Autonomy or Heteronomy
– Proposal for a two-tier interpretation of Art. 6 GDPR

Andreas Sattler[*]

To be published in: Lohsse/Schulze/Staudenmayer (Eds.), Data as Counter-Performance – Contract Law 2.0?, 5th Münster Colloquia on EU Law and the Digital Economy V, Nomos/Hart, 2020.

Last Update: June 2019

I. Introduction

Growing up is a complex challenge for individuals and societies alike. Parents teach their children: Never take candy from strangers! Once matured, most people have learned the lesson that "there is no such thing as a free lunch". However, if sweets are narrowed down to so-called "Cookies" and "free lunch" is exchanged for "free digital content" many consumers suddenly regress to unexperienced infants.

Experts in the area of behavioral economics have demonstrated it is not only children that find it hard to resist sweets and seemingly "free digital content". Experimental research reveals human biases, information asymmetries and a so-called privacy paradoxon,[1] thus shattering faith in human rationality and the efficient market hypothesis. Bounded rationality has not only become a descriptive feature of the *conditio humana*, the insights of behavioral economics are accepted as justification for legislation that aims at 'nudging' citizens to make better decisions. Accordingly, the foundation on which human dignity was originally based i.e. *Kant's* idea of a liberation from self-imposed immaturity, has increasingly been complemented by ideas of participatory empowerment.[2] Formal autonomy to conclude contracts and thereafter be bound by them (*pacta sunt servanda*) has – sometimes for good reason – been 'materialized' in order to enable superior individual choices (decision architecture) and to promote concepts of fairness.[3]

---

[*] Dr. jur., LL.M. (Nottingham), Senior Lecturer (Akad. Rat a.Z.), Ludwig-Maximilians-University, Munich.

[1] As regards the 'price for privacy': Sören Preibusch, Dorothea Kübler and Alastair R. Beresford, 'Price versus privacy. An Experiment into the competitive advantage of collecting less personal information', 2012 (available at: http://test.preibusch.net/publications/Preibusch-Kuebler-Beresford__Price_versus_privacy_experiment.pdf

[2] As regards privacy: Christoph Krönke, 'Datenpaternalismus – Staatliche Interventionen im Online-Datenverkehr zwischen Privaten, dargestellt am Beispiel der Datenschutz-Grundverordnung', DER STAAT 55: 319.

[3] Criticizing the principle of freedom to conclude contracts as 'mystifying beacon' Anne Röthel, 'Privatautonomie im Spiegel der Privatrechtsentwicklung: ein mystifizierendes Leuchtfeuer', in Christian Bumke and Anne Röthel,

This article cannot provide a detailed analysis of the different philosophical theories that support the notions of autonomy and heteronomy. Nevertheless, both terms can function as opposite beacons. As an analysis of the General Data Protection Regulation (GDPR) and the Directive on Certain Aspects concerning Contracts for the Supply of Digital Content and Digital Services (DCSD) illustrates, the European legislator has found shelter in a halfway house along the route between these two beacons. However, this halfway house is not built on solid middle ground nor on balanced compromise. Instead, the European legislator introduced two conflicting sets of rules[4] and entrusted the national courts and eventually the CJEU with the task of synchronization.

Academia in general and the fascinating volumes of *Münster Colloquia on EU Law and the Digital Economy* in particular can support such future synchronization. Hoping that it will contribute to such a prolific volume, this article commences with a short analysis of a current gap that is left by the GDPR and the DCSD (II). Hereafter, three prerequisites will be identified as starting point when trying to bridge this gap (III). Any new proposal would be redundant if existing options could provide for such synchronization therefore current options and their respective disadvantages will be illustrated (IV). Finally, this article proposes a two-tier interpretation of Art. 6 (1) GDPR[5] that could help the judiciary or the European legislator to reconcile the rules stipulated by the GDPR, the DCSD and general contract law (V).

II. Mind the Gap: Between Fundamental Right and Economic Commodity

Currently, there is an almost ideological conflict between proponents and opponents of rigid data protection. One side emphasizes that privacy is rooted in human dignity and is therefore sacrosanct. The other side, principally enterprises, search for correlations in huge sets of data thus exploiting the semantic level of personal data to increase knowledge. The business models of powerful platforms and the current legal framework illustrates this conflict between economic reality (1) and the legal framework (2).

Autonomie und Recht. Gegenwartsdebatten über einen rechtlichen Grundbegriff (Mohr Siebeck 2017, 91 ssq. In response and defending such freedom of contract: Karl Riesenhuber, Privatautonomie – Rechtsprinzip oder 'mystifizierendes Leuchtfeuer', ZfPW 2018, 352 ssq.

[4] This is probably a result of the fact that two different Directorates General were responsible for the respective proposal. GDPR: Directorate General JUST (Justice and Consumers), for the DCSD: Directorate General CONNECT (Communication Networks, Content and Technology).

[5] Hereafter all articles without further specification refer to the GDPR.

1. Fundamentals of platform economies

In recent years, multi-sided platforms (more generally referred to as intermediaries) have been the object of intense discussion. Many innovative platforms rely on a – at least – two-sided market structure. Currently, US enterprises, in particular *Google (Alphabet), Amazon, Facebook, Apple and Microsoft* (GAFAM) and their Chinese counterparts *Baidu, Alibaba and Tencent* (BAT) are the most successful intermediaries and have thus become synonyms for 'the platform economy'.

Many of the current business models of GAFAM and BAT – although to a different extent – depend on the processing of personal data. If viewed from a data subject's perspective, most two-sided platforms collect personal data at the front end and subsequently exploit and monetize it at the platform's back end. Targeted advertisement is based on personal data, which is aggregated according to certain social and economic criterions. The possibility of targeted advertisement and customer attention is auctioned against remuneration in money, thus financing the offer of digital content and digital services (DCS) at the platform's front end. Only if viewed naïvely can these offers be considered "for free" because users do not pay a monetary price. As personal data is provided as remuneration that understanding is erroneous. *Facebook's* statement that its services "remain free" amounts to misleading advertisement[6] as it supports such misinterpretation.

Due to the effects of economies of scope, economies of scale and direct/indirect network effects,[7] multi-sided intermediaries tend to rapidly increase their share in a particular market and subsequently expand into other markets. Economic analysis reveals that platform economies have a strong tendency towards highly concentrated markets. This poses the danger that only a few competitors will be left and barriers for new market entrants become prohibitively high.[8] Most anti-trust agencies fear that intermediaries with a dominant market position might reach a so-called 'tipping point', thus, posing the risk that one 'winner takes all'.[9]

---

[6] Art. 6 (1) Unfair Commercial Practices Directive (2005/29/EC). With a different opinion: District Court Berlin, MMR 2018, 328 (330).

[7] Nestor Duch-Brown, Bertin Martens and Frank Mueller-Langer, 'The economics of ownership, access and trade in digital data', JRC Digital Economy Working Paper 2017-01, 40 sseq., available at: https://ec.europa.eu/jrc/sites/jrcsh/files/jrc104756.pdf.

[8] Jean-Charles Rochet and Jean Tirole, ''Two-sided markets: A Progress Report', 35 RAND Journal of Economics (2006), 645 ssq.; Wolfgang Kerber, 'A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis', GRUR Int. 2016, 989; Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, 'Competition policy for the digital era, Report for the EU Commission' (2019), 19 ssq./54 ssq, available at: http://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.

[9] Executive summary of the Working Paper 'The Market Power of Platforms and Networks' by the German Bundeskartellamt, 2016, available at: https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Berichte/Think-

Although the economic prowess of GAFAM and BAT enables and incentivizes an abuse of their respective dominant position in some markets, it should, nevertheless, be acknowledged that GAFAM and BAT offer valuable products to individual consumers and society as a whole.[10] Some of the services are commonly considered to be essential infrastructure of modern society.[11] Thus, it is important to bear in mind that many data subjects would have to invest a significant portion of their monetary income in order to maintain the level of consumption of DCS currently enjoyed on the basis of granting access to personal data for targeted advertisement. Despite the great difficulty of attributing a price to personal data,[12] it could even be argued that – until now and thanks to regulation[13] – cautious data subjects receive good value for personal data.[14]

2. Legal Framework

Currently all branches of the legal profession struggle with the challenges posed by the platform economy in general and the role of personal data in particular.[15] The regulatory framework is

---

Tank-Bericht-Zusammenfassung.pdf?__blob=publicationFile&v=4; see also Joint Report of the Autorité de la concurrence and the Bundeskartellamt on 'Competition Law and Data', 10.5.2016, p. 26 sseq. available at: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2; applied at: Bundeskartellamt, Beschluss v. 6.2.2019, B6-22/16 – *Facebook*, para. 432 sseq.

[10] Presumably of different opinion: Vanessa Mak, 'Contract and Consumer Law', in Vanessa Mak, Eric Tjin Tai and Anna Berlee (eds.) *Research Handbook in Data Science and Law* (Edward Elgar 2018), 20 („After all, why should Google be allowed to make money on my data, while I receive nothing?").

[11] Such characterization as essential infrastructure usually relates to examinations of anti-competitive behavior and a potential abuse of dominant position. However, if overstated this might raise the question on a government's responsibility to safeguard the availability of such infrastructure. In short: Providing the infrastructure for traditional telecoms required public funding and state-owned companies that were only thereafter privatized. Contrastingly, the current infrastructure is increasingly provided by private companies – although based on partially publically funded networks – and are only thereafter regulated, similar to traditional telecoms. See for example Art. 7 (4) GDPR as expansion of Art. 102 TFEU and the specific § 95 (5) German TKG (telecom sector).

[12] The choices provided by media websites such as the Austrian "Standard" (€ 6/month) or the "Washington Post" ($ 90/year) provide for a near to market expectation of the value of an average website user.

[13] This will be different if personal data is processed for other means than personalized advertisement such as calculating individual premiums for health insurances.

[14] Companies paying for targeted advertisement on platforms are themselves subject to information asymmetries. Intermediaries might be able to trace the impact of marketing efforts more accurately. However, as long as these intermediaries use 'walled gardens' to shield their customers from direct marketing access, advertisers might still be paying prices for derivatives of aggregated data beyond real impact. The famous adage that "Half the money I spend on advertising is wasted; the trouble is I don't know which half", that is credited to John Wanamaker (1838-1922) might, although on a much lower level – still hold true in the age of the platform economy.

[15] The European Data Protection Board (EDPB) tends to turn a blind eye on the platform economy. Its "Guidelines 2/2019 on the processing of personal data under Article 6 (1)(b) GDPR in the context of the provision of online services to data subjects" (8.10.2019) discusses the (lack of) applicability of Art. 6 (1)(b) GDPR in specific situations. However, the business models of GAFAM and BAT are hardly mentioned (https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf).

complex and can be compared to a patchwork rug.[16] In addition to the GDPR and the DCSD – the topic of this article – exist multiple other European and national rules that have an impact on data-based business models. To mention but a few: The law of monopolies,[17] the directive on the protection of databases,[18] the directive on the protection of trade secrets,[19] the directive on unfair contract terms,[20] the directive on unfair commercial practices,[21] the directive concerning misleading and comparative advertising,[22] and the directive on privacy and electronic communications.[23] Almost all of these acts have recently been, are currently or will soon be under revision due to the challenges posed by digitalization. Additional legislation on consumer protection[24] and even on the protection of businesses[25] have been proposed and will impact data-based business models once passed as laws.

The protection of privacy has only recently gained momentum. Legal protection of information relating to an identified or identifiable natural person (personal data) has followed a calm and steady stream until May 2018 when the GDPR became applicable. While the reasons for new legal challenges are manifold, the single most important is a combination of money and

---

[16] Using this image in the context of laws protecting industrial data: Malte Grützmacher, 'Dateneigentum – Ein Flickenteppich', CR 2016, 485.

[17] Access to (personal) data leads to new economic theory and subsequently different legal approaches as regards merger control (Art. 101 TFEU) and the abuse of dominant market position (Art. 102 TFEU). For recent changes of the German Act against Restraints of Competition (Competition Act – GWB) to factor in data as counter-performance and the impact of intermediaries, see Art. 18 (2)(a) and (3)(a) GWB respectively (http://www.gesetze-im-internet.de/englisch_gwb/englisch_gwb.html#p0024). For an overview on the impact of digitization on the law against anti-competitive behavior: Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, 'Competition policy for the digital era', Report for the EU Commission, 2019.

[18] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27.3.1996, p. 20–28.

[19] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, OJ L 157, 15.6.2016, p. 1–18.

[20] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ L 95, 21.4.1993, p. 29–34.

[21] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market (Unfair Commercial Practices Directive), OJ L 149, 11.6.2005, p. 22–39.

[22] Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising, OJ L 376, 27.12.2006, p. 21–27.

[23] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002, p. 37–0047.

[24] Proposal for a directive on representative actions for the protection of the collective interests of consumers, and repealing Directive 2009/22/EC, COM (2018) 184 final – 2018/0089 (COD).

[25] Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:PE_56_2019_REV_1&from=EN.

enforcement. The option of fining a company with up to EUR 20 million. or 4 % of its global annual turnover has catapulted the GDPR onto the agenda of management boards worldwide.

However, the debate on data protection law seems to be dangerously biased. The discussions leading up to the GDPR were partially impacted due to an excessive focus on GAFAM. The requirements for valid consent (Art. 7), the right to erasure (Art. 17) and the right to data portability (Art. 20) can be perceived as effective instruments to restrict primarily US IT Companies. However, such regulation appears excessive when considering that it is equally applicable to small retail businesses or non-profit organizations. The approach of 'one size fits all' can be justified due to privacy rooting in fundamental rights.[26] However, Art. 7 (3) and (4) in particular might lack proportionality if interpreted strictly, as currently proposed by most data protection authorities and some courts.[27] Such interpretation follows a perspective that takes little account of the commercialization of personal data and it overemphasizes the fundamental right to the protection of personal data (Art. 8 ECHR, Art. 16 TFEU) at the risk of neglecting the freedoms to choose an occupation (Art. 15 ECHR), to conduct business (Art. 16 ECHR) and to conclude contracts.[28]

In contrast to the final wording of the DCSD, the EU Commission originally proposed a draft which brought personal data under the material scope of the DCSD, and also accepted that personal data can be commercialized. Consequently, it identified personal data as a type of counter-performance.[29] However, such an approach – which the former European Data Protection Supervisor polemically compared to trading organs of a living person[30] – was unacceptable for members of the EU Parliament. As a result, all references to the term "counter-performance"[31] were deleted. Contrastingly, the final wording includes the utopian proclamation that personal data is "no-commodity".[32] In order to achieve a level playing field for all providers of

---

[26] Ironically, it is very likely that GAFAM will be able to cope with the strict regulation. The real cost will be borne by start-ups and companies which have to comply with the same rules, although their business model is not focused on personal data. Put short: The GDPR will help GAFAM to strengthen their market position as it raises barriers of market entrance for competitors.

[27] Austrian OGH, Urt. v. 31.08.2018 – 6 Ob 140/18h = BeckRS 2018, 30960 = ZD 2019, 72, para. 47.

[28] On Art. 16 ECHR see CJEU, 21. 12. 2016 – C-201/15 = EuZW 2017, 229 (para. 66 f.); CJEU, 22. 1. 2013 – C-283/11 = EuZW 2013, 347 (para. 42 ff.) – *Sky Austria*.

[29] Art. 3 (1) of the proposal for a directive on certain aspects concerning contracts for the supply of digital content, Brussels, 9.12.2015, COM(2015) 634 final – 2015/0287(COD).

[30] Speech of Giovanni Buttarelli (EU-Data Protection Supervisor), available at: https://edps.europa.eu/sites/edp/files/publication/17-01-12_digital_content_directive_sd_en.pdf.

[31] Recitals 13, 14, 37, 42 of the Commission's proposal.

[32] Recital 24 DCSD. Repeating this mantra: Guidelines 2/2019 of the EDPB (FN 15), para. 54.

DCS, the directive remains applicable, irrespective of whether consumers provide remuneration in money or grant access to personal data.

Art. 16 (1) s.2 DCSD illustrates that both categories of remuneration cannot be treated equally. A right to reduction is only granted as a remedy to defective DCS if consumers have paid a monetary remuneration. If consumers grant access to personal data instead, they are entitled to terminate the contract even if the lack of conformity of DCS is minor under Art. 14 (6) DCSD. Thus, the absence of a right to reduction is partly compensated by a lower threshold as regards the termination right.[33]

As an attempt to avoid disputes, the DCSD stipulates that in any case of conflict the GDPR shall prevail, Art. 3 (8) and Art. 16 (2) DCSD. However, such superiority hardly provides solutions as the GDPR ignores the commercialization of personal data. Moreover, deleting the term "counter-performance" in the DCSD has no impact on the persistent tension between GDPR, DCSD and general contract law. While a contract is defined by its reliable and binding mutual nature (*quid pro quo – do ut des*), the GDPR provides no such reliability as Art. 7 (3) generally allows a data subject to withdraw consent at any time without cause. Put short: The European legislator has not provided a solution to the challenges stemming from an approval of personal data as remuneration (DCSD) and the right to withdraw consent (GDPR), yet.[34]

III. Bridging the Gap

Only a superficial observation might suggest that European law contains an unambiguous decision that personal data is no object of trade. The policy statement that personal data is "no commodity" is the result of political compromise. Nevertheless, reality proves such proclamations wrong. Public opinion and most data protection authorities neglect the fact that the GDPR has two regulatory purposes (1). Moreover, personal data has been an object of trade for decades. This reality is not sufficiently taken into account (2). The sheer amount of 87 verbose recitals illustrates that the few mandatory articles of the DCSD represent the lowest common denominator. The European legislator was unable to strike a balance between the protection of privacy and economic reality. Consequently, the DCSD delegates the task of synchronizing GDPR and DCSD to the judiciary (3).

---

[33] It is difficult to reduce the volume of personal data provided once the digital content or service is defective. However, this approach saves courts from the difficult task of determining the value of the personal data.

[34] Instead, an evasive recital 40 provides that the DCSD "should not regulate the consequences for the contracts covered by this Directive in the event that the consumer withdraws the consent for the processing of the consumer's personal data. Such consequences should remain a matter for national law" (see below IV.3).

1. Acknowledging the other side of the coin

According to its subject-matter and objectives, the GDPR lays down rules relating to the protection of natural persons with regard to the processing of personal data *and* rules relating to the free movement of personal data, Art. 1 (1) GDPR. Of course, there is not a single article within the GDPR that focuses on the free flow of data. Its regulatory emphasis is almost exclusively on the protection of privacy. Such disparity encourages an interpretation that represses the second rationale of enabling the free movement of personal data within the EU.[35] Obviously, any adjustment of diverse national laws reduces transaction costs and therefore removes market barriers. Thus, harmonization automatically facilitates the EU internal market. However, the objective of enabling a free flow of personal data should not be misunderstood as a mere factual consequence or by-product of the adjustments provided for by the GDPR, nor as paying mere lip service to the principle of conferred powers, Art. 114 (1) and Art. 115 TFEU.

The equal status assigned to the aim of removing obstacles to trade in the internal market and the right to the protection of personal data is an ambiguous starting point and has to be considered by both the courts and data protection authorities when applying the GDPR. This is particularly important when the European Data Protection Board (EDPB) provides interpretative guidelines and adopts a decision that is binding for national supervisory authorities, Art. 65 (1).[36] While such decisions by the EDPB are essential for supervisory authorities to achieve a homogeneous interpretation, courts should consider these guidelines very carefully. It is the task of the judiciary to scrutinize these guidelines and decisions, especially if the EDPB neglect the free flow of personal data as second objective of the GDPR.

2. Personal data as object of trade

The EU Commission's proposal of the DCSD (2015)[37] was – when compared to the wording of the final DCSD – straightforward. Recitals 13, 14, 37 and 42 of the proposal mentioned that personal data should be considered as "counter-performance". According to Art. 3 (1) of the proposal, the directive was applicable to any contract under which a provider of digital content received either a price or a "counter-performance other than money in the form of personal data

[35] See also rec. 5 GDPR.

[36] While such decisions by the EDPB are essential to achieve a homogeneous interpretation amongst supervisory authorities, courts should consider these guidelines carefully, but should not hesitate to reject their findings.

[37] Proposal for a directive on certain aspects concerning contracts for the supply of digital content, Brussels, 9.12.2015, COM(2015) 634 final – 2015/0287(COD).

or any other data".[38] The proposal initiated a discussion on how the *de facto* commercialization of personal data should be treated in the context of contract law. As already mentioned, all references to personal data as "counter-performance" were eventually deleted. Contrastingly, recital 24 DCSD proclaims that personal data is "no commodity". However, such wording is meaningless in the context of economic reality.

Firstly, there is an obvious tension stemming from the freedom of contract and the approach taken by the GDPR. Derived from its historical evolution as a legal defense against oppressive government,[39] privacy law is based on a prohibition of processing personal data unless consent or a formal legislative act allows otherwise, Art. 6 (1) and Art. 9 (1) GDPR. Conversely, contract law roots in the freedom of contract. Thus, voiding a contract is an exception.

Secondly, it is good law – at least in Germany – that a consent allowing the processing of personal data cannot always be withdrawn at any time without cause. German courts held that a consent to produce and publish nude photography against remuneration in money could not be withdrawn because the pictured person opted for a more "serious" lifestyle.[40] More recently, and in the context of labor law and therefore a legal field that is traditionally perceived as an area that safeguards employees, the German Federal Labor Court denied an employee the right to freely withdraw a given consent. The employee had consented to being filmed for a marketing video of his employer. This video was publicly available on the employer's website. A few months after termination of the labor contract, the former employee withdrew his consent and sued for an injunction, damages and erasure of the relevant video clip. Balancing the interests at stake, the court decided against such a right to withdraw consent, thus, decoupling the labor contract from the consent to a processing of personal data.[41] The video clip – including the image of the former employee – could remain on the website.

Despite the right to withdraw consent according to Art. 7 (3) and the right to erasure ("be forgotten") according to Art. 17, both judgements are arguably still good law after May 2018. They fall within the scope of the so-called opening clauses for national law stipulated in Art.

---

[38] Furthermore, the EU-Commission did foresee a post-contractual conflict if a consumer provided user generated content (UGC), including personal data (Doc: ST 14827 2016 INIT 1.12.2016, p. 11 (no. 29) available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil:ST_14827_2016_INIT). Upon termination of the contract, the provider had to stop the processing of all personal data. However, Art. 13 (2)(b) of the proposal provided an exception for such UGC and personal data, which the consumer had generated jointly with other customers, who continue to make use of such multi-relational data.

[39] Andreas Sattler, 'Personality to Property? – Revisiting the Fundamentals of the Protection of Personal Data' in Mor Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law* (Springer 2018), 27 ssq.

[40] District Court Munich, 17.3.1989 – 21 U 4729/88, NJW-RR 1990, 999.

[41] German Federal Labor Court (BAG), 11.12.2014 – 8 AZR 1010/13, ZD 2015, 330.

85 (freedom of expression and information) and Art. 88 (processing in the context of employment) respectively. However, both decisions illustrate that a strict and verbatim interpretation of Art. 6 and Art. 7 can easily lead to contradictory decisions under the GDPR and national law.

Let us presume that the GDPR was applicable to the aforementioned facts. In the first example, sensitive personal data is concerned and such a situation would therefore not be open to a balancing of interests by a court.[42] As regards the second example, processing would not be possible under the GDPR either if the interpretation of Art. 6 (1)(a) as proposed by the Art. 29 Working Group is correct. According to its Working Paper 259,[43] the Art. 29 Working Group proposes an interpretation of Art. 6 that would bar data controllers from relying on more than one legal basis when processing personal data for a specific purpose. Consequently, all data controllers would be prohibited from switching to a different legal basis once a data subject withdraws consent.[44] According to that understanding, a court would be prevented from applying Art. 6 (1)(f) GDPR (balancing of interests) once consent has been withdrawn.

This interpretation of the Art. 29 Working Group bluntly contradicts the wording of Art. 6 (1) which requires that *at least one* legal basis justifies the processing. Therefore according to the verbatim law, controllers are free to rely on several justifications for the same data processing.[45] The narrow interpretation of the Art. 29 Working Group would only be feasible if the respective legal justifications provided in Art. 6 (1) were sufficiently precise and easy to apply.[46] As none of these conditions are met, such restrictive interpretation is not convincing from a legal perspective and utterly unrealistic from an economic standpoint.[47]

---

[42] Processing of sensitive data for commercial purposes requires – in general – either a consent or a public interest, Art. 9 (2) GDPR.

[43] Article 29 Working Party, WP259 rev.01, Guidelines on consent under Regulation 2016/679, adopted on 28.11.2017, as last revised and adopted on 10.4.2018.

[44] Article 29 Working Party, WP259 rev.01, p. 22: "It is important to note here that if a controller chooses to rely on consent for any part of the processing, they must be prepared to respect that choice and stop that part of the processing if an individual withdraws consent. Sending out the message that data will be processed on the basis of consent, while actually some other lawful basis is relied on, would be fundamentally unfair to individuals".

[45] This understanding is confirmed by Art. 17 (1)(b) GDPR which stipulates that withdrawal of consent is not sufficient to constitute a right to erasure if such data processing can be based on another justification.

[46] The EDPB seems less strict on this issue. According to recital 20 of the Guidelines 2/2019 (FN 15) the controller can rely on different legal basis but "should make sure to avoid any confusion as to what the applicable legal basis is". Thus, instead of promoting exclusivity of the legal basis the EDPB seem to emphasize the principle of transparency.

[47] Despite the relevance of the guidelines of the former Art. 29 Working Group – which was succeeded by the European Data Protection Board –, courts and antitrust offices should, nevertheless, be cautious when referring to these guidelines, as the EDPB tends to take a perspective that focuses on the rights of data subjects and might therefore neglect other interests involved. Strongly relying on the Working Papers of the Art. 29 Working Group: Bundeskartellamt, Beschluss v. 6.2.2019, B6-22/16 – *Facebook* (a short summary is available in English: https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=4).

Thirdly, the GDPR largely blanks out celebrity merchandising that reaches beyond cheesy tabloid "stories" – to which Art. 85 GDPR arguably applies.[48] Popular actors, athletes and politicians have been licensing and thus commercializing their names, images and other aspects of their identity for decades. It remains open for debate how such licensing of economic parts of personality rights[49] will be treated under the GDPR. The answer is not trivial nor of only theoretical interest.[50]

3. Courts as bridge builders

The analysis of the GDPR and the DCSD reveals fundamental conflicts that were not solved by the legislator. According to Art. 3 (1) s.2 DCSD consumers are granted similar rights irrespective of whether they pay a monetary price or provide personal data instead. Consequently, the DCSD – at least partially – achieves its aim to create a level playing field for providers irrespective of the nature of remuneration. However, as personal data is not accepted as counter-performance, the DCSD lacks detailed remedies once the contract is terminated and given consent is withdrawn. In contrast, Art. 3 (8) stipulates that the DCSD shall be without prejudice to the GDPR. Similarly, Art. 16 (2) DCSD demands that providers of DCS shall comply with the obligations applicable under the GDPR as far as personal data of consumers are concerned.

Instead of providing detailed rules for obvious legal conflicts, the DCSD points to the GDPR, a regulation that deliberately turns a blind eye to the *de facto* commercialization of personal data. As if the relationship between GDPR and DCSD was not already complex, recital 40 DCSD leaves the contractual consequences of a withdrawal of consent entirely to the national laws of the Members States. The respective European institutions were well aware of the conflicts during trilogue proceedings. However, they could not strike a reasonable compromise. Consequently, the task of synchronizing has – like a hot potato – been passed on to the courts. Fundamental economic policy decisions were delegated to the realm of the CJEU.

---

[48] Rec. 153 para. 7 GDPR.

[49] In US American law such business models are facilitated by a broad right to publicity. See for a comparison: James Q.Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty' (2004) 113 Yale Law Journal 1151, available at: http://www.yalelawjournal.org/article/the-two-western-cultures-of-privacy-dignity-versus-liberty.

[50] An application of Art. 6 (1)(b) provides no convincing solution. See below IV.2.

IV. Alterative Options for Synchronization

Prior to proposing a two-tier interpretation of Art. 6 (1) it is sensible to briefly illustrate the alternative options and describe their disadvantages. One option could be to interpret the provision of personal data as a mere condition (1). The second option relies on a flexible interpretation of Art. 6 (1)(b) combined with a strict control of General Terms and Conditions (2). The third option relies on an extensive application of Art. 6 (1)(f) GDPR (3).

1. Personal data as condition

Ever since *Lawrence Lessig* coined the phrase "Code is Law"[51] it is accepted that software (code) can partially substitute enforceable legal duties. Even without entering into the specifics of current research on so-called smart contracts based on blockchain technologies, it is easy to imagine simple transactions that are performed by software and subject to technical requirements. Access to DCS can depend on the technical requirement that access to personal data is granted also. Leaving aside the actual complexity of modern contracts, it is possible to code a basic exchange of digital objects as technical conditions (if x then y). Such software-based transactions help to avoid some of the risks which were traditionally solved through contract law. Technology can reduce the need for mutual trust and thus substitute expensive precautions that would otherwise be necessary when dealing with strangers over long distances (i.e. insurance coverage, securitization, clearing agencies or a trustee as intermediary). Code is particularly effective in eliminating the risks triggered by duties of pre-performance.

It is convincingly argued that many of the products provided by GAFAM and BAT are based on numerous micro exchanges of bits and bytes. From a legal perspective, such micro transactions can be interpreted as performances based on mutual legal conditions. Technical code and legal conditions correspond.[52] Indeed, usage of search machines or social networks usually depend on an enabling of tracking tools either by accepting cookies or by logging on to an user account. In brief, code provides access to DCS and access to personal data concurrently.[53]

---

[51] Lawrence Lessig, *Code and other laws of cyberspace*, 1999.

[52] Philipp Hacker, 'Daten als Gegenleistung: Rechtsgeschäfte im Spannungsfeld von DS-GVO und allgemeinem Vertragsrecht', ZfPW 2019, 148 (172 ssq.).

[53] Art. 3 (1) of the Commission's proposal required the consumer to "actively provide" personal data. For criticism of such wording: EU Parliament, 27.11.2017, COM (2015)0634 – C8 – 0394/2015 – 2015/0287 (COD); Axel Metzger, Zohar Efroni, Lena Mischau and Jakob Metzger, 'Data- Related Aspects of the Digital Content Directive', 9 (2018) JIPITEC 90, para. 25-28; Axel Metzger, 'Verträge über digitale Inhalte und digitale Dienstleistungen: Neuer BGB-Vertragstypus oder punktuelle Reform?', JZ 2019, 577 (579).

The main advantage of an interpretation of such technical access to personal data as a legal condition is its conformity with the GDPR and the DCSD.[54] According to a mnemonic that every German undergraduate student is taught: A condition suspends, but is not enforceable (German: "Die Bedingung suspendiert, zwingt aber nicht").[55] Therefore, if granting access to personal data is a mere legal condition, such an interpretation is consistent with both the right to withdraw consent at any time according to Art. 7 (3) and the reluctance to denote personal data as counter-performance or commodity. As remarked by *Michael Grünberger*, the right to withdraw consent at any time and without cause facilitates competition as it provides a strong incentive for providers to offer "good value for data".[56]

However, such congruence of technical code and legal condition poses many legal challenges. This article will focus on two aspects, which indicate that the option of perceiving access to personal data as a legal condition is insufficient. *Firstly*, relying on micro transactions based on technical code and legal conditions will benefit a particular business model. If processing of personal data is merely based on a condition and not subject to contractual duties, this incentivizes an immediate and exhaustive exploitation of personal data. The right to withdraw consent is intended to provide data subjects with control and thus protect privacy. In practice, the option of access to personal data as a condition plays into the hands of GAFAM and BAT or more generally, dominant platforms.

The disadvantages of micro transactions based on coded conditions will be borne by those market entrants who cannot afford to treat their customers as "walled gardens" and who need to plan ahead when establishing their business model. Enterprises who take privacy seriously and seek to build a basis of mutual trust, might require a more reliable foundation for their business model, and therefore depend on a secured stream of personal data. Such stability is typically delivered by contractually binding temporal duties to perform.

While Art. 20 GDPR (right to data portability) is supposed to reduce lock-in effects and assist at switching providers, it also reinforces such unpredictability. Art. 20 enables data subjects to combine the right to withdraw consent and the right to migrate personal data to a new

---

[54] The European Parliament has mentioned such interpretation of access to personal data as condition. However, the concept was not elaborated on: Report of the European Parliament, 27.11.2017, p. 8, ("The report deletes the term 'counter-performance', criticized by the EDPS, and replaces it with the term 'condition' "), available at: http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/614707/EPRS_BRI%282018%29614707_EN.pdf). The term is repeated by the EDPB in its Guidelines 2/2019 (FN 15), no. 27 ("conditional").

[55] *Savigny*, System des heutigen Römischen Rechts III, 1840, § 128, p. 231; as cited by: Philipp Hacker, 'Daten als Gegenleistung: Rechtsgeschäfte im Spannungsfeld von DS-GVO und allgemeinem Vertragsrecht', ZfPW 2019, 148 (196).

[56] Discussion at a workshop on "rights in data", 22.2.2019, University of Bayreuth.

provider. As the preparation for and the actual performance of data portability causes costs for providers, all data controllers need to earn that money in advance. They are well advised to collect and exploit personal data prior to providing access to digital content or digital services. As withdrawal of consent has only relative effect, it encourages data controllers to obtain a consent that includes processing by third parties and thereafter immediately provide the personal data to such third parties. Once consent is withdrawn, data controllers are merely obliged to inform subsequent data controllers, if such notice does not cause disproportionate efforts. Whenever controller and data subject are of differing opinions on the interpretation of what amounts to "disproportionate efforts", it will be for the data subject to enforce the right to information – according to Art. 15 (c) and Art. 19 s.2 GDPR – against each subsequent controller and thereafter request the data to be erased. Rational apathy will deter data subjects from such a 'scavenger hunt' that follows the chain of data processing initiated by the original consent.

Secondly, in the words of *Martin Schmidt-Kessel,* such conditioned micro exchanges recall "the stone age of the law on obligations".[57] Although it is correct that the law on data contracts is still in its infancy, nevertheless, it is crucial to realize that such streams of independent and subsequent micro transactions tend to evade strict legal control. Businesses that rely on continued access to personal data for a certain period and are willing to provide a high level of privacy would not even be able to rely on consent for a short period due to the unstable and elusive nature of consent.

2. Option: Extensive application of Art. 6 (1)(b) GDPR

According to Art. 6 (1)(b) processing of personal data shall be lawful only if and to the extent that it is necessary for the performance of a contract to which the data subject is party. Art. 6 (1)(b) does not provide an implied consent.[58] In contrast, it stipulates a statutory basis for the processing of personal data that is accessory to a contract. Art. 6 (1)(b) can justify a process that uses a customer's postal address and contact details when delivering parcels ordered by a customer or to issue an invoice.[59] However, it is not for the parties to agree on a 'data license' which defines the processing of personal data or targeted advertising as the main contractual

[57] Discussion at a workshop on "rights in data", 22.2.2019, University of Bayreuth.

[58] However, in practice it can be very difficult to distinguish between data processing based on Art. 6 (2)(b) and on consent, in particular as Art. 6 (2)(a) does – in contrast to Art. 9 (2)(a) – not require an explicit consent.

[59] EDPB, Guidelines 2/2019 (FN 15), no 35.

performance. Consequently, Art. 6 (1)(b) is subject to a strict proportionality test[60] that is, therefore, inflexible and leaves little room for interpretative reasoning.

When comparing the wording of Art. 3 (1) s.2 DCSD and Art. 6 (1)(b) it becomes obvious that the DCSD is not applicable if personal data provided by the consumer is exclusively processed by the trader for the purpose of supplying DCS.[61] Therefore, it is unlikely that Art. 6 (1)(b) provides an option to synchronize the DCSD and the GDPR. However, the relationship between Art. 3 (1) s.2 DSCD and Art. 6 (1)(b) is less clear than the respective wording suggests. The interpretation of the term "necessary for the performance" is key to its application. As one would expect, data protection authorities suggest the most restrictive interpretation. According to the "Guidelines 2/2019 on the processing of personal data under Article 6 (1)(b) GDPR",[62] published by the EDPB, Art. 6 (1)(b) is not available for negotiation. Instead, it only allows auxiliary or supportive processing if required for the performance of a different contractual purpose.

Of course, it is the core contractual purpose of a social network to allow a customer to connect and communicate with other customers of the network. In other words, there can be no doubt that the processing of huge volumes of personal data is "necessary for the performance" of a contract aimed at connection based on names, pictures, geographical locations and interests. Nevertheless, the EDPB has made clear – or rather unclear – that Art. 6 (1)(b) should not be applicable if a business model relies on targeted advertising for funding. It argues that "personal data cannot be considered as a tradeable commodity. Even if data subjects can agree to processing of personal data, they cannot trade away their fundamental rights through this agreement".[63]

People with a background in law could interpret such language as a proposal to interpret the wording of Art. 6 (1)(b) in the light of Art. 8 ECHR/Art. 16 TFEU and thus reduce its scope, specifically to exclude contracts for the use of networks such as *Facebook* or *LinkedIn* which are seemingly "for free", simply because they are paid for by advertisers on the back end of the platform. However, the EDPB's assessment remains vague, as it also admits "that personalization of content may (but does not always) constitute an intrinsic or expected element of certain

---

[60] EDPB, Guidelines 2/2019, (FN 15), no 25.

[61] Furthermore, the DCSD is not applicable if the processing can be based on Art. 6 (1)(c) GDPR (Art. 3 (1) s.2 DCSD: "for allowing the trader to comply with legal requirements to which the trader is subject"). Presumably the DCSD is not applicable if the processing can be based on Art. 6 (1)(d) GDPR (necessary to protect the vital interests of a natural person) as it has no link to contract law.

[62] EDPB, 2/2019 (FN 15), para. 54.

[63] EDPB, 2/2019 (FN. 15), para. 51 as regards "Processing for online behavioural advertising".

online services, and therefore may be regarded as necessary for the performance of the contract with the service user in some cases".[64] That reasoning could, of course, also be applied to social networks as average users expect that their messages, 'likes' and timelines on these platforms are to be received by accepted 'friends' and 'connections' rather than a random bunch of strangers.

In summary, while it is very likely and reasonable that the DCSD will not apply in case the processing of personal data is based on Art. 6 (1)(b) GDPR, it is less clear how the latter will be applied as the number of business models that rely on some form of personalization soar.

3. Option: Extensive Application of Art. 6 (1)(f) GDPR

According to Art. 6 (1)(f) processing of personal data shall be lawful only if and to the extent that it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

As mentioned above, several institutions have proposed very restrictive interpretations of the legal preconditions required for valid consent or processing based on a contract. If these interpretations of Art. 6 (1) (a) and (b) were correct and thus upheld by the CJEU, consequently most current business models, which are based on the processing of personal data, would have to rely on Art. 6 (1)(f). General clauses are well known as flexible tools, not only in administrative law but in private law too. They work as an overpressure relief valve, to be applied when detailed legal rules are overstrained by technical, economic or social development. However, they function only for safety and as a mechanism of last resort. When applied too often, the case law becomes vague and poses a danger to legal certainty. Consequently, while offering a technology neutral and flexible basis for the processing of personal data, Art. 6 (1)(f) places the burden of striking the right balance on data controllers (*ex ante*). Multiple data protection authorities and hundreds of national administrative and civil courts will decide *ex-post* whether these attempts of synchronization meet their respective interpretation of European and national laws. The person who is least involved in that entire process is the data subject itself.

Art. 6 (1)(f) does not require the conclusion of a contract and it would suffice to inform data subjects of their right to object to the processing (Art. 21 GDPR) in a controller's 'Privacy Policy'. Viewed from the perspective of empowering individual autonomy, the right to object

[64] EDPB, 2/2019 (FN. 15), para. 57 as regards "Processing for personalisation of content".

provides a weak tool. Eventually, it will be for data protection authorities and courts to balance all interests involved and thus arrive at a decision whether a business model is legal or illegal. This task requires assertive judges, who presume that they know the preferences of data subjects best. In short, individual autonomy is replaced by balancing of interest performed by businesses and courts, thus facilitating heteronomy.[65]

V. Proposal for a two-tier interpretation of Art. 6 GDPR

The most promising option is both extremely unpopular and – perhaps surprisingly – very old. It is based on three prerequisites:

First, those working in the legal professions must focus on what they do best: Differentiation. Currently, the GDPR follows the model of 'one size fits all', an approach that has a tendency towards hubris. At least according to data protection authorities and the German Federal Competition Agency, the GDPR compromises notions of anti-trust law below the traditional threshold of anti-trust law[66] and adopts instruments traditionally perceived as consumer protection law, while it also applies to entrepreneurs. Furthermore, the GDPR has been constructed to provide a leverage in international trade conflicts with a clear focus on regulating US corporations, in particular the platforms of GAFAM and (in the future) BAT. Ever since its applicability after May 2018, and driven by major 'data scandals', public opinion and some politicians have started to misinterpret data protection law as a tool to avoid so-called 'echo chambers' and the manipulation and radicalization of opinions, especially prior to general elections. In short: Being overambitious itself, the functions assigned to the GDPR are in a danger of overblowing it completely. It is time to re-focus on the objectives stipulated in Art. 1 GDPR.

Secondly, personal data – like personality rights – are special in that they contain an unalienable linkage to a human being. Due to that linkage to human dignity, personal data will not develop into a new type of immaterial property right.[67] However, despite that linkage personal

---

[65] It is very likely that most decisions on Art. 6 (1)(f) will be based on complaints logged by not-for-profit bodies, organizations or associations according Art. 80 (2) GDPR.

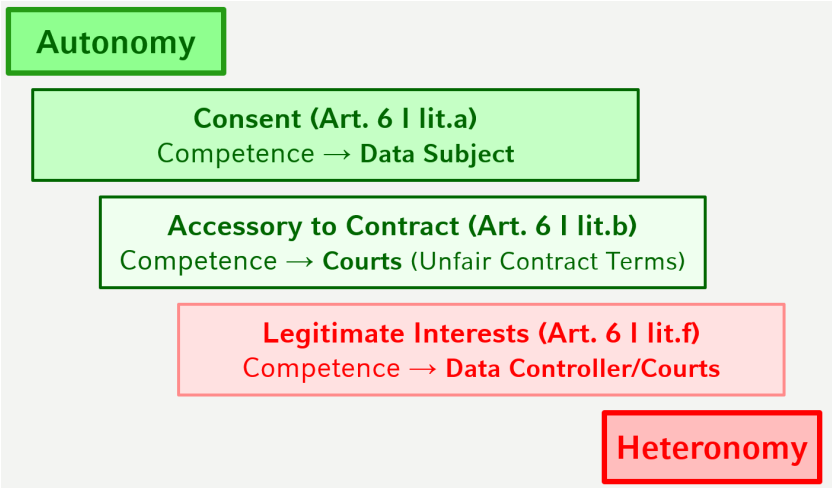
[66] According to such understanding Art. 7 (4) GDPR lowers the requirements otherwise stipulated by Art. 102 TFEU (abuse of a dominant market position), see Bundeskartellamt (German Federal Competition Agency), Beschl. 6.2.2019 (B6–22/16) para. 621 ssq. and para. 646. Against such interpretation and rejecting the decision of the Bundeskartellamt: OLG Düsseldorf, 1. Kartellsenat, Beschl. 26.8.2019 − VI-Kart 1/19 (V), BeckRS 2019, 18837 para. 67 – Facebook I („[…] es handelt sich um eine rein datenschutzrechtliche, nicht um eine kartellrechtliche Bestimmung" [engl.: Art. 7 (4) is about data protection law and not about competiton law].

[67] On such discussion: Herbert Zech, 'A legal framework for a data economy in the European Digital Single Market: Rights to use data', Journal of Intellectual Property Law & Practice, 2016, Vol. 11, No. 6, 460 (463); for the US: Shyamkrishna Balganesh, 'Quasi-Property: Like, But Not Quite Property', (2012) 160 University of Pennsylvania Law Review 1889; Pamela Samuelson, 'Privacy as Intellectual Property', (1999) 52 Stan. L. Rev. 1125.

data can be commercialized and is thus a *de facto* commodity comparable to the economic parts of traditional personality rights.[68] Consequently, personal data can be traded, but not transferred.[69] Rather than denying it altogether, legislators should start to manage such commercialization actively.

Thirdly, any interpretation of the GDPR should focus on strengthening autonomy rather than heteronomy. Despite the difficulties of tagging sets or even streams of personal data with a price, it is nevertheless fundamental to allow data subjects the ability to choose. Although consent is imperfect and compromised due to information asymmetries, biases, negative externalities and other market failures, it remains the best option to account for individual preferences, and thus incentivize data-based innovations valued by data subjects. Of course, there is a crucial need for icons according to Art. 12 (7), (8). If these are not delivered soon, European Parliament or Council needs to take back control according to Art. 92 (3). As regards enforcement these icons – if developed rigorously – can complement the potentially high financial penalties.

As has been illustrated above, data as a condition and an extensive application of Art. 6 (1)(b) and (f) would be detrimental to the target of strengthening autonomy. Therefore, the following figure classifies the available options according to the opposition of autonomy and heteronomy:



[68] Huw Beverley-Smith, Ansgar Ohly and Agnes Lucas-Schloetter, *Privacy, Property and Personality* (Cambridge University Press 2005), 94 ssq.; Franz Hofmann, 'The Economic Part of the Right to Personality as an Intellectual Property Law? – A Comparison between English and German Law' (2010) 2 Zeitschrift für Geistiges Eigentum/Intellectual Property Journal, 1 ssq.

[69] Andreas Sattler, 'Personality to Property? – Revisiting the Fundamentals of the Protection of Personal Data', in Mor Bakhoum et al. *Personal Data in Competition, Consumer Protection and Intellectual Property Law – Towards a Holistic Approach?* (Springer 2018), 27 (39 ssq.).

The case of celebrity merchandising illustrates the need to strengthen autonomy. It is obvious that such merchandising should be based on a celebrity's consent according to Art. 6 (1)(a). However, as the GDPR applies irrespective of whether a data subject is a consumer or an entrepreneur, such celebrity merchandising would be subject to Art. 7 (3) too. However, if Art. 7 (3) is mandatory law irrespective of the status of the data subject, the fate of these contacts would be subject to the right to withdraw consent at any time, and without cause as well. In short, if Art. 7 (3) is interpreted as strictly as most legal scholars and data protection authorities propose, this would jeopardize the long-established contractual basis of celebrity merchandising. Thus, it is suggested that the legal requirement for valid consent is interpreted in a more flexible manner. The fundamental right to protection of personal data could be guaranteed while striking a proportionate balance with other fundamental freedoms granted to individuals and businesses.

Such an interpretation can be based on an assessment that the definition of consent in Art. 4 no.11 only provides the minimum standard under European law. This interpretation has a crucial impact: Art. 4 no.11 would continue to exclude silence of a data subject or a pre-ticked box as a declaration of will and consent.[70] If Art. 4 no.11 provides only the minimum standard required according to Art. 8 ECHR, it does not preclude national contract laws from accepting forms of consent that reach beyond such a minimum standard. As a consequence of such interpretation, Art. 7 (3) should be construed as to refer only to such a minimum standard of consent. In applying legal doctrine, the (too) far reaching wording of Art. 7 (3) should be reduced to situations in which consent reaches only the minimum threshold as required by Art. 4 no.11. Above this minimum standard and following such a teleological reduction of its wording, Art. 7 (3) would have dispositive character and is thus subject to agreement.[71] Such interpretation would generally extend the options of consent, allowing for a tiered approach.

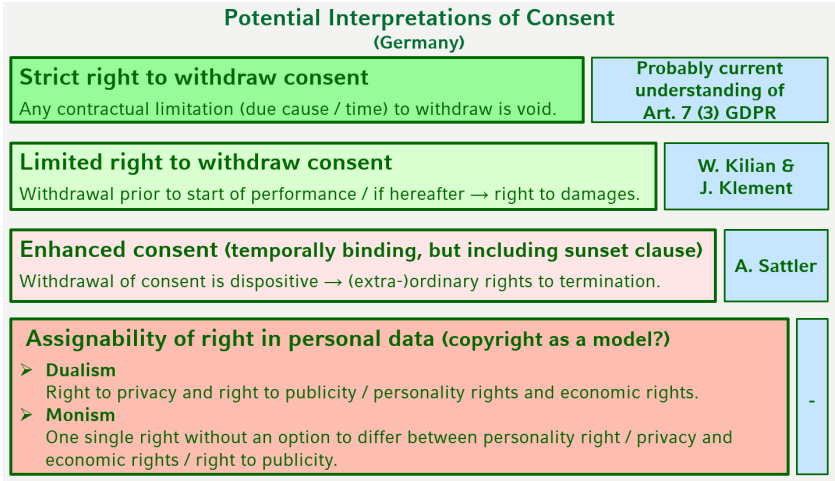
Consequently, the term 'consent' could be developed into a much more sophisticated European concept than currently envisioned. The subsequent figure – which is based on German law[72] – resembles the emancipatory route that the term 'consent' might travel as societies progress:

---

[70] Recital 32 s.3 GDPR.

[71] For details on the doctrinal methodology and its consistency with EU-Law: Andreas Sattler, 'Personenbezogene Daten als Leistungsgegenstand', JZ 2017, 1036 (1041 ssq.).

[72] On the German concept of consent: Ansgar Ohly, *Volenti non fit iniuria - die Einwilligung im Privatrecht* (Mohr Siebeck 2002).



While the wording of Art. 7 (3) seems to support only the first level of a strict right to withdraw consent, some authors have suggested that in cases that amount to an abuse of such right, data subjects might be obliged to compensate data controllers.[73]

Bearing in mind that contract law and consumer law provide many instruments to protect data subjects who are consumers, a third level of consent should be considered. As has been shown, it is likely that the wording of Art. 7 (3) reaches too far and should not apply in cases of celebrity merchandising. While celebrities tend to have legal advisors and might therefore be entrepreneurial data subjects, the same reasoning applies if ordinary data subjects provide personal data for commercial advertising and become "the face to a product". Although all these cases are within the scope of the GDPR, it is very unlikely that Art. 7 (3) will be applicable, if celebrities, models and freelancers provide personal data for money.

There might be reasons why the deliberate commercialization of personal data for money is not comparable to data subjects providing personal data for access to DCS.[74] However, it is worthwhile considering whether the right to withdraw consent could be suspended for a short and pre-fixed period of time (for example as sunset clause of two months[75]), thus allowing more stable relationships between data subjects and data controllers. Of course, there should be no

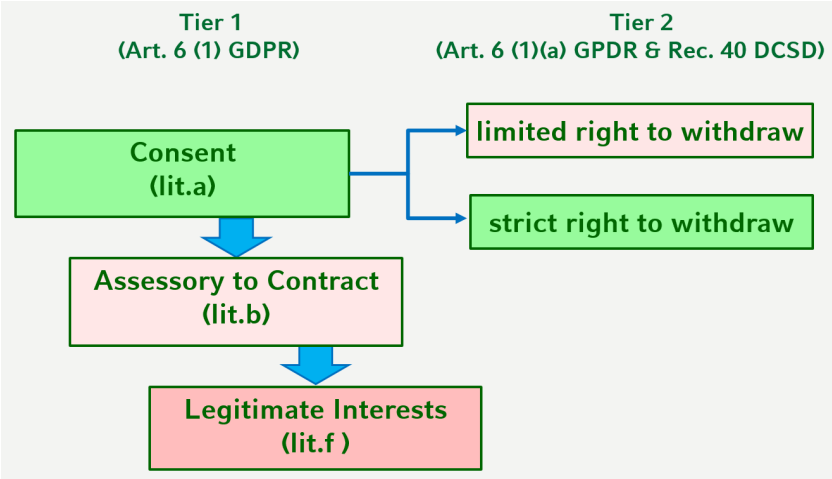
---

[73] Wolfgang Kilian, in *Gedächtnisschrift für Steinmüller*, 2014, 195 (212); Wolfgang Kilian, 'Personal Data: The impact of Emerging Trends in the Information Society. How the marketability of personal data should affect the concept of data protection law', (2002) 28 Computer und Recht International 169 ssq.; Jan Henrik Klement, in Spiros Simitis, Gerrit Hornung and Indra Spiecker, *Datenschutzrecht* (Nomos 2019), Art. 7 para. 92; Carmen Langhanke and Martin Schmidt-Kessel, 'Consumer Data as Consideration' EuCML 2015, 218 (221: "justified breach").

[74] When exchanging data for data it is particularly difficult to determine a value and fairness of a transaction.

[75] In contrast to the original consent that is – in general – not limited in time (German Federal Supreme Court, 1.2.2018, ZR III 196/17 para. 31), such deviation from the right to withdraw consent should be for a limited period, thus, requiring active renewal.

automatic extension of consent,[76] such General Terms and Conditions would be subject to transparency and fairness control and would not preclude any cause for an (extra)ordinary termination right of both contract and consent. Despite the proposed option to suspend the right to withdraw consent according to Art. 7(3) for a certain period, the link between a human being and personal data remains unassailable and can itself provide a cause for extraordinary termination. Merged into a two-tiered model this leads to the following options of processing personal data under private law.



Obviously, such an interpretation of the GDPR requires further research and a more synchronized approach towards contract law, consumer protection law and data protection law.[77] If this article can stimulate such research on a European concept of 'consent', it has achieved all the author could hope.

VI. Conclusions

Instead of a summary, this article will conclude with ten theses. As it is the ultimate expectation that all theses to be falsified, it is hoped that each thesis will give cause for criticism.

1. Personal data is a commodity: Famous actors and athletes have been exploiting the economic parts of their personality rights for many decades. Ordinary data subjects provide access to personal data and receive access to DCS in reverse. Thus, personal data has

[76] Thus, it would require a stricter rule than provided by no.1 lit.h of the Annex ("Terms referred to in Article 3 (3)") to Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ L 95, 21.4.1993, p. 29–34.

[77] For an overview see the conference volume: Mor Bakhoum, Beatriz Conde Gallego, Mark-Oliver Mackenrodt and Gintare Surblyte-Namaviciene (eds.) *Personal Data in Competition, Consumer Protection and Intellectual Property Law – Towards a Holistic Approach*? (Springer 2018).

been and will be commercialized despite the utopian proclamation in recital 24 DCSD ("no-commodity").

2. Personal data is tradeable, but not transferable: In contrast to many other commodities, personal data cannot be transferred. Personal data is defined by an unassailable link to a data subject. This link is guaranteed by Art. 8 ECHR and it justifies (extra)ordinary rights to terminate a contract. However, it does not preclude data subjects and controllers from concluding contracts to process and thus economically exploit personal data.
3. The processing of personal data is an ideological battlefield: The European legislator was unable to provide legal solutions to a fundamental conflict. While the Commission's proposal accepted personal data as counter-performance and corresponded with economic reality, Parliament and the European Data Protection Supervisor rejected such concept. The legislator was unable to reconcile the fundamental right to the protection of personal data with other fundamental rights such as freedom to choose an occupation (Art. 15 ECHR), freedom to conduct business (Art. 16 ECHR) and freedom to conclude contracts.
4. The EU legislator opted for evasion through delegation: In order to reach political compromise, the DCSD is based on the lowest common denominator. The national laws that implement the DCSD will be applicable if a consumer provides access to personal data in order to obtain access to DCS. However, as regards the conflicts that follow from Art. 3 (1) s.2 DCSD, the legislator points towards the GDPR (Art. 3 (8) and Art. 16 (2) DCSD) and national contract law (Recital 40 DCSD). Legal conflicts that are both essential and obvious are thus delegated to the courts of Member States and the CJEU.
5. Synchronization of the DCSD and the GDPR based on the interpretation that access to personal data is a mere condition corresponds with the right to withdraw consent according to Art. 7 (3) GDPR. However, such understanding leads to streams of micro transactions that benefit the current business models of already dominant platforms. If binding contractual relationships are precluded, many innovative business models will not occur.
6. Synchronization based on an extensive interpretation of Art. 6 (1)(b) GDPR (accessory to a contract) seems to be excluded by the wording of Art. 3 (1) S.2 and recitals 24 and 25 DCSD. However, when considering the drafted guidelines of the EDPB on the interpretation of Art. 6 (1)(b) GDPR – and recital 26 DCSD – this is less clear.
7. Synchronization based on an extensive interpretation of Art. 6 (1)(f) GDPR (balancing of interests) is an option. As such, balancing of interests will be performed by the data controller (*ex ante*) and national data protection authorities and courts (*ex post*). Such a general clause is a flexible tool and works as a safety net. Despite the right to object contained

in Art. 21 GDPR, Art. 6 (1)(f), nevertheless, facilitates heteronomy. It will be judges who decide what is best for controllers, data subjects and other natural persons involved.

8. When arranged on a staircase that starts at autonomy and ascends to heteronomy, Art. 6 (1)(f) is at the lowest level. Further up and at the second level follows Art. 6(1)(b). Consent is placed on the top level. Art. 6 (1)(a) can be interpreted to contain different levels of consent. As no European concept of 'consent' exists, it is worthwhile considering the different levels of consent accepted according to national laws of the Member States.

9. Viewed from a German perspective, Art. 4 no.11 can be interpreted to contain the minimum standard of consent as required according to Art. 8 ECHR. However, the definition does not preclude agreement on a type of 'consent' that reaches beyond this European minimum standard.

10. Art. 7 (3) can be interpreted to be only applicable to such minimum standard of consent as defined by Art. 4 no.11 GDPR. Such a teleological reduction of the (too) extensive wording of Art. 7 (3) is supported by the fact that personal data has been the object of contracts for decades. A right to withdraw consent at any time and without cause would jeopardize the long-established licensing practice in the area of celebrity merchandising. Consequently, Art. 7 (3) is dispositive. Data subjects and data controllers can generally contract out. However, European law will have to provide a strict framework – including a sunset clause – for such deviation from Art. 7 (3) if data subjects are consumers.