Entrepreneurial Freedom under Art. 16 CFR

A literal interpretation of Art. 6 (1) (b) GDPR makes it possible to protect fundamental rights including the freedom of the company that has concluded a contract with the data subject (Art. 16 CFR).

The CJEU has addressed this provision several times in recent years, developing the following principles:

aa) Protective scope

Art. 16 protects the right to conduct a business which covers the freedom to exercise an economic or commercial activity including the freedom of contract.[118] The freedom of contract protects, in particular, the freedom to choose with whom to do business and the freedom to deter mine the price of a service.[119] Similarly, the fundamental freedom of services (like the freedom of establishment) protects the offering of particular services

[117] See *European Data Protection Supervisor*, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, 17 March 2017, https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf, p. 8 para. 18; p. 20, para. 82.
[118] CJEU, 22. January 2013, C-283/11, Sky Österreich, EU:C:2013:28**,** para. 42.
[119] CJEU, 20 December 2017, C-277/16, Polkomtel, EU:C:2017:989, para. 50.

for a particular form of remuneration.[120] Entrepreneurial freedom also includes the right of each company to freely dispose of its economic and financial resources within the limits of its responsibility for its own actions. The freedom of contract can be exercised by an undertaking, also vis-à-vis users without any bargaining power, by way of a standard form contract. In that case the freedom of contract of the user consists, essentially, in deciding whether or not to accept the terms of such a contract. There is no doubt that this provision protects the right of a digital economy company to define a specific business model and to carry it out on the basis of freely concluded contracts.[121]

bb) Substantive Interference

In the opinion of the CJEU, a restriction of this right exists whenever a regulation or measure has a significant impact on the use of entrepreneurial freedom. A restriction of the right to conduct a business is, inter alia, the obligation to take measures which may represent a significant cost for an economic operator, have a considerable impact on the organization of his or her activities, or require different and complex technical solutions.[122] The Court of Justice has ruled, for example, that state interference with the freedom of the company to set prices constitutes interference with the exercise of the right guaranteed by Art. 16 of the Charter.[123] Regulations that force the company to design its product in a certain way are likely to restrict the exercise of its entrepreneurial freedom.[124] Of course, prohibitions or regulatory interventions may also have the effect of interfering with the exercise of entrepreneurial freedom.[125] The CJEU has also stated that an actually unacceptable fundamental right burden can be legitimized by opening

[120] CJEU, 5 October 2004, C-442/02, Caixa Bank France, EU:C:2004:586, para. 12 et seq.
[121] CJEU, 15 April 2021, C-798/18, Federazione nazionale delle imprese elettrotecniche ed elettroniche (Anie) and Others, EU:C:2021:280 para. 60; Advocate General Saugmandsgaard Øe, 20 October 2020, C-798/18, Federazione nazionale delle imprese elettrotecniche ed elettroniche (Anie) and Others, EU:C:2020:876, para. 73.
[122] CJEU, 27 March 2014, C-314/12, UPC Telekabel Wien, EU:C:2014:192, para. 50.
[123] CJEU, 20 December 2017, Polkomtel, C277/16, EU:C:2017:989, para. 51.
[124] CJEU, 30 June 2016, C-134/15, Lidl, EU:C:2016:498, para. 29.
[125] CJEU, 17 December 2015, C-157/14, Neptune Distribution, EU:C:2015:823, para. 67.

up freedom of choice for the company. In such cases, it is necessary to leave those service providers to determine the specific measures to be taken in order to achieve the result sought; accordingly, they can choose to put in place the measures which are best adapted to the resources and abilities available to them and which are compatible with the other obligations and challenges which they will encounter in the exercise of their activity.[126]

Against the background of this case law,[127] it cannot be doubted that a restrictive interpretation of Art. 6 (1) (b) GDPR would result in an interference with fundamental rights. [128] It would severely limit the freedoms established in Art. 16 CFR if EU data protection law would put the implementation of a validly concluded contract in question by giving one side the freedom and duty to require "active required choosing" downstream. It does not need to be mentioned here that Art. 6(1)(f) GDPR can offer a way out here; but then the balancing of interests is placed in the hands of authorities and courts. Any interpretation of Art. 6 (1) GDPR which applies the requirement of Art. 6 (1) (a) GDPR to a validly concluded contractual agreement on data processing is a regulatory interference with corporate freedom. First, the company must fulfil additional justification burdens regardless of the agreement already made and - depending on the position of the data protection authority or the court - is prevented from implementing the contractual agreement. Second, the substantive reciprocity of the contract is altered if one side is given the right to unilaterally opt out. The application of Art. 6 (1) a) GDPR in cases, in which a binding legal contract is concluded, would result in a unilateral intervention in the material contractual relationship in favour of the contractual counterparty.

---

[126] CJEU, 27 March 2014, C-314/12, UPC Telekabel Wien, EU:C:2014:192, para. 52; CJEU, 26 April 2022, C-401/19, Poland/Parliament and Council, EU:C:2022:297, para. 75.

[127] See Advocate General Saugmandsgaard Øe, 20 October 2020, C-798/18, Federazione nazionale delle imprese elettrotecniche ed elettroniche (Anie) and Others, EU:C:2020:876, para. 70 et seq.

[128] On the Relationship between Article 16 CFR and the GDPR Rights of Data Subjects: *Ferretti,* Common Market Law Review 2014 (51), 843 (852); see also: *Mayer-Schoenberger,* Generational development of data protection in Europe in: Agre/ Rotenberg (eds.), Technology and Privacy: The New Landscape, ed. 1997, p. 219; *Heisenberg,* Negotiating Privacy, 2005, chapters 1–3.

c) Freedom of contract of the individual according to Art. 6 CFR

A literal interpretation of Art. 6 (1) (b) GDPR also ensures the freedom of the data subject to enter into digital contracts that provide for the processing of his or her data. The CJEU has not yet had to explicitly decide the question of whether private individuals enjoy fundamental legal protection of their private contractual autonomy in the EU's fundamental rights system. However, it has explicitly answered this question in the affirmative for companies. It already held in 2013 that Art. 16 CFR "covers in particular freedom of contract, as is clear from the explanatory notes drafted as guidance for the interpretation of the Charter of Fundamental Rights (OJ 2007, C 303, p. 17), which must be taken into account for the interpretation of the Charter pursuant to Art. 6 (1)(3) TEU and Article 52(7) of the Charter.... ."[129]

It would be incomprehensible and contradictory if the EU fundamental rights system granted companies, but not other persons, the freedom to conclude contracts as a protected fundamental right . If this freedom were not protected, the EU institutions could take away natural persons' private contractual autonomy without any recourse to fundamental rights. This would be incompatible with the idea of freedom in EU law (Article 2 TEU). Private contractual freedom is widely protected by EU Member State fundamental rights systems (Art. 6 (3) TEU). There is no conceivable reason why this should not be the case within the CFR system. It is not necessary here to discuss in more detail the question of where the fundamental rights protection of private contractual autonomy (outside of Art. 16 CFR) is to be located; these reasons best speak for Art. 6 CFR.

An interpretation of Art. 6 (1) (b) GDPR that excludes the application of this justification ground for validly concluded contracts or individual contractual arrangements would then also restrict the data subject's right to freedom. Such an exclusion would, as explained above, only seemingly improve his or her position; on a deeper view, a

[129] CJEU, 18 July 2013, C-426/11, Alemo-Herron, EU:C:2013:521, para. 32, with reference to CJEU, 22 January 2013, C-283/11, Sky Österreich, EU:C:2013:28, para. 42.

person loses private autonomy if he or she is prevented from establishing effectively binding contractual obligations. It is part of the consumer's freedom, protected by fundamental rights, to contractually agree with the company on a personalized offer that may be more favorable than the offer that the company makes available to those customers who make use of the right under Art. 6 (1) (a) GDPR.

4. Preservation of the standard of protection required under Art. 8 (1) CFR

Finally, a literal interpretation of Art. 6 (1) (b) GDPR does not compromise the standard of protection required by Art. 8 (1) CFR. The establishment of a consent requirement under Art. 6 (1) (a) of the GDPR after the conclusion of a binding contract does not result in any gain in protection under Art. 8 (1) CFR.

a) Diffuseness of the "digital harm" theory of data protection law

There are many ambiguities and misunderstandings in dealing with and understanding Art. 8 (1) CFR.[130] Some want to interpret the provision as a *right of freedom*. This then leads to calls for the "optimizing" of data protection - without it being clear, however, what "optimized data protection" exactly looks like. Occasionally, it seems as if the process of optimization is seen in the extension of consent requirements under Art. 6 (1) (a) GDPR. But that would obviously contradict Art. 8 (2) GDPR. Others seem to want to recognize a state of optimized data protection when as little personal data as possible is in the hands of other actors - data protection would then be result in “data scarcity”[131]. In the further course of the 21st century, if this were really decisive, it would no longer be possible to speak of data protection at some point. Still others simply leave open what they understand by optimal data protection and limit themselves to a stringing together of superficialities, generalities and banalities. In the EDPB's statements, reference is frequently made to Art. 8 CFR. However, what its protection actually consists of is regularly left completely vague. The EDPB has never attempted to describe precisely and conclusively the form and level of protection required by Art. 8 (1) CFR. This

[130] See *Sydow* in: *Sydow,* DS-GVO, BDSG Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: Handkommentar, 3 ed. 2022. Introduction para. 10 et seq.
[131] See, e.g., *Weiß/Reisener,* ZInsO 2017 (20), 416.

constitutional law cornerstone of data protection has never been systematically and conclusively interpreted until now by the data protection authorities.

Art. 8 CFR is not a right of freedom. Although Art. 8 CFR establishes a subjective right, it is not a guarantee that opens up arbitrary freedom within its scope of protection. In this respect, it would thus be fundamentally wrong to search for answers to the question of how far protection under Art. 8 (1) CFR must revolve around the enablement of individual subjective free will. It is therefore also pointless to speak of optimization here. Rather, the protection mandate of Art. 8 (1) CFR must be taken at its word: Natural persons are to be legally *protected* against the processing of their personal data leading to damage to fundamental rights values and interests. Art. 8 (1) CFR therefore requires the development of a theory of "digital harm". This approach corresponds to demands in the more recent discussion on data protection philosophy: there, too, it has recently been demanded that data protection be thought of in terms of the preservation and safeguarding of human integrity (*Helen Nissenbaum*[132]). A fundamental right such as Art. 8 CFR can therefore only be meaningfully filled with life if it is clarified to which impairment it reacts and confers protection. In other words, any form of interpretation of Art. 8 CFR must be based on concrete and specific statements as to what exactly the "harm" consists of, the defence against which is at stake by the EU or Member State measure to be justified.

However, one will hardly encounter any contradiction if one notes that the theory of the fundamental right from Art. 8 CFR is still in search of a clear and sufficiently determined “object of protection”. Neither the European courts nor the data protection authorities in the EU have been able to develop a clear "theory of harm". It is striking how superficial and unspecific the statements on the protective purpose of Art. 8 CFR and the resulting consequences for the interpretation of the GDPR are in many official decisions and academic contributions. It is certainly not wrong to state that Art. 8 CFR is the EU fundamental right with the most vague protective purpose.

[132] *Nissenbaum*, Theoretical Inquiries in Law 2019 (20), 221.

It is also striking that precisely those contributions that remain particularly vague with regard to the protective purposes of Art. 8 CFR then argue in a particularly resolute manner when determining a concrete need for intervention to protect natural persons from alleged or actual impairments. In many cases, human beings are described as more ignorant, manipulable and sensitive than they assume themselves to be. Human beings are infantilized, as noted above. The fact that natural persons interpret and classify digital challenges differently is not reflected throughout: Data protection authorities in particular seem to conceive of such diverse natural persons as a homogenous mass whose risk assessment is identical and who must be protected in the same way (frequently with paternalistic intentions). The assertion by some data protection authorities that their risk and threat assessments are shared by all or even most EU citizens is questionable; it is also not supported by empirical evidence. It should be clear, however, that in a pluralistic society there is a wide divergence of views on what effective and fair information management should look like in an emerging new "digital constellation". In many cases, the plurality of views does not seem to be compatible with the data protection law's self-image of wanting to protect human beings from the alleged risks and dangers of the digital economy (and also from themselves and their choices).

In any case, anyone who follows the current discussions quickly realizes that the assessments of what constitutes "digital harm" are very far apart. This is not only true if one compares the political and scientific discussions in the USA and in the EU. Even within the EU, the assessments differ widely. In any case, it is certain that the fact that third parties collect and use personal information about a person cannot constitute as such a "harm" under data protection law within the meaning of Art. 8 (1) CFR. If one were to regard this as harm, one would be inclined towards a conception of human life that fundamentally knows no sociality and no integration into social contexts. It would be an inhuman conception of human life. Art. 8 CFR is based on the concept of human life in a social community: this is the starting point for the question of what an appropriate information order should look like, how information should be allocated, what constitutes appropriate protection, what instruments should be used to grant this protection in individual constellations (contract, consent, etc.), and what constitutes “digital harm” in the

sense of Art. 8 (1) CFR. Here, a distinction must obviously be made between contractually agreed processing and access to personal data outside of contractual relationships.

b) The substantive content of Art. 8 para. 1 CFR

If it is true that fundamental rights respond to historical experiences and political conflicts, it is inevitable to take into account the current political discussions about "digital harm" when searching for the meaning of Art. 8 (1) CFR. The interpretation of Art. 8 (1) CFR does not move in a vacuum, nor can it be done from a point in nowhere, but takes place in a concrete socio-cultural and socio-political environment. Art. 8 CFR is, to use Emile Durkheim's words,[133] a social fact - an entity that is the product of political practice and, in turn, carries juridical and political practice.[134]

In current discussions of data protection policy, a wide variety of risk, danger, and harm scenarios are painted (sometimes thoughtfully, sometimes in strident tones). They range from the impairment of human autonomy,[135] to accusations of disenfranchisement and exploitation,[136] to concerns about the destruction of the image that human beings have

[133] *Durkheim,* Les règles de la méthode sociologique, 19 ed. 1977, p. 57.
[134] Art. 8 CFR establishes a subjective juridical right. The theory of subjective individual rights has worked out that this statement raises at least four problems that require clarification: 1) What is the teleological nature of this right? (genuine empowerment or mere defense against damage, etc.?); 2) What is the essence and meaning of this right (universal legal position, which must be attributed to every human being depending on time and place? Rights inherent in man by virtue of nature - or at any rate to be ascribed to him? Or: culture- and history-dependent attribution?); 3) Form (creation of spheres of individual arbitrariness, or providing people with an argument that must be decided upon - collectively - in the political process? 4) Concrete content (What does successful data protection at the constitutional level look like? (after all, one cannot simply say that the GDPR perfectly reflects Art. 8 CFR).
[135] Impairment is claimed above all when people have to act in decision-making situations in which they are "manipulated" or even "oppressed" ("oppression").
[136] There is often talk of "digital exploitation" or an illegitimate "extraction of value. In some cases, one also reads the accusation of "resource extraction. The accusation is that the data subjects' data that actually "belongs" to them is taken away without authorization and then turned into money by the "thieves.

of themselves.[137] In some cases, persons also claim that their right to equal treatment has been impaired.[138] It is obvious that many of these claims cannot be integrated into a fundamental rights theory of "digital harm" under Art. 8 (1) CFR. In particular, it does not need to be explained here that not everything that is politically displeasing can be considered "digital harm" in the sense of Art. 8 (1) CFR. This also follows from recital 75 of the GDPR, according to which only certain risks and harms are legally relevant. Moreover, fundamental rights provisions such as Art. 8 (1) CFR cannot protect supra-individual legal interests. Art. 8 (1) CFR cannot therefore protect man's image of himself. This is a matter of generic ethical questioning , which is not a direct subject of data protection under fundamental rights.[139] Art. 8 (1) CFR would also be obviously misunderstood if the provision were read as a guarantee aimed at promising natural persons a good and self-determined life in the digital world. No constitutional provision is seriously capable of establishing such guarantees. A fundamental rights provision must not promise more than protection against unreasonable interference - nor can it effectuate it in legal practice. Moreover, Art. 8 (1) CFR is a constitutional provision that does not dominate or eliminate the political leeway of the EU legislator, but only provides a framework for legislative action. The protection mandate of Art. 8 (1) CFR can therefore only extend to protection concerns that should not be made the subject of a political majority decision.

If we take the concern (described above) of enabling natural persons to live a self-determined life in the digital society as a guideline, the following protective goals can be attributed to Art. 8 (1) CFR:

---

[137] Some critics accuse the digital economy and the practices developed there of damaging the self-image of the human being - for example, by making the human being "readable," by producing "data twins" from the human being, by confronting the human being with biopolitical "data doubles. Other critics speak of a "commodification of the human being," of "biospecting," and of a colonization of the human lifeworld.

[138] More recently, digital business models have been accused on the one hand that the services offered discriminate between different groups or people, thus compromising the value of equal treatment. On the other hand, it has been claimed that the revenues that can be generated from digital business models are unfairly distributed.

[139] The EU legislator can address such protection concerns legislatively, but in doing so must respect the liberties of the data subjects.

First, Art. 8 (1) CFR must protect data subjects from an unreasonable encroachment on their digital autonomy. In this regard, it is a matter of combating measures and actions that cause a normatively inappropriate erosion or diminution of natural persons' right to self-determination in the digital society. Protection must extend to natural persons' ability to formulate first- and second-order preferences in a sufficiently independent process based on critical reflection and free from undue influence. But protection must also extend to the preservation of that legal, socio-cultural, and economic space in which a life plan based on these preferences can be realized. Secondly, it must be ensured that data subjects are not subject to inappropriate discrimination when formulating and implementing a life plan in the digital society.[140]

This protection is directed first and foremost against EU and Member State measures within the scope of application of EU law (Article 51 (1) CFR). At the same time, however, Art. 8 (1) CFR also obliges the EU institutions and, within the scope of application of the Charter, the Member State institutions to ensure that the actions of private individuals do not unduly undermine natural persons' digital autonomy. Art. 8 (1) CFR thus establishes a duty to protect.

Once the requirements of Art. 8 (1) CFR are laid out in detail, it is possible to see where the EU legislator has complied with fundamental rights requirements in enacting the GDPR and where it has made legal policy decisions within a decision-making framework opened up by fundamental rights. The view that the standard of protection envisaged by Art. 8(1) CFR has been met exactly by the GDPR is not convincing in terms of fundamental rights theory and would also have problematic consequences: Any amendment to the GDPR that would lower the standard of protection even slightly would be a violation of fundamental rights.

[140] It is an open question whether Art. 8 CFR also contains a guarantee for fair economic distribution. If one assumes that personal data has an economic value or assigns the data to the individual in some other way ("data as labour"), it does not seem impossible to conclude that Art. 8 (1) CFR contains a mandate to protect against unilateral "exploitation." However, this potential interpretation has so far no support in the case law of the EU courts and the practice of the data protection authorities. It would raise difficult questions of substance and competence.

c) Digital "harm" in contractual relationships?

In the following, the article will not deal in the abstract with the question of the extent to which the protection mandate of Art. 8 (1) CFR allows access to and processing of personal data, especially outside of contractual relationships. Rather, it is a matter of identifying the standards of protection required by Art. 8 (1) CFR for data processing in contractual relationships.

The answer to this is clear in principle: none of the three protection goals developed above are impaired when data subjects enter into contracts with companies in the digital economy that have as their object one of the common digital business models that are the subject of this study.[141] Digital autonomy is not impaired by these contracts, but rather realized. EU consumer contract law and the contract laws of the Member States ensure that the contracts concluded are not only self-determined from a formal point of view, but that there is also material private autonomy. Data processing in contractual relationships is characterized by the fact that the parties face each other in a legal relationship whose fundamental reciprocity and fairness of interests is ensured by contract law; moreover, the assessment of the benefit is the responsibility of the two contracting parties. Both parties have entered into this relationship because they assume that the commitment is more in line with their interests than a state outside the contract.[142]

Even a closer look does not call this general statement into question. None of the business models currently being developed in the digital economy provides for practices that may not be the subject of a contractual agreement concluded transparently and fairly. This also applies to contracts for the provision of services financed by behavioural advertising. [143] It is simply not recognizable why it should be incompatible with

---

[141] See I. above.
[142] *Hofmann,* „Absolute Rechte“ an Daten – immaterialgüterrechtliche Perspektive in: Pertot (eds.), Rechte an Daten, ed. 2020, p. 9 (14).
[143] It is not evident at the outset that personalized advertising impairs people's capacity for self-determination in such a way that one could speak of a tangible loss of digital autonomy. Sweeping assertions without empirical evidence fall short here. If a business model as such were to be incompatible with Art. 8 (1) CFR, this would also have to

the idea and the legal concept of digital autonomy if a person contractually chooses a service financed through behavioral advertising, especially if the service is rendered free as a consequence. Certainly, behavioral advertising, like all advertising, is meant to influence the human decision-making process. However, it is already not clear in which instances it promotes this process and in which effects of disruption are manifested. In addition, the intensity of the effects of behavioral advertising are typically so low that it is not possible to speak of a relevant impairment according to Art. 8 (1) CFR.[144] If it were possible to prove concrete harmful effects of this form of advertising, the data protection authorities would have long since invoked such findings. But that is not the case. In empirical terms, the relevant statements by the data protection authorities are completely insufficient - or purely speculative.

It does not require any further explanation here that none of the currently widespread digital business models leads to unreasonable unequal treatment of natural persons in the digital society, which is incompatible with the protection mandate of Art. 8 (1) CFR. Nor does "exploitation" occur in data processing in contractual relationships: it is up to the informed data subject to decide whether to use the service provided by the company, which may include processing of personal data. A data protection authority does not have proper standards to make this decision for the data subject. It cannot substitute its calculation of benefits for the calculation of benefits of the data subject.

It is not evident that any of the digital business models currently offered and implemented in effective contracts would impair the digital autonomy of the contracting data subjects in such a way that the level of protection sought by Art. 8 (1) CFR would be compromised.

Art. 8 (1) CFR serves to protect the self-determination of natural persons. The fundamental rights provision is not a lever for EU or Member State paternalism. No harm has ever been empirically demonstrated that could justify the assumption that the use of Art.

---

apply to all forms and designs. In view of the fact that personalized advertising can take very different forms, this cannot be justified at all.

[144] If "digital damage" were actually to be observed here, it could not be remedied by applying Art. 6(1)(a) GDPR either.

6 (1) (b) GDPR would cause a shortfall in the level of protection required by Art. 8 (1) CFR. To the contrary, it must be assumed that the protection mandate of Art. 8 (1) CFR is met when concluding and implementing contracts of the type discussed here on the basis of Art. 6 (1) (b) GDPR.

V. The doctrinal structure of Art. 6 1) (b) GDPR

The above considerations can be made fruitful for dogmatic purposes. The legal understanding of Art. 6 (1) (b) GDPR must correspond to the systematic position of the provision as one of several justifications of equal legal status and equivalent value to Art. 6 (1) (a) GDPR. The provision must be interpreted in light of its functional-teleological meaning and purpose. Art. 6 (1) (b) of the GDPR can only be understood at all if the provision is interpreted in the context of the provisions of a digital contract law.[145] Anyone who ignores this background (or does not even take note of it) cannot give the provision any meaning. For the scope of application of Art. 6 (1) (b) GDPR, it is therefore important on the one hand to open up sufficient scope for private autonomy. In a free legal and social order, natural persons must be given room to express their values, interests, and preferences. The paternalistic reflex to dictate to others how they must define their interests in a "well-understood" way must not be yielded to.

This interpretation leads to the following principles guiding the application of Art. 6 (1) (b) GDPR:

1. Relevance of the concrete content of the specific contract

When applying Art. 6 (1) (b) GDPR, the concrete content of the contract that the controller has concluded with the data subjects must be identified and set as the benchmark in each and every case. This content must be determined on the basis of the rules of the relevant national contract law. While the EDPB does not have jurisdiction to determine the validity of contracts pursuant to national contractual law, Art. 6 (1) (b) GDPR nevertheless forces national data protection authorities to deal with (possibly unusual) preliminary questions as to the interpretation of the substance and fundamental objectives of the contract. This is however unavoidable when applying the necessity test under Art. 6 (1) (b) GDPR in a meaningful way. Data protection authorities do not do justice to this provision if they talk about the (supposed) content, the main and secondary purposes, or the ‘nature’ of a contract in the abstract and without specific reference to what

[145] See *Sattler,* JZ 2017 (72), 1036.

has been actually agreed. It is their task to establish, on the basis of the relevant contract law, what has been made the substance of the contract.

a) Necessity of determining the "exact rationale" of the contract actually concluded

The European data protection authorities have repeatedly stated that the application of Art. 6 (1) (b) GDPR depends on 'determining the exact rationale of the contract, i.e. its substance and fundamental objective'.[146] It is agreed that the 'fundamental and mutually understood contractual purpose' is important (paragraph 113). As a consequence, it is necessary to clarify, by use of relevant contract law standards of interpretation, what has been contractually agreed between two parties. This has been stated explicitly by the EDPB: "The EDPB recalls that for the assessment of necessity under Art. 6 (1) (b) GDPR, '[i]t is important to determine the exact rationale of the contract, i.e. its substance and fundamental objective, as it is against this that it will be tested whether the data processing is necessary for its performance' ".[147] As the EDPB has previously stated, regard should be given to the particular aim, purpose, or objective of the service and, for applicability of Art. 6 (1) (b) GDPR, it is required that the processing is

[146] *Article 29 Working Party*, Overview of results of public consultation on Opinion on legitimate interests of the data controller (Opinion 06/2014), 14 November 2014, https://ec.europa.eu/justice/article-29/press-material/public-consultation/notion-legitimate-interests/files/20141126_overview_relating_to_consultation_on_opinion_legitimate_interest_.pdfp. 17; *European Data Protection Board*, Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR), 5 December 2022, https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-32022-dispute-submitted_en, para. 112 with reference to the opinion of the WP29 Committee.
[147] *ibid.*, Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR), 5 December 2022, https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-32022-dispute-submitted_enpara. 89; *ibid.*, Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding WhatsApp Ireland Limited (Art. 65 GDPR), 5 december 2022, https://edpb.europa.eu/system/files/2023-01/edpb_bindingdecision_202205_ie_sa_whatsapp_en.pdf, para. 105.

objectively necessary for a purpose and *integral* to the delivery of that contractual service to the data subject."[148]

It depends on the applicable contract law which concrete connection must exist between the declarations of intent of the contracting parties involved. Contract law also decides whether and how a valid contract has been concluded if there are differences of opinion.[149] In particular, contract law determines what has been agreed in the regularly occurring case that the parties' ideas were (and are) not entirely congruent.[150] Data protection law cannot replace these contract law tests; it is not contract law in disguise. Art. 6 (1) (b) of the GDPR is also not an instrument for overriding civil law assessments. This requires a contract law determination of the content of the concluded contract that cannot be replaced by vague and obscure general statements. In its Binding Decision 3/2022, the EDPB indulges in dark intimations about the problems of the contract concluded between the data controller and its users. It claims, without evidence or analysis, that the controller's offer was formulated in a rather non-transparent manner (e.g., paragraph 123), without explaining why it has the authority to make this (contract law) determination more properly within the competence of Member State courts, and also leaving open whether and how this is relevant to the content of the agreement. It cites questionable and unrepresentative opinion surveys about the views of part of the general

[148] *ibid.*, Binding Decision 2/2022 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR, 8 July 2022, https://edpb.europa.eu/system/files/2022-09/edpb_bindingdecision_20222_ie_sa_instagramchildusers_en.pdf, para. 89.

[149] In this case, the EDPB seems to want to carry out a data protection assessment as to whether there is "a genuine mutual understanding on the contractual purpose" (*ibid.*, Guidelines 2/2019 on the processing of personal data under Art. 6 (1) (b) GDPR in the context of the provision of online services to data subjects, 8 October 2019, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf, para. 32. However, the benchmarks in this regard remain unclear.

[150] The EDPB claims in the Guidelines 2/2019 that users of a service are often already unaware of what information is collected (example: tracking of user behavior for advertising purposes). It argues that this is also often not apparent from the nature of the service provided (ibid., para. 4). It is an empirical question whether these claims are true; the EDPB cites no empirical evidence. In any case, in 2023, the question is whether the claims about people's ignorance and cluelessness that have been made repeatedly for 20 years are still true.

population of an EU Member State (paragraph 97) instead of assessing the specific content of the actual contract and addressing any discrepancies between the contracting parties' ideas of the purpose of the agreement. It is conspicuous that the EDPB repeatedly defines what the 'main purpose' of the contract is without concrete reference to the content of the legally agreed upon general terms and conditions of the specific contract.[151]

b) Inadmissibility of the use of idealized or hypothetical contracts

Data protection authorities are thus not permitted to base their application of Art. 6 (1) (b) GDPR on hypothetical contracts. The EDPB's approach must therefore be rejected. The EDPB substitutes its ideal of a good and appropriate digital service for the concretely agreed offer. The EDPB's comments are obviously based on the idea that it is not only possible for a company to operate a social network without behavioral advertising, but that this hypothetical alternative should also serve as the standard of review under data protection law. The EDPB's decision is not based on the service agreed in the specific contract, but on a hypothesized and typified ideal. This idealization concerns the financing side of the service and thus an essential aspect that belongs to the core of the entrepreneurial freedom protected in Art. 16 CFR.[152] The question of how this hypothesized and typified ideal is derived and why it is decisive is not answered, let alone raised, by the EDPB.[153]

Anyone who attempts to reduce the scope of Art. 6 (1) (b) GDPR (either by excluding certain contracts/business models in principle or by claiming that certain elements of a business model are not "necessary") is reducing digital autonomy and therefore cannot rely on Art. 8(1) CFR. It is then a matter of enforcing policy preferences. If one moves

[151] For example, *European Data Protection Board*, Binding Decision 2/2022 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR, 8 July 2022, https://edpb.europa.eu/system/files/2022-09/edpb_bindingdecision_20222_ie_sa_instagramchildusers_en.pdf, para. 129.
[152] See chapter IV. 3. above.
[153] The EDPB speaks in the Guidelines 2/2019, para. 32, of the standard of the "reasonable view of the data subject when concluding the contract". This openly expresses the paternalistic concern. The EDPB claims to be able to decide what is the "reasonable view" of the persons concluding contract.

away from the contract and the agreements contained therein and makes hypothetical or idealized contracts the controlling standard for the necessity test, one moves into legal policy territory. Legal standards for the choice of such constructions are found neither in Art. 8 (1) CFR nor in the GDPR, nor has the EDPB been democratically granted these powers.

There is then nothing more than the subjective opinion and the more or less arbitrary evaluations of the data protection authorities. The standards that determine whether this question is to be answered in the affirmative or in the negative are consistently not revealed. As a result, it seems to be a matter of subjective opinion as to which contractual arrangements are prudent, sensible or appropriate in the digital society. This becomes clear, for example, in an analysis of EDPB Opinion 1/19, where certain forms of personalized service are approved, while forms of behavioral advertising are to be excluded from the scope of Art. 6 (1) (b) GDPR for reasons that are not explained in detail.

c) Inadmissibility of the quasi-political evaluation of digital business models

In the EDPB's view, the decision as to whether the contract actually concluded or a hypothetical-idealized contract is selected for the examination of Art. 6 (1) (b) GDPR, depends on whether the digital business model behind the contract actually concluded corresponds to the EDPB's subjective preferences. In this respect, the EDPB claims a legal evaluation of the business model of digital companies. This was already observed in the Guidelines 2/2019 (processing of personal data under Art. 6 (1) (b) GDPR) drafted by the EDPB. However, the standards applied remain unclear. The only thing that is clear is that certain manifestations of personalized advertising are considered harmful and disagreeable by the members of the EDPB. The EDPB also adopts a similar approach in Binding Decision 3/2022: Here, too, it is implicitly examined whether the contractually agreed business model is "good" or "bad". The EDPB is of the opinion that business models which finance a free service through the placement of advertising are basically "good". In contrast, the EDPB assumes that a business model that provides for the financing of a free service through the placement of behavioural advertising is "bad" and therefore cannot be based on Art. 6 (1) (b) GDPR.

It is not difficult to see that the introduction of such normative standards is incompatible with the requirements of the GDPR. The EDPB shifts the standard of review.[154] Instead of examining whether the processing carried out by the controller is necessary for the implementation of what has been specifically contracted, the EDPB checks whether the business model developed by the controller and agreed in the contracts with the users is, in its view, preferable. However, it is not the competence of the EDPB to measure real digital business models against hypothetical models. Why should the members of the EDPB have a special ability to make statements about how an idealized ('good') service should look ? They are not ethicists, nor are they called to make legal policy (or disregard legal policy that has been set by EU legislatures). Why should the subjective ideas of the members of the EDPB be more relevant than those of other actors on this issue, let alone the corresponding will of the controller and the data subject, as manifested in the contract? Finally, what exactly are the standards for determining whether a business model is still 'good' or already 'bad'? Anyone who ponders these questions must come to a single conclusion: It is beyond the legal competence of the EDPB to substitute for the concrete content of the contract between the controller and its contractual partners hypotheses and ideals that have no basis in written EU law, but are based solely on subjective preferences of the members of the EDPB.

The EDPB's claim to review the legitimacy of business models also raises constitutional law concerns. In the representative democracy of the European Union (Article 2 TEU, Art. 10 (1) TEU), the administrative authorities and bodies of the EU are responsible for implementing the law. They have the power and the right to exploit legal leeway, taking into account the requirements of EU primary law, including EU fundamental rights, using teleological considerations, and developing expedient solutions. However, if administrative authorities, which are not subject to direct democratic control and supervision, claim to be able to go beyond the applicable law and to effectively create new regulations that are political in nature, problems arise with regard to the rule of law and democracy (Article 2 TEU).

[154] The shift in the standard of review is indicated in paragraph 111, which no longer refers only to what has been specifically agreed, but also to the 'nature of the service'.

The EDPB's efforts to make Art. 6 (1) (b) GDPR a lever to review entrepreneurial business models of the digital economy for their ethical or political appropriateness is an example of where the EDPB crosses the line. The EDPB breaks away from the (restrictive) wording of Art. 6 (1) (b) GDPR and claims power to develop its own opinion about what constitutes a righteous business model. The EDPB's intention to deny companies the ability to invoke Art. 6 (1) (b) GDPR to process personal data if their business models fail to meet the EDPB's hypothetical alternative model encroaches on the competences of the EU legislature and amounts to legal policy. However, in the democratic system of the EU, an independent administrative authority such as the EDPB does not have the power to engage in such significant law making decisions; even more, it does not have the right to do so by twisting the wording of Art. 6 (1) (b) GDPR. To the extent that an independent administrative authority makes policy and creates new rules beyond its mandate vested by the law, it destroys the democratic legitimacy under which it operates.

Art. 6 (1) (b) GDPR is not a lever with which data protection authorities can 'sanction' business models they subjectively and partially consider disagreeable. If the members of a data protection agency or of the EDPB think that behavioural advertising is really as dangerous as they claim, they should contact EU lawmakers and push for a change in the law. What they must not do is seek, in effect, to change democratically enacted legislation to suit their world view via the back door.

Of course, this does not mean that a company can freely define its business model and implement any business model on the market. Contractual protection of its data processing practices (also in terms of data protection law) can of course only be effective where contractual partners are found who are willing to enter into a business relationship in the first place. The attractiveness of the service offered must be so great that customers agree to it. The evaluation of the business model must therefore be carried out by the individuals; the data protection authorities cannot put themselves in their place.

d) Inadmissibility of data protection paternalism

As a consequence, data protection authorities must respect what the undertaking has agreed with its users in a legally valid contract. Data protection law is not an instrument

of paternalism. Nor is it an instrument with which data protection authorities can impose their subjective view of which business models in the digital economy are ethically, politically or legally good. Anyone who believes that a particular business model should be banned must persuade the legislature to enforce this through outright prohibition, administrative regulation, or civil law restrictions.

2. Interrelationships between contract law and data protection law

It would be a misunderstanding to assume that the above considerations lead to the undermining of the objectives of data protection. The opposite is the case. EU consumer protection law and the legal systems of the member states protect the material autonomy of data subjects and prevent digital damage. Moreover, Art. 5 GDPR has a reinforcing effect on contract law: the transparency obligations provided for there must also be complied with if a digital company relies on Art. 6 (1) (b) GDPR. In this respect, they formulate minimum standards for the relevant contract law. However, the requirements in this regard must not be exaggerated: It does not strengthen digital autonomy if data subjects are confronted with excessively long descriptions of the content of the contract and the processing operations provided for therein.

3. Possibility of interpreting contract law in accordance with fundamental rights

Sufficient protection of data subjects is not only brought about by the fact that contract law and data protection law are intertwined via Art. 5 GDPR (2. above). The data protection authorities, like the courts, are free to examine whether the relevant contract law will comply with the protection standards of Art. 8(1) CFR by way of an interpretation in conformity with fundamental rights in cases where the application of Art. 6 (1) (b) CFR is at stake.

EU Member State contract law must obviously be interpreted in accordance with fundamental rights, including Art. 8 CFR. If a controller chooses wording in its general terms and conditions that conceals its intentions and the contractual purposes more than it discloses them, this can lead a Member State court to declare the invalidity of the contract - which would prevent the controller from relying on Art. 6 (1) (b) GDPR - in light of

Art. 8 CFR.[155] If Member State courts have identified contract law deficits, they can be eliminated by such an interpretation. The exclusion of the application of Art. 6 (1) (b) of the GDPR (and the associated reference to Art. 6 (1) (a) of the GDPR) is not capable of doing so.

4. Necessity of the processing

The justification ground of Art. 6 (1) (b) GDPR can only legitimize processing if it is necessary for the performance of the contract. The reference point, as explained above, is the specific content of the contract concluded between the parties. The EDPB rightly states that it is not decisive that the processing itself is mentioned in the contract: "On the other hand, processing may be objectively necessary even if it is not explicitly mentioned in the contract."[156] The decisive factor is whether the obligations imposed on the company by the contract or the company's contractually negotiated powers can only be fulfilled if the data processing in question takes place. Contracts regularly give companies the freedom to determine performance and to act, the exercise of which may make data processing necessary.[157]

---

[155] *European Data Protection Board*, Guidelines 2/2019 on the processing of personal data under Art. 6 (1) (b) GDPR in the context of the provision of online services to data subjects, 8 October 2019, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf, paras. 9, 13: Contracts within the meaning of lit. b) must comply with the requirements of contract law (in particular consumer protection law).

[156] Ibid., para. 27.

[157] The EDPB's view that data processing is only necessary if it was carried out to perform a contractual obligation of the company (*European Data Protection Board*, Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR), 5 December 2022, https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-32022-dispute-submitted_en, para. 118) cannot be correct because the "performance of a contract" under Art. 6(1)(b) GDPR) also extends to those acts that the company can take in the exercise of its right to determine the content of its service, but is not contractually obliged to perform.

According to the above findings, the necessity test is misused if it results in the determination that the company could also define its service offering differently (and make it the subject of a contract in this other form). The necessity test would also be misunderstood if it amounted to a finding that the consumer would have meaningfully concluded a different contract. Art. 6 (1) (b) of the GDPR is also not a lever to intervene in and reshape existing contractual relationships. The desire under data protection law to force natural persons to conclude "good" contracts cannot be realized via Art. 6 (1) (b) GDPR. This would require legislative measures.

The necessity test must be carried out "objectively" in the sense that the causal link between the objective of realizing the subject matter of the contract and the processing planned or intended for this purpose must be shown.[158] It is certainly not compatible with the GDPR to leave the assessment of necessity entirely to the controller . On the other hand, it is also clear from what has been said that there is no standard of objectivity that can be detached from the purposes and interests of both the contracting parties (the agreement between the contracting parties cannot simply be replaced by an assessment of administrative authorities or courts).

5. Inadmissibility of an abusive application of Art. 6 (1) (b) GDPR

Finally, it should be noted that it is inherent in every legal empowerment that any legal basis be subject to an abuse proviso. A controller must be denied the right to invoke Art. 6 (1) (b) GDPR if the use of this justification is abusive regardless of the fact that the processing has been effectively contractually agreed. However, such a review should not be carried out hastily and out of paternalistic instincts. The accusation of abuse can only be raised where a data processing practice would be irreconcilable with notions of fundamental legal appropriateness. To simply conclude that business models relying on behavioral advertising are abusive by default is out of the question. In the year 2023, it

[158] *ibid.*, Guidelines 2/2019 on the processing of personal data under Art. 6 (1) (b) GDPR in the context of the provision of online services to data subjects, 8 October 2019, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf, para. 27.

would be almost absurd to say that these business models, which have been common for two decades now and have been used by millions of EU citizens for many years to enable them to benefit from a range of useful services free of charge are inherently abusive.[159] The EDPB does not present any arguments that could justify this conclusion.

[159] See *ibid.*, Binding Decision 2/2022 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR, 8 July 2022, https://edpb.europa.eu/system/files/2022-09/edpb_bindingdecision_20222_ie_sa_instagramchildusers_en.pdf, para. 57, questioning the utility of personalization.

Bibliography

All internet resources were accessed on 23 April 2023.

Amstutz, Marc: Dateneigentum Funktion und Form, AcP 2018 (218), pp. 438–551

Ausloos, Jef/Mahieu, Rene/Veale, Michael: Getting Data Subject Rights Right JIPITEC 2019 (10), pp. 283–309

Baldwin, Robert: From Regulation to Behaviour Change: Giving Nudge the Third Degree, The Modern Law Review 2014 (77), pp. 831–857

Bauer, Hannes/Fuhr, Alfred/Heynike, Francois, et al.: Risikofeststellung Dateneigentum, in: Datenschutz, Stiftung (eds.), Dateneigentum und Datenhandel. DatenDebatten Band 3, Berlin, 2018, pp. 15–28

Beaulieu, Anne/Leonelli, Sabina: Data and Society: A Critical Introduction, Los Angeles, 2021

Bertschek, Irene/Bonin, Holger/Kühling, Jürgen, et al., Entwicklung eines Konzepts zur Datenallmende. Erstellt im Auftrag des Bundesministeriums für Arbeit und Soziales 2021) <https://www.bmas.de/SharedDocs/Downloads/DE/Publikationen/Forschungsberichte/fb-581-entwicklung-eines-konzepts-zur-datenallmende.pdf?__blob=publicationFile&v=2>

Black, Steve: Who Owns Your Data?, Ind. L. Rev. 2022 (54), 2, pp. 305–339

Braun, Matthias/Hummel, Patrik: Data justice and data solidarity, Cell Patterns 2022 (3), 100427, pp. 1–8

Brillowski, F./Overhage, V./Tegetmeyer-Kleine, T., et al.: Overcoming Data Scarcity in the Quality Control of Safety-Critical Fibre-Reinforced Composites by means of Transfer and Curriculum Learning, in: Herberger, D./Hübner, M. (eds.), Proceedings of the Conference on Production Systems and Logistics, Hannover, 2022, pp. 83–90

Buchner, Benedikt: Informed consent in Germany, in: Vansweevelt, Thierry/Glover-Thomas, Nicola (eds.), Informed consent and health: a global analysis, Cheltenhem/Northhampton, 2020, pp. 216–234

Bunnenberg, Jan Niklas: Privates Datenschutzrecht –Über Privatautonomie im Datenschutzrecht – unter besonderer Berücksichtigung der Einwilligung und ihrer vertraglichen Kopplung nach Art. 7 Abs. 4 DS-GVO, Baden-Baden, 2020

Citron, Danielle Keats: The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age, London, 2022

Clifford, Damian/Graef, Inge/Valcke, Peggy: Pre-formulated Declarations of Data Subject Consent—Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections, German Law Journal 2019 (20), pp. 679–721

Cofone, Ignacio: Beyond Data Ownership, Cardozo L. Rev. 2021 (43), 2, pp. 501–572

Cohen, Julie E.: Between truth and power the legal constructions of informational capitalism, Oxford, 2019

ibid.: Turning Privacy Inside Out, Theoretical Inquiries in Law 2019 (20), pp. 1–32.

ibid.: What Privacy is for, Harv. L. Rev. 2013 (126), pp. 1904–1933

Cohen, Julie E. : Configuring the Networked Self, New Haven, 2012
DeBrabander, Firmin: Life after privacy reclaiming democracy in a surveillance society, Cambridge, 2020
Drechsler, Laura: Defining personal data transfers for the context of the General Data Protection Regulation a critical perspective on the Guidelines 5/2021 of the European Data Protection Board, PinG 2022 (10), pp. 24–29
Durkheim, Émile: Les règles de la méthode sociologique, 19 ed. 1977
Esposito, Fabrizio: Book Review: Nudge and the Law: A European Perspective. by Alberto Alemanno and Anne-Lise Sibony (Eds.) 2015, European Journal of Risk Regulation 2015 (6), pp. 331–340
Fazlioglu, Muge: The United States and the EU's general data protection regulation, in: Cortez, Elif Kiesow (eds.), Data protection around the world, The Hague, 2021, pp. 231–248
Feiler, Lukas/Forgó, Nikolaus/Nebel, Michaela: The EU General Data Protection Regulation (GDPR): a commentary, Surrey, 2 ed. 2021.
Ferretti, Federico: Data protection and the legitimate interest of data controllers: much ado about nothing or the winter of rights?, Common Market Law Review 2014 (51), pp. 843–868
Fierens, Michiel/Ooms, Wannes, Personal data as a commodity: is the door open for small-scale data processing? (KU Leuven CiTiP, 4 August 2022)
Floridi, Luciano: On Human Dignity as a Foundation for the Right to Privacy, Philosophy & Technology 2016 (29), pp. 307–312
Fries, Martin: Data as counter-performance in B2B contracts in: Lohsse, Sebastian/Schulze, Reiner/Staudenmayer, Dirk (eds.), Data as counter-performance – contract law 2.0?, Baden-Baden, 2020, pp. 253–261
Gerhalter, Marek: Internationale Datentransfers im Lichte der DSGVO und der DSRL-PJ, Wien, 2021
Gola, Peter: Datenschutz-Grundverordnung VO (EU) 2016/679 – Bundesdatenschutzgesetz. Kommentar, München, 3 ed. 2022
Gstrein, Oscar J./Beaulieu, Anne: How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches, Philos Technol 2022 (35), 1, pp. 1–38
Hacker, Philipp: Datenprivatrecht, DGRI-Jahrbuch 2021 (2019/2020), pp. 1–744
ibid.: Manipulation by algorithms. Exploring the triangle of unfair commercial practice, data protection, and privacy law, European Law Journal 2021 (Version Online), pp. 1–34
ibid.: Nudging and Autonomy – A Philosophical and Legal Appraisal, in: Micklitz, Hans-W./Sibony, Anne-Lise/Esposito, Fabrizio (eds.), Handbook of Research Methods in Consumer Law, Cheltenham/Northampton, 2017, pp. 77–118
Hansen, Pelle Guldborg/Jespersen, Andreas Maaløe: Nudge and the Manipulation of Choice: A Framework for the Responsible Use of the Nudge Approach to Behaviour Change in Public Policy, European Journal of Risk Regulation 2013 (4), pp. 3–28
Heisenberg, Dorothee: Negotiating Privacy, Boulder, Colorado, 2005
Hofmann, Franz: „Absolute Rechte“ an Daten – immaterialgüterrechtliche Perspektive, in: Pertot, Tereza (eds.), Rechte an Daten, Tübingen, 2020, pp. 9–32

Hornung, Gerrit/Papakōnstantinu, Euangelos/Spicker, Indra: European General Data Protection Regulation. Article-by-Article Commentary, Baden-Baden, 2022
Hummel, Patrik/Braun, Matthias/Dabrock, Peter: Own Data? Ethical Reflections on Data Ownership, Philosophy & Technology 2021 (34), pp. 545–572
Jurcys, Paulius/Donewald, Christopher/Fenwick, Mark, et al.: Ownership of User-Held Data: Why Property Law is the Right Approach, Harvard Journal of Law & Technology Digest 2021 pp. 1–30
Kerber, Wolfgang: Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives GRUR International 2022 (72), pp. 120–135
Klement, Jan Henrik: Öffentliches Interesse an Privatheit. Das europäische Datenschutzrecht zwischen Binnenmarkt, Freiheit und Gemeinwohl, JZ 2017 (72), pp. 161–170
Krzysztofek, Mariusz/Behlert, Marcin/Paszkowski, Paweł: GDPR personal data protection in the European Union, The Hague, 2021
Kühling, Jürgen/Buchner, Benedikt: Datenschutz-Grundverordnung BDSG. Kommentar, München, 4 ed. 2023
Ladeur, Karl-Heinz: "Big Data" im Gesundheitsrecht - Ende der "Datensparsamkeit"? , DuD 2016 (40), pp. 360–364
Langhanke, Carmen: Daten als Leistung – Eine rechtsvergleichende Untersuchung zu Deutschland, Österreich und der Schweiz, Tübingen, 2018
Leistner, Matthias/Antoine, Lucie/Sagstetter, Thomas: Big Data Rahmenbedingungen im europäischen Datenschutz- und Immaterialgüterrecht und übergreifende Reformperspektive, Tübingen, 2021
Leitner, Lisa Maria: Das Rechtsinstitut der Einwilligung im Datenschutzrecht im Lichte der DS-GVO, Graz, 2021
Linardatos, Dimitrios: Autonome und vernetzte Aktanten im Zivilrecht, Tübingen, 2021
Lynskey, Orla: The Foundations of EU Data Protection Law, Oxford, 2015
Mayer-Schoenberger, Viktor: Generational development of data protection in Europe, in: Agre, Philip/Rotenberg, Marc (eds.), Technology and Privacy: The New Landscape, Cambridge, Massachusetts 1997, pp. 219–242
Mischau, Lena: Market Power Assessment in Digital Markets – A German Perspective, GRUR International 2020 (69), pp. 233–248
Möslein, Florian/Beise, Clara: Datensouveränität als Privatautonomie, in: Augsberg, Steffen/Gehring, Petra (eds.), Datensouveränität – Positionen zur Debatte, München, 2022, pp. 103–120
Mulligan, Deirdre K./Koopman, Colin/Doty, Nick: Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy, Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 2016 (374), 20160118, pp. 1–17
Nettesheim, Martin: Critical Comments on the European Data Protection Board's Understanding of Contracts as A Ground to Process Personal Data, EU Law Live 2023 (129), Weekend Edition, pp. 3–16
ibid., Digital Autonomy in Contractual Relationships (Verfassungsblog, 2022) <https://verfassungsblog.de/dig-aut-contr-rel/>
Nissenbaum, Helen: A contextual approach to privacy online, in: Savirimuthu, Jospeh (eds.), The library of essays on law and privacy. Part 3: Security and privacy, Farnham, 2015, pp. 32–48

ibid.: Contextual Integrity Up and Down the Data Food Chain, Theoretical Inquiries in Law 2019 (20), pp. 221–256
Nolin, Jan: Data as oil, infrastructure or asset? Three metaphors of data as economic value, Journal of Information, Communication and Ethics in Society 2019 (18), pp. 28–43
Paal, Boris P./Pauly, Daniel A./Ernst, Stefan: Datenschutz-Grundverordnung - Bundesdatenschutzgesetz, München, 3. ed. 2021
Pearce, Henry: Could the doctrine of moral rights be used as a basis for understanding the notion of control within data protection law?, Inf. Commun. Technol. Law 2018 (27), pp. 133–165
Peitz, Martin/Schweitzer, Heike: Ein neuer europäischer Ordnungsrahmen für Datenmärkte?, NJW 2018 pp. 275–279
Peukert, Alexander: Güterzuordnung als Rechtsprinzip, Tübingen, 2013
Rebonato, Riccardo: Taking Liberties – A Critical Examination of Libertarian Paternalism, London, 2012
Riehm, Thomas: Freie Widerrufbarkeit der Einwilligung und Struktur der Obligation – Daten als Gegenleistung?, in: Pertot, Tereza (eds.), Rechte an Daten, Tübingen, 2020, pp. 175–206
Riesenhuber, Karl: Die Einwilligung des Arbeitnehmers im Datenschutzrecht, Recht der Arbeit 2011 (64), pp. 257–265
Sandel, Michael J.: What money can't buy. The moral limits of markets, New York, 2013
Sattler, Andreas: Personenbezogene Daten als Leistungsgegenstand, JZ 2017 (72), pp. 1036–1046
ibid.: Personenbezug als Hindernis des Datenhandels, in: Pertot, Tereza (eds.), Rechte and Daten, Tübingen, 2020, pp. 49–86
Schafer, Burkhard: Of wicked wizards and indigo jackals: Legal regulation of privacy and identity in cultural comparative perspective, in: Buchner, Benedikt/Petri, Thomas (eds.), Informationelle Menschenrechte und digitale Gesellschaft, Tübingen, 2023, pp. 27–46
Scheibenpflug, Andreas: Personenbezogene Daten als Gegenleistung – Ein Beitrag Zur Rechtlichen Einordnung Datengetriebener Austauschverhaltnisse, Berlin, 2022
Schmitz, Moritz: Die Digitalisierung der gesetzlichen Formen, Passau, 2022
Schweitzer, Heike: Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung, GRUR 2019 pp. 569–580
Shoemaker, David W.: Self-exposure and exposure of the self: informational privacy and the presentation of identity, Ethics of Information Technology 2010 (12), pp. 3–15
Simitis, Spiros/Hornung, Gerrit/Spiecker Döhmann, Indra, et al.: Datenschutzrecht DSGVO mit BDSG, Baden-Baden, 1. Auflage 2019
Solove, Daniel J.: The meaning and value of privacy, in: Roessler, Beate/Mokrosinska, Dorota (eds.), Social Dimensions of Privacy: Interdisciplinary Perspectives, Cambridge, 2015, pp. 71–82
ibid.: Privacy Self-Management and the Consent Dilemma, Harv. L. Rev. 2013 (123), pp. 1880–1903
ibid.: A Taxonomy of Privacy, U. Pa. L. Rev. 2006 (154), pp. 477–564
ibid.: Understanding Privacy, Harvard, 2009

Solove, Daniel J./Citron, Danielle Keats: Risk and Anxiety: A Theory of Data Breach Harms, Tex. L. Rev. 2018 (96), pp. 737–786
Spiecker Döhmann, Indra/Papakōnstantinu, Euangelos/Hornung, Gerrit, et al.: General Data Protection Regulation. Article-by-Article Commentary, Baden-Baden, 1 ed. 2023
Steinrötter, Björn: Gegenstand und Bausteine eines EU-Datenwirtschaftsrechts, Recht digital 2021 (1), pp. 480–486
Sunstein, Cass R.: Choosing not to Choose, Duke L.J. 2014 (64), pp. 1–52
ibid.: Requiring choice is a form of paternalism, Journal of Behavioral Economics for Policy 2017 (1), pp. 11–14
Sydow, Gernot: DS-GVO, BDSG Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: Handkommentar, Baden-Baden, 3 ed. 2022
Thouvenin, Florent: Informational Self-Determination: A Convincing Rationale for Data Protection Law?, JIPITEC 2021 (12), pp. 246–256
Thouvenin, Florent/Weber, Rolf H./Früh, Alfred: Data ownership: Taking stock and mapping the issues, in: Dehmer, Matthias/Emmert-Streib, Frank (eds.), Frontiers in Data Science, Boca Raton, 2017, pp. 111–146
Veit, Raoul-Darius: Einheit und Vielfalt im europäischen Datenschutzrecht, Tübingen, 2023
Vrabec, Helena U.: Data subject rights under the GDPR – with a commentary through the lens of the data-driven economy, Oxford, 2021
Wein, Thomas: Data protection, cookie consent, and prices, Economies 2022 (10), 12, pp. 1–26
Weiß, Christian/Reisener, Nico: Datensparsamkeit, Datenvermeidung und Pseudonymisierung Problembewusstsein für Datenschutz in der Insolvenzverwaltung?!, ZInsO 2017 (20), pp. 416–420
Wendehorst, Christiane: Of Elephants in the Room and Paper Tigers How to Reconcile Data Protection and the Data Economy, in: Lohsse, Sebastian/Schulze, Reiner/Staudenmayer, Dirk (eds.), Trading Data in the Digital Economy – Legal Concepts and Tools, Baden-Baden, 2017, pp. 327–356
Wendehorst, Christiane/Schwamberger, Sebastian/Grinzinger, Julia: Datentreuhand – wie hilfreich sind sachenrechtliche Konzepte?, in: Pertot, Tereza (eds.), Rechte an Daten, Tübingen, 2020, pp. 103
Wolff, Heinrich Amadeus/Brink, Stefan/Albers, Marion: Datenschutzrecht. DS-GVO, BDSG, Grundlagen, bereichsspezifischer Datenschutz: Kommentar, 2. ed. 2022
Zech, Herbert: Daten als Wirtschaftsgut – Überlegungen zu einem „Recht des Datenerzeugers“, in: Wimmers, Jörg/Metzger, Axel (eds.), DGRI Jahrbuch, 2015, pp. 1
ibid.: Information als Schutzgegenstand, Tübingen, 2012
Zins, Chaim: Conceptual approaches for defining data, information, and knowledge, Journal of the American Society for Information Science and Technology 2007 (58), pp. 459-609

Governmental and Other Documents

Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217), 9 April 2014, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf>

ibid., Overview of results of public consultation on Opinion on legitimate interests of the data controller (Opinion 06/2014), 14 November 2014, <https://ec.europa.eu/justice/article-29/press-material/public-consultation/notion-legitimate-interests/files/20141126_overview_relating_to_consultation_on_opinion_legitimate_interest_.pdf>

European Academies, European Academies Science Advisory Council, FEAM,Deutsche Akademie der Naturforscher Leopoldina,, International sharing of personal health data for research, EASAC policy report 41, 2021, <https://easac.eu/fileadmin/PDF_s/reports_statements/Health_Data/2021_ALLEA_EASAC_FEAM_Policy-Report_International_Sharing_Health_Data_en.pdf>

European Commission, Amended Proposal for a Council Directive on the potection of individuals with regard to the processing of personal data and on the free movement of such data, , 15 October 1992, (COM(92) 422 final (SYN 287), <http://aei.pitt.edu/10375/1/10375.pdf>

ibid., A European Strategy of Data (COM/2020/66 final), 2020, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066>

ibid., 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) (SEC(2012) 72 final), 2012, <https://www.europarl.europa.eu/cmsdata/59702/att_20130508ATT65856-1873079025799224642.pdf>

ibid., Proposal for a Regulation of the European Parliament and the Councial 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) (COM/2012/011 final), 2012, <https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf>

ibid., Questions and Answers on the data protection reform package, 25 January 2012, <https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_1441>

ibid., Speech: Viviane Reding, European Commissioner for Justice, Fundamental Rights and Citizenship: 'A comprehensive approach on personal data protection in the European Union', 25 January 2012,

ibid., Speech: Viviane Reding, Vice-President of the European Commission, EU Justice Commissioner: 'Data protection reform – The EU as the global gold standard' 4 June 2014,

European Data Protection Board - European Data Protection Supervisor, Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), 4 May 2022, <https://edpb.europa.eu/system/files/2022-05/edpb-edps_joint_opinion_22022_on_data_act_proposal_en.pdf>

European Data Protection Board, Binding Decision 2/2022 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR, 8 July 2022, <https://edpb.europa.eu/system/files/2022-09/edpb_bindingdecision_20222_ie_sa_instagramchildusers_en.pdf>

ibid., Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR), 5 December 2022, <https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-32022-dispute-submitted_en>

ibid., Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding WhatsApp Ireland Limited (Art. 65 GDPR), 5 december 2022, <https://edpb.europa.eu/system/files/2023-01/edpb_bindingdecision_202205_ie_sa_whatsapp_en.pdf>

ibid., Guidelines 2/2019 on the processing of personal data under Art. 6 (1) (b) GDPR in the context of the provision of online services to data subjects, 8 October 2019, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf>

ibid., Guidelines 8/2020 on the targeting of social media users, Version 2.0, 13 April 2021, <https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf>

ibid., Statement 05/2021 on the Data Governance Act in light of the legislative developments, 19 May 2021, <https://edpb.europa.eu/system/files/2021-05/edpb_statementondga_19052021_en_0.pdf>

European Data Protection Supervisor, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, 17 March 2017, <https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf>

Federal Constitutional Court: Decisions of the Federal Constitutional Court. Volume 6: General right of personality, Baden-Baden, 1. Auflage 2022

Organisation for Economic Cooperation and Development. Working Party on Security and Privacy in the Digital Economy, Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking, 21 May 2014, <https://one.oecd.org/document/DSTI/ICCP/REG(2014)3/en/pdf>