# Part IV Solutions to settle the inconsistencies

## *1. Direct application of the KUG in merchandising cases based on Art. 85 (1) GDPR*

### 1.1 Art. 85 (1) GDPR as a stand-alone opening clause

An extensive reading of journalistic purposes in Art. 85 (2) GDPR cannot support a direct application of the KUG in merchandising defined in this dissertation (see Part II Section 2.3.2). Accordingly, some scholars postulate that Art. 85 (1) GDPR being a stand-alone opening clause would solve the awkward situation of the KUG after the GDPR came into effect.[602]

Art. 85 (1) GDPR reads, "*Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression*".

At first glance, this paragraph appears to be an independent opening clause from Art. 85 (2) GDPR since Art. 85 (1), by its wording, also allows ("*shall*") the Member States to reconcile the GDPR with freedom of speech by law. In this sense, the Member States' discretion is no longer limited to processing data for journalistic purposes, etc., exclusively enumerated in Art. 85 (2) because Art. 85 (1) GDPR uses the term "including" instead of exclusively. In this wise, if the German legal regime for merchandising meets the two requirements, namely the need for the freedom of speech and in the form of law,[603] Germany can advocate the application of the

602 *Lauber-Rönsberg and Hartlaub,* NJW, 2017, 1057 (1062); *Ziebarth and Elsaß,* ZUM, 2018, 578 (583f.); *Golz and Gössling,* IPRB, 2018, 68 (72); *Nettesheim*, AfP, 2019, 473 (479); *Lauber-Rönsberg,* AfP, 2019, 373 (377); *Krüger and Wiencke*, MMR, 2019, 76 (78); Frey, in *Schwartmann, et al.*, DS-GVO/BDSG, Art. 85 Rn. 33; von Strobl-Albeg, in *Wenzel, et al.*, Das Recht der Wort- und Bildberichterstattung, § 7 Rn. 124; Lauber-Rönsberg, in *Götting/Schertz/Seitz*, Handbuch Persönlichkeitsrecht, § 22 Rn. 45; *Bienemann*, Reformbedarf des Kunsturhebergesetzes im digitalen Zeitalter, S. 43f. with further references in the footnote 95.

603 Leaves the questions of whether the jurisprudence of the KUG can be regarded as law from the EU perspective, and whether merchandising falls under the scope of the freedom of speech aside.

KUG as a principle on the one hand, and not relinquish protection provided by the GDPR in certain aspects on the other.

According to *Bienemann*, who explores this issue in her dissertation and reaches the conclusion that Art. 85 (1) GDPR is an independent opening clause with a sweeping (*pauschal*) effect, the overall assessment of four methods of interpretation – wording, systematics, history, and telos – of Art. 85 (1) GDPR speaks for an "optional general opening clause" (*fakultative allgemeine Öffnungsklausel*):[604] The most powerful argumentation for the wider reading of Art. 85 (1) GDPR is that the word "including" suggests that its applicable scope is wider than the processing for "journalistic purposes and the purposes of academic, artistic or literary expression";[605] According to the systematic interpretation, Art. 85 (1) GDPR would be redundant if it is not an "optional general opening clause". *Lauber-Rönsberg* and *Hartlaub*, who also support this idea, have forwarded another pragmatical argument: The legal fragmentation as a result of the opposing interpretation would ultimately lead to serious legal uncertainty and delimitation problems.[606] Moreover, unlike the GDPR, the KUG rests on abundant case law developed for more than a century to reconcile personality rights including the right to privacy and the right to freedom of expression and information. The cost of abandoning this precious heritage would take years or even decades to make up for.[607]

In addition, the German Federal Parliament (*Bundestag*) and the Federal Ministry of the Interior (*BMI*) also supported this solution by stating that the KUG continues to apply after the GDPR came into force based on Art. 85 (1) GDPR despite the lack of argumentation.[608] Noteworthy, as

---

604 *Bienemann,* Reformbedarf des Kunsturhebergesetzes im digitalen Zeitalter, S. 43f.; Similar argumentation see *Ziebarth and Elsaß,* ZUM, 2018, 578 (583f.); Vgl. *Krüger and Wiencke,* MMR, 2019, 76 (79).

605 *Bienemann,* Reformbedarf des Kunsturhebergesetzes im digitalen Zeitalter, S. 49; *Krüger and Wiencke,* MMR, 2019, 76 (78); Frey, in *Schwartmann, et al.*, DS-GVO/BDSG, Art. 85 Rn. 2.

606 *Lauber-Rönsberg and Hartlaub,* NJW, 2017, 1057 (1062).

607 Ibid. It has been argued that "it would probably take several years or even decades until a consolidated case law of the ECJ on specific cases would have developed."

608 The German Federal Parliament (*Bundestag*) and the Federal Ministry of the Interior (*BMI*) have stated that the KUG continues to apply after the GDPR came into force based on Art. 85 (1) GDPR without thorough argumentationBT-Drs. 19/4421, Antwort des Parlamentarischen Staatssekretärs Dr. Günter Krings vom 20. September 2018, S. 47 f.; FAQs zur Datenschutz-Grundverordnung, "Unter welchen Voraussetzungen ist das Anfertigen und Verbreiten personenbezogen-

mentioned in Part II Section 3.1.2, some German courts also implicitly share this view.

Pragmatically, this proposal is appealing as the self-contained regulation of merchandising based on the established jurisprudence of the KUG would remain unchanged, and the problems identified above would disappear. The under-protection issue for lacking material damages for celebrities in unauthorized merchandising cases can be resolved. Moreover, data subjects affected by unauthorized merchandising can still invoke the non-monetary remedies that they are familiar with such as injunctive relief, the auxiliary claims for information and accounting, etc. As noted above, they have more benefits for the data subjects in unauthorized merchandising scenarios compared to the scenarios concerning data subject's rights. Besides, the soft-licensing model adopted in merchandising agreements would remain according to the KUG and its jurisprudence. Merchandising contracts are binding, while the assignment of the right to one's image is prohibited. Moreover, the construction of the ambit of authorization in case of doubt is still limited to what is necessary for relation to the purposes of that contract. The data subject's rights are not available in the German legal regime. While omissions of granting such rights would lead to a notable under-protection issue, the rights are either inapplicable or ill-suited for merchandising cases because they are primarily designed to combat the risks posed by untransparent data processing or the lock-in effect aroused by platforms, such as the right to portability, and the right to not be subject to automated decisions.[609] After all, as argued above, Art. 85 (1) GDPR provides the Member States with flexibility in reconciliation within its law with the GDPR: German courts can freely decide to what extent they should deploy the rules in the GDPR to strike a fair balance between the protection of personal data and the freedom of speech in respect of merchandising.

It is important to note that the German legal regime by recognizing the commercial value of personal images and assigning this value to the person depicted offers more thorough protection for data subjects against unau-

---

er Fotografien künftig zulässig?" (Under what conditions is the taking and dissemination of personal photographs permissible in the future?), The Federal Ministry of the Interior, at https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2018/04/faqs-datenschutz-grundverordnung.html.

609 WP29, Guidelines on the right to "data portability", wp242 rev.01, 3; See Hert, Papakonstantinou, Malgieri, Beslay and Sanchez, 34 Computer Law & Security Review 193 (2018) (194-196); EDPS, Meeting the challenges of big data, Opinion 7/2015, 7-8, and 11.

thorized merchandising. Take the *hair salon* case as an example. In this typical case of users' merchandising, the economic interests attached to the processing of personal data are the main motive driving the controller to conduct users' merchandising. If, the data subject in this scenario feels no more humiliated like the girl called "*flour of the family*" did more than a century ago,[610] but only commercially exploited like Mr. Zeppelin felt and thus would like to claim reasonable material damages from the social platform,[611] the GDPR is restrained. On the contrary, the German legal regime can offer different compensation catering to the depicted person's needs.

### 1.2 Counterarguments for the independent nature of Art. 85 (1) GDPR

Many scholars argue that Art. 85 (1) GDPR is a mere *Anpassungsauftrag* (an instruction to adjustments) that specifies the purpose and means of the derogations or exemptions by the Member States.[612] Thus, the direct application of the KUG in merchandising cannot base on Art. 85 (1) GDPR after the GDPR became effective.

Except for the wording of Art. 85 (1) GDPR, the argumentation based on the historical, systematic, and teleological interpretation can also be used to support the opposite conclusion that Art. 85 (1) should not be a stand-alone opening clause. From an intra-systematic view, if Art. 85 (1) GDPR is an independent opening clause, the conditions, and limitations in Art. 85 (2) would be meaningless; Moreover, Art. 85 (3) GDPR only addresses "paragraph 2" as the legal basis for derogations or exemptions from the GDPR, and the omission in Art. 85 (3) of mentioning the first paragraph should not be qualified as a "legislative error"(*fehlerhaft*)[613] as the scholars suggest.[614] From an inter-systematic view, the overstretching

610 Roberson v. Rochester Folding Box Co. 171 N.Y. 538, 64 N.E. 442 (N.Y. 1902)
611 Cf. Fraley v. Facebook, Inc. 830 F. Supp. 2d 785, 808 (N.D. Cal. 2011)
612 *Dregelies*, AfP, 2019, 298; Pauly, in *Paal and Pauly,* DS-GVO BDSG, Art. 85 Rn. 4; *Benedikt and Kranig,* ZD, 2019, 4 (5); *Kahl and Piltz*, K&R, 2018, 289 (292); *Klein*, Personenbilder im Spannungsfeld von Datenschutzgrundverordnung und Kunsturhebergesetz, S. 201ff.; *Assmus and Winzer*, ZD, 2018, 508(512); Buchner/Tinnefeld, in *Kühling/Buchner,* DSGVO/BDSG, Art. 85 Rn. 12; *Benecke and Wagner*, DVBl, 2016, 600 (602f.); *Raji,* ZD, 2019, 61 (64).
613 *Bienemann,* Reformbedarf des Kunsturhebergesetzes im digitalen Zeitalter, S. 63.
614 Vgl. *Dregelies,* AfP, 2019, 298 (303).

of Art. 85 (1) GDPR would sabotage the fine-tuned Art. 6 GDPR.[615] The teleological interpretation is even more so because the dual objectives of the GDPR, especially the free flow of personal data within the EU cannot be achieved if the authority of the Member States is so extensive in reconciling the GDPR and the freedom of speech. The same problem arises for having multiple meanings in the arguments based on historical interpretation. In the Communication from the Commission to the European Parliament and the Council, Art. 85 (1) GDPR is rather an instruction specifying the purpose and means of derogations or exemptions instead of a mandate itself.[616]

Against its pragmatic advantages, some scholars contend that regarding Art. 85 (1) GDPR as a stand-alone opening clause is, in essence, an appeal of "it cannot be what it is not allowed to be" (*es kann nicht sein, was nicht sein darf*).[617] In addition, the limited applicable scope of the KUG would undermine the advantages.[618] Since the KUG does not entail regulations against unauthorized production and storage of photographs, these activities would be governed by the GDPR if they are not operated wholly manually.[619] Thus, a complete exploitation process of personal photos (data) would be artificially divided into many parts and subject to completely dif-

615 Vgl. *Kühling, et al.*, Die DSGVO und das nationale Recht, 2016, S. 287.

616 The EU Commission, Communication from the Commission to the European Parliament and the Council, Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018, 8. It states, "in accordance with the Regulation, Member States have to take the necessary steps to adapt their legislation by repealing and amending existing laws, … and laying down the rules for the reconciliation of freedom of expression and data protection" according to Art. 85 (1) GDPR.

617 *Krüger and Wiencke*, MMR, 2019, 76 (79).

618 *Klein*, Personenbilder im Spannungsfeld von Datenschutzgrundverordnung und Kunsturhebergesetz, S. 180 ff.; *Benedikt and Kranig*, ZD, 2019, 4 (5); *Kahl and Piltz*, K&R, 2018, 289 (292); *Assmus and Winzer*, ZD, 2018, 508 (512). The opposite opinion that the KUG is compliant with GDPR and can continue to apply since the KUG is a stricter law. See *Remmertz*, MMR, 2018, 507 (509). This opinion is not followed here because neither the logic of its arguments nor the arguments are tenable. Moreover, even the adherent to the idea that the KUG still applies after the GDPR came into effect advocates a profound reform for the KUG to delineate it from the otherwise intertwined applicable scope of the GDPR. See *Bienemann*, Reformbedarf des Kunsturhebergesetzes im digitalen Zeitalter, S. 244f.; Frey, in *Schwartmann, et al.*, DS-GVO/BDSG, Art. 85 Rn. 39.

619 However, if the album constitutes or is intended to constitute a filing system structured according to specific criteria, it might fall under the scope of the GDPR. See Recital 15.

ferent laws, It would be far more complex than admitting the precedence of the GDPR. Moreover, it would be questionable whether the case law about "apron protection" (*Vorfeldschutz*)[620], based on the general personality right, fulfills the requirements underscored in Art. 85 (1) GDPR. If not, legal fragmentation and uncertainty because of the production chain of personal photos would be inevitable and might bring far more serious problems than not being able to apply the KUG. Moreover, the numerous and extensive regulatory differences between the GDPR and the KUG remain and await balancing depending on concrete assessments.

There are some pragmatic solutions in Germany being sought to tackle this controversy. The concern that new provisions in the GDPR, in particular, Art. 6 (1)(f) GDPR would not be supported by sufficient case law, can be addressed by introducing German jurisprudence in weighing adversarial interests. Against the backdrop that the German casuistry has succeeded in striking a fair balance between the personality rights and the freedom of expression following the case law of the ECtHR in the field of §§ 22, 23 KUG, the BVerfG has interpreted the GDPR in compliance with the European fundamental rights anchored in the Charter through a "German lens". In doing so, it respects the primacy of EU law on the one hand, and on the other incorporates considerations of German jurisprudence in the areas covered by EU law.

### 1.3 Evaluation

Based on a reflection of the literature, Art. 85 (1) GDPR is a rather typical, yet deliberately ambiguous norm created by the EU legislator. There is some validity to the arguments of both opposing sides. On the one hand, a too restrictive interpretation of the maneuver space of the Member States granted by Art. 85 GDPR would create the risk that the EU law would achieve full harmonization with respect to the balance between freedom of expression and the right to privacy and personality through the "back door" of data protection.[621] Not that it is impossible or unimagined be-

620 Before the GDPR, even when the KUG had been given the special law status over the BDSG, the photo production phase, i.e., before disclosure and publication, had not uniformly treated

621 Schulz/Heilmann, in *Gierschmann, Schlender and al.*, Kommentar Datenschutz-Grundverordnung, Art. 85 Rn. 10.

fore,[622] the balance in this respect depends and shall depend greatly on national culture, history, and values. On the other hand, the GDPR is devised to fully harmonize "the level of protection of the rights and freedoms of natural persons with regard to the processing of such data" for the dual objectives (recital 10). A wide and flexible leeway for the Member States without substantial restrictions prescribed in Art. 85 (2) GDPR is hardly conceivable. Moreover, the continued validity of the KUG cannot be denied for the reason that Germany has only notified the Commission about its state laws on press privilege pursuant to Art. 85 (3) GDPR without mentioning the KUG at all.[623] Because firstly, the obligation for notification laid down in Art. 85 (3) is not a constitutive condition for derogations or exemptions, and secondly, Art. 85 (3) GDPR does not mention Art. 85 (1) GDPR. Therefore, even if it is an independent opening clause, the Member States do not have the obligation to notify the Commission about the adopted national pursuant to Art. 85 (1) GDPR.

Nevertheless, one must be very cautious and refrained in interpreting the opening clauses to avoid preemption of the regulation provided by the GDPR. In addition, this relatively narrow reading of Art. 85 GDPR can be compensated by the liberal understanding of journalistic purposes in the light of "citizen journalism" (see Part II Section 2.3.2). Moreover, even if Art. 85 (1) GDPR is understood as an independent opening clause, it is doubtful whether the KUG can join hands with the GDPR to govern the controversy about (digital) personal portraits. Among other reasons, issues of legal fragmentation and the growing dominance of platforms in users' merchandising scenarios would highlight the incompetence of the KUG in the online environment. Thus, the postulation of Art. 85 (1) GDPR as an independent opening clause fails in its feasibility.

In Germany, a broad understanding of Art. 85 (1) GDPR is rejected by the German highest courts in constitutional law and civil law. Similar to *Recht auf Vergessen I*,[624] the BVerfG only recognized Art. 85 (2) GDPR as

622 *Ohly*, GRUR Int, 2004, 902.

623 EU Member States notifications to the European Commission under the GDPR, see „Notifizierungspflichtige Vorschriften Deutschlands gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) Gesetze des Bundes", at https://ec.europa.eu/info/sites/default/files/de_notification_articles_49.5_51.4_83.9_84.2_85.3_88.3_90.2_publish.pdf.

624 BVerfG, GRUR 2020, 74 - Recht auf Vergessen I, para. 74.

the opening clause: As activities conducted by search engines are not serving journalistic purposes, the BVerfG rejected the application of domestic law deviating from the GDPR in this constellation.[625] This consideration also held in the case of *Recht auf Vergessenwerden* ruled by the BGH.[626]

Specified in merchandising scenarios, the replacement of the recourse mechanism in the GDPR by the German remedies is superfluous in solving the under-protection problem. In essence, this proposal offers no more benefit than the assistance of the law of unjust enrichment that coexists with the recourse mechanism of the GDPR. However, the substitution of German remedies would result in data subjects being placed at a disadvantage relative to the GDPR in terms of moral compensation. For one, moral damages must be severe to receive compensation in Germany. For another, the person depicted loses the protection facilitated by the data subject's rights and thus the damages due to the failure to respond to rights in time. In this case, a reverse-discrimination for celebrities is conceivable. Merchandisers are also likely to be free from damages when they are negligent in fulfilling the GDPR-compliant requirements. Even though these would not make a huge difference in merchandising cases as mental impairment is very rare in some residual unauthorized merchandising cases, the discrepancy between the German legal regime and the GDPR in terms of mental damages seems unjustified. Given the inferior position of commercial speech in the freedom of speech,[627] there seems to be no legitimate reason for controllers not to provide sufficient information to the data subject promptly.

As many regulations in the regime of the right to one's image rely on both the BGB and the case law. A conclusion that they all strike a fair balance between the freedom of speech and information and the protection for personal data pursuant to the GDPR can neither be drawn in principle nor without a careful evaluation based on detailed comparisons. Therefore, a well-reasoned application of the KUG in merchandising would be indispensable because courts must demonstrate that the specific law/case law reconciles the GDPR and the freedom of speech. In this wise, a full account of the motivation and significance of the data processing must be taken in applying the KUG and its jurisprudence based on Art. 85 (1)

625 BVerfG, NJW 2020, 314 - Recht auf Vergessen II, para. 41.
626 BGH, GRUR 2020, 1331 - Recht auf Vergessenwerden, para. 36.
627 *Peers, Hervey, Kenner and Ward*, The EU Charter of Fundamental Rights: A Commentary, Art. 11 paras. 11.28 and 11.40; *Harris, O'Boyle and Warbrick*, Law of the European Convention on Human Rights, 461 et seq.

GDPR. Issues about legal uncertainty would probably take place because no one knows when exemptions and derogations from the GDPR would be made.

The high degree of legislative freedom enjoyed by member states based on Art. 85 (1) GDPR can seriously affect the harmonization of data protection within the EU. This broad understanding of freedom of expression, and in particular the inclusion of purely commercial advertising in the scope of what needs to be considered, runs the risk of circumventing the entire regulation of the GDPR. It would bring uncertainty at the EU level because every Member State would form a self-contained system of merchandising. After all, opening clauses should be restrictively understood as a principle to guarantee the harmonization of data protection within the EU.

At the micro-level within one Member State, the high degree of flexibility enjoyed by courts in deciding to what extent is the application of the KUG or the GDPR reasonable presents, from the other side of the coin, legal uncertainty. More importantly, this problem is almost unsolvable because the reconciliation between data protection and freedom of speech relies on the weighing of interests in individual cases. As mentioned above, the application of certain provisions in the GDPR is also necessary in merchandising cases, but the reasonableness lies in the detail.

## 2. *Art. 6 (1) (f) GDPR as an additional lawful ground for authorized merchandising*

### 2.1 The significance of this proposal

#### 2.1.1 The application of Art. 6 (1) (f) GDPR in a contractual relationship

As argued in Part II Section 3.1, merchandisers cannot invoke Art. 6 (1) (f) GDPR as the lawful ground for data processing for merchandising purposes because the interests and rights of the data subject override the commercial interests of the controller. However, in the case of commercial cooperation in merchandising, the balance of interests may be slightly different because the data controller acquires additionally legally protected reliance interests derived from the contract or consent given by the data subject based on the contract.

Though it may seem odd to rely on a legal ground rather than on the autonomous decision of the data subject to legitimize data processing

that has been approved and desired by that data subject,[628] Recital 47 of the GDPR does not preclude the application of Art. 6 (1) (f) GDPR in a contractual relationship.[629] In this wise, in addition to the purpose of promoting its products, the reliance interest of the controller arising from the commercial cooperation with the data subject, as a legally protected commercial interest, could also constitute a legitimate interest prescribed in Art. 6 (1) (f) GDPR. Against this backdrop, it might be possible for the controller to rely on Art. 6 (1) (f) GDPR to legitimize its data processing for merchandising on the premise of a valid merchandising contract between the controller and the data subject. One of the questions is, nonetheless, whether the lawful ground at this point is Art. 6 (1) (f) GDPR alone or a cumulation of consent (Art. 6 (1) (a)), the contract (Art. 6 (1) (b)) and the balance of interests (Art. 6 (1) (f)). For the same reasons mentioned in Part II Section 4.3.2 (2), it is argued here that the balance of interests should be relied upon alone.[630] As long as the merchandising contract has not been invalidated or withdrawn under the national law, the controller has the protected interests in the data processing.

The other question is more substantial as to whether the legitimate interests of the controller outweigh the rights, freedoms, and interests of the data subject in this context. The reliance interest of the controller derives from the commitment of the data subject in the freely negotiated merchandising contract. Upon the reliance interest in the binding contract, the controller usually invests not insignificant money and time to increase sales or brand exposure for a relatively long period (during the duration of the contract).

German courts have consistently ruled that the revocation of consent in merchandising contracts requires a weighing of interests following the

628 According to Art. 8 (2) of the Charter, lawful grounds for data processing are distinguished between autonomy (consent and arguably the contract) and heteronomy. The first sentence of Art. 8 (2) of the Charter states, "such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law". Also considering Art. 6 (1) (f) GDPR as a foreign body (*Fremdkörper*) for the partnership, see *Bunnenberg*, Privates Datenschutzrecht: über Privatautonomie im Datenschutzrecht, S. 61, 64.

629 The second sentence of Recital 47 suggests that legitimate interests of the controller for data processing could exist "where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller".

630 Simply put, it is mainly to avoid causing misunderstandings of the data subject, and the cumulation does not bring more guarantee to the data controller.

principle of good faith in § 241 (2) BGB, even though the conflicting interest is the right of self-determination in the image of the person depicted.[631] In other words, the person depicted must demonstrate convincingly that why he or she has to exert the right of self-determination in a contrary way to override the reliance interests of the merchandiser. Although the interests-balancing according to Art. 6 (1) (f) GDPR should be observed from the perspective of the EU data protection in light of the fundamental rights and freedoms, the reasonable expectations of the data subject introduce the possibility of reflection based on the (legal) culture and traditions of the Member States (see Part II Section 3.1.1 (4)). Moreover, as German cases show, the balance of interests in assessing the revocability of consent has already taken the fundamental rights and freedoms anchored into account.

Therefore, it is possible to argue that upon a valid merchandising contract under national law, the controller may invoke Art. 6 (1) (f) GDPR to legitimize its data processing for merchandising, and the reliance interest of the controller overrides as it also falls under the scope of the reasonable expectations of the data subject in Germany, at least. The controller should make it clear to the data subject that the contract between them is not the lawful ground for data processing under the perspective of the GDPR. In this sense, the data subject is unable to withdraw consent at any time according to Art. 7 (3) GDPR because the lawful ground for data processing is not the consent under Art. 6 (1) (a) GDPR. However, if the contract expires, or the consent in the contract law is successfully withdrawn by the data subject according to national law, then Art. 6 (1) (f) GDPR alone cannot support further data processing because the reliance interest of the controller would no longer be extant.

### 2.1.2 Conducive for the bindingness of a merchandising relationship

The advantages of this solution are obvious. First, Art. 6 (1) (f) GDPR provides a more stable legal position for the data controller compared to the anytime revocable consent. Since this lawful ground derives from heteronomy instead of autonomy, the control of personal data does not lie in the hand of the data subject. Second, by relying purely on the balancing

631 See BAG, GRUR 2015, 922 - Veröffentlichung von Arbeitnehmer-Bildnissen zu Werbezwecken, Rn. 34f. and 38; LG Köln, AfP 1996, 186 - Model in Playboy; OLG München, NJW-RR 1990, 999 - Wirtin.

test coupled with merchandising contracts under German law, controllers do not have to worry about consent and contracts, which have strict yet controversial conditions for validity, such as the requirement of necessity. Third, controllers (merchandisers) hardly need to make changes to the existing business operations in the context of Art. 6 (1) (f) GDPR. In addition to the documentation of the merchandising contract (as controllers used to do before the GDPR), they merely need to keep documentation about the assessment of the conflicting interests of both sides according to the principle of accountability. Lastly, the risk-based approach seems to favor a lightened interests-balancing for the data controller in authorized merchandising cases.

## 2.2 Limitations of this proposal

### 2.2.1 Legal uncertainty and overpressure on the general clause

Disadvantages of Art. 6 (1) (f) GDPR as the lawful ground for a relatively long-term relationship valuing trust and cooperation are at hand.

The balance of interests is by nature uncertain. It closely depends on concrete facts. In merchandising cases, details of the contract, professionality of the data subject and his or her power in relation to the controller, and ways of presentation are all capable of changing the result of the balancing test. For instance, as some scholars stated, if the merchandiser in a time-for-print contract has taken unfair advantage of the informational and power asymmetry of the model, then the validity of that contract should be questioned.[632] In this wise, the legitimacy of the controller is still uncertain because it is dependent of the validity of the merchandising contract. It is therefore almost unrealistic for merchandising companies to tie their entire business model to the lawful ground that is both subject to rejection at any time and dependent on the balance of interests.

Even though the controller is confident about the outcome of the balancing of interests, it must stop processing until the "verification whether the legitimate grounds of the controller override those of the data subject" whenever the data subject claims the right to restriction in Art. 18 (1) (d) in combination with Art. 21 (1) GDPR. Thus, the merchandiser must take down the advertising online or stop the circulation of the prospects or magazines (Art. 18 (2) GDPR). While the GDPR seems to hold the

632 *Vogler*, AfP, 2011, 139 (141).

opinion that the verification should be carried out by the controller itself, scholars argue that the courts have the final decision.[633] Thereby, the legitimacy of the controller is in a position that it can be challenged at any time. It is unthinkable for a businessman as a degree of certainty and predictability are fundamental to business operations.[634]

Another flaw originates from the nature of general clauses. Extensive use of a general clause contradicts its purpose of being an "overpressure relief valve" for vastly developing technology and society.[635] The general clause, always in the tension of legal flexibility and uncertainty, is the last resort for guaranteeing the principle of fairness in concrete cases.[636] Since the questioned binding effectiveness of merchandising contracts under the GDPR is a systematical problem created by the overarching data paternalism in the EU data protection law, it would be better to seek a systematical solution instead of applying the general clause of the lawfulness of data processing in the GDPR systematically.

### 2.2.2 Fundamentally incompatible in authorized merchandising scenarios

Apart from the drawbacks, the most detrimental disadvantage derives from the fundamental incompatibility between the rationales underlining Art. 6 (1) (f) GDPR and authorized merchandising. In Germany, the right to one's image takes a long journey from a defensive right that only focuses on moral interests to a positive right that is licensable to some extent. The analogy of the soft licensing model of one's portraits with the copyright in Germany is an elegant dogmatical solution to enhance instead of undermining human dignity and the free development of personality by legitimatizing the practical development of self-determination without dismissing the market-inalienability of personality. It has been acclaimed both in academia and practice.

Admittedly, the freely negotiated merchandising contract is the central hinge of this solution under the guise of balance tests according to Art. 6 (1) (f) GDPR. However, from the surface, the decision has once again been

633 Dix, in *Simitis, et al.*, Datenschutzrecht, Art. 18 Rn. 9; Herbst, in *Kühling/Buchner*, DSGVO/BDSG, Art. 18 Rn. 27.

634 See *Beale*, in: *de Elizalde, Uniform Rules for European Contract Law?: A Critical Assessment*, 9 (23).

635 *Sattler, in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance – Contract Law 2.0?*, 225 (243).

636 *Ohly*, AcP, 2001, 1 (7).

taken from the hand of the data subject to the court and, essentially, the controller. Against this backdrop of the GDPR, the heteronomy facilitated by this lawful ground takes place of the autonomy in merchandising scenarios, and the contract between the data subject and the controller is reduced to the accompaniment of the balance test.[637] In this sense, it would not amount to an elegant solution for merchandising scenarios. The reliance on the heteronomy would also restrict the rights granted by the GDPR for the data subject. For instance, the right to portability is merely applicable for the data processing based on the autonomous decision of the data subject, although the restriction would be harmless as the right to portability would not have made much sense in merchandising cases.

### 2.2.3 Unable to address the long-term consequences

Leaving the objections aside, Art. 6 (1) (f) GDPR focuses merely on lawful data processing i.e., authorized merchandising. Even though the under-protection problem per se is innocuous because the restitution for a fictive licensee fee based on unjust enrichment in Germany can be smoothly applied in unauthorized merchandising cases, it cannot address the long-term consequences of the under-protection problem. The general insensitivity of data subjects to the commercial value of their data would still be the case. To make matters worse, Art. 6 (1) (f) GDPR helps in covering these problems by replacing the autonomous decision of the data subject with the objective interests-balancing. It seems that the data subject is being decided by the controller and the court instead of being the decider for merchandising.

637 *Veil*, NJW, 2018, 3337 (3343). It addresses the highly different connecting factors for self-determination (consent) and the balance of interests as lawful grounds for data processing.

## 3. Recalibrating the application of Art. 6 (1) (b) GDPR in the B2B merchandising

### 3.1 Other possibilities of the interpretation of Art. 6 (1) (b) GDPR

#### 3.1.1 The EDPB's Guidelines and some scholars' proposition

There are two other noteworthy points of view, both of which tend to interpret the ambit of Art. 6 (1) (b) GDPR broadly for their own agenda.

Besides some similarities, the EDPB's *Guidelines*' interpretation of Art. 6 (1) (b) GDPR in the online environment have major differences to the mainstream opinion discussed in Part II Section 4.3.1. Likely, this interpretation lends Art. 6 (1) (b) GDPR to applying to merchandising contracts, though it is merely aimed at online services.

The EDPB's *Guidelines* do not confine the applicability of Art. 6 (1) (b) GDPR within accessory types of data processing to the performance of a contract; Rather, it maintains that the requirement of necessity means that Art. 6 (1) (b) GDPR can legitimize data processing that is absolutely necessary to achieve the (objective) purpose of the contract.[638] In the first step, the EDPB inquiries about the objective expectations of the contracting parties and categorizes the contract according to the nature and specific characteristics of the service provided by controllers;[639] Subsequently, the EDPB compares the objectively determined purpose with the data processing envisioned by the controller and assesses objectively whether there is a less intrusive operation of data processing.[640] The approach to confine data processing to the least intrusive operation stems from the interpretation of CJEU regarding Art. 7 and 8 of the Charter.[641]

---

638 See EDPB, 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, para. 15 and 25.

639 See ibid., para. 30, 33, 36. It encourages finding out the expectation of average data subjects by asking questions, such as "what is the nature of the service being provided to the data subject", "what is the exact rationale of the contract", and "what are the mutual perspectives and expectations of the parties to the contract".

640 See ibid., para. 25.

641 See CJEU, Volker und Markus Schecke, Joined Cases C-92/09 and C-93/09, para. 74, 76 and 77; CJEU, Digital Rights Ireland and Others, Joined Cases C-293/12 and C-594/12, para. 56; CJEU, Rīgas, C-13/16, para. 30; Recital 39 of the GDPR; *Bygrave,* Data Privacy Law: An International Perspective, S. 150.

As a result, while the EDPB's interpretation and the prevailing opinion both reject the application of Art. 6 (1) (b) GDPR in the commercialization of personal data, their reasons are different. The EDPB does not consider the commercialization of personal data meets the genuine wish of average data subjects, whereas scholars holding the prevailing opinion fear that it would circumvent the enhanced protection for data subjects facilitated by the anytime revocable consent. In other words, the majority opinion does not base on the wish of the data subject. Hence, one would argue that a deviation from the free choice of the data subject is observed in the dominant opinion in respect of the commercialization of personal data, while the EDPB's approach respects the data subject's self-determination but negates the commercialization for other reasons.

Therefore, the difference between this opinion and the leading one in the literature emerges in those scenarios where the data processing is primary performance of the contract as well as absolutely necessary to achieve the objective contractual purpose. For instance, as the EDPB reckons, data processing for the provision of personalized content may invoke Art. 6 (1) (b) GDPR as it may be necessary for the performance of the contract.[642] While it is arguably that the main performance of such contracts is data processing, this service is on top of a large amount of personal data and profiling. The data processing in this context is by no means an accessory type.

Against this backdrop, it motivates one to wonder the standpoint of the EDPB for merchandising. First of all, as drawn in Part II Section 4.3.1 (2), the requirement of (absolute) necessity is in general fulfilled in merchandising contracts since there is no less intrusive means to achieve the contractual purpose agreed upon by the data subject has freely and prudently.[643] Secondly, it motivates one to wonder the standpoint of the EDPB for merchandising since it considers that the data processing for the provision of personalized content might meet the necessity requirement, and clearly, merchandising needs significantly less personal data and is less risky than it. Therefore, one may argue that merchandisers may invoke Art. 6 (1) (b) GDPR to legitimize the data processing according to the rela-

642 See EDPB, 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, , para. 57.

643 Vgl. Ettig, in *Koreng and Lachenmann,* Formularhandbuch Datenschutzrecht, J. Datenschutz und Personenbildnisse, III. Model-Release-Vereinbarung, S. 1317.

tively conservative opinion of the EDPB, while an official interpretation by the CJEU stalls.

### 3.1.2 A relatively liberal reading of the ambit of Art. 6 (1) (b) GDPR by some scholars

Stemming from the principle of private autonomy, some scholars propose a relatively liberal reading of the ambit of Art. 6 (1) (b) GDPR.[644] Just as the mutual understanding of data subjects and controllers in implementing their willing should be respected, so too should the construction of the contract regarding data processing.[645] Data processing is thus *prima facie* "necessary for the performance of a contract" if it has been specified, anticipated and desired by the data subject to achieve the purposes pursued by both parties; thereby, the rejection to provide personal data by the data subject would be considered as in bad faith.[646] After all, the literal interpretation of Art. 6 (1) (b) GDPR also leaves room for this interpretation. Moreover, this approach would not compromise the fundamental rights of data subjects – the right to the protection for personal data because the compliance rules in the GDPR including the principles of data processing and the contractual and consumer protection laws in the Member States are also applicable.[647]

This premise for this proposition is relatively narrow as the free negotiation between data subjects and controllers must be present.[648] Otherwise, data controllers would exploit personal data unrestrictedly under the guise of contracts without being subject to the anytime revocable consent by merely including the data processing in the contract.[649] In this sense, this approach shares several commonalities with the mainstream opinion. They

644 Vgl. *Engeler*, ZD, 2018, 55 (57f.); Albers/Veit, in *Brink/Wolff*, BeckOK Datenschutzrecht, Art. 6 Rn. 44f.; *Bunnenberg*, Privates Datenschutzrecht: über Privatautonomie im Datenschutzrecht, S. 53 ff.

645 *Heinzke and Engel*, ZD, 2020, 189 (192).

646 See Schantz, in *Simitis, et al.*, Datenschutzrecht, Art. 6 Rn. 32; Schulz, in *Gola*, DSGVO, Art. 6 Rn. 37; *Bunnenberg*, Privates Datenschutzrecht: über Privatautonomie im Datenschutzrecht, S. 57.

647 See *Engeler*, PinG, 2019, 149 (152f.); *Rott*, GRUR Int., 2018, 1010 (1012).

648 Schantz, in *Simitis, et al.*, Datenschutzrecht, Art. 6 Rn. 32.

649 Vgl. Albers/Veit, in *Brink/Wolff*, BeckOK Datenschutzrecht, Art. 6 Rn. 32; Buchner/Petri, in *Kühling/Buchner*, DSGVO/BDSG, Art. 6 Rn. 39; Schulz, in *Gola*, DSGVO, Art. 6 Rn. 39.

both agree to prohibit the commercialization of personal data through standard contracts. In addition, both approaches require a direct connection between the data processing and the specific purpose of the contract by ordering the processing must be "adequate, relevant and limited to what is necessary" for that purpose.[650]

Another scholarly view chooses the term "necessary" in Art. 6 (1) (b) GDPR as the dogmatic starting point to distinguish the applicable scope of Art. 6 (1) (a) and (b) GDPR and thus to reconcile the national contract law and the GDPR.[651] By considering that the free revocable consent is less intrusive than a binding contract for the data subject, it assesses whether the free revocability of consent as an alternative for the binding contract is objectively reasonable for the controller.[652] In this wise, the requirement of necessity, on the one hand, is not stretched too much to exclude data processing as the main performance of the contract in general, and on the other, does not allow every data processing prescribed in the contract to enter the gate.

Both scholarly opinions offer a hint of breathing space for merchandising contracts to apply Art. 6 (1) (b) GDPR when the contracts are not pre-drafted standard contracts that models/data subjects cannot insert any influences in the terms.

## 3.2 The objections to these interpretation

### 3.2.1 Criticism of the EDPB's Guidelines and evaluation

The approach taken by the EDPB is criticized by scholars for many reasons. The most convincing one is that the purely objective assessment is, in essence, a balancing of interests anchored in Art. 6 (1) (f) GDPR and thereby ignores the protection of personal autonomy advocated by Art. 6

650 Recital 39 of the GDPR; EDPB, 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; See also Recital 44; Albers/Veit, in *Brink/Wolff*, BeckOK Datenschutzrecht, Art. 6 Rn. 32; *Plath*, DSGVO/BDSG, Art. 6 Rn. 12; Buchner/Petri, in *Kühling/Buchner*, DSGVO/BDSG, Art. 6 Rn. 38; Schulz, in *Gola*, DSGVO, Art. 6 Rn. 38; In this direction, see Schantz, in *Simitis, et al.*, Datenschutzrecht, Art. 6 Rn. 33.

651 *Bunnenberg*, Privates Datenschutzrecht: über Privatautonomie im Datenschutzrecht, S. 54.

652 Ibid., S. 56f.

(1) (b) GDPR.[653] By forbidding "artificially" expanding the scope of data processing by the controller, this approach cannot find its support in the GDPR and also poses risks in reshaping national contract law.[654] The categorization of contracts to explore the "*essentilia negotii*" of that contract is subject to criticism of being willful.[655] Moreover, its feasibility is also rightfully challenged because of the trend toward convergence in the variety of web services.[656] Large platforms try to combine all services, which makes it increasingly difficult to judge the necessity of the approach by distinguishing the different purposes of data processing. Lastly, as the EDPB rejects the application of Art. 6 (1)(b) GDPR in justifying the commercialization of personal data,[657] it is difficult to explain the application of Art. 6 (1)(b) GDPR to free personalized service prevailing on platforms. Last but not least, the proposal of the EDPB is relatively conservative compared with the prevailing opinion as it confines itself within the business model "data against service".[658] This business model is quite limited in application in the dawn of big data, machine learning and AI.[659] Conceivably, controllers will come up with new business models to harvest personal data. It thus would make more sense not aim at a particular business model but a business logic.

Besides, it is also contended here that the argumentation drawn by the EDPB suffer from some flaws that render its application untenable.

At the outset, the EDPB argues that because data subjects usually do not know that targeted advertising based on profiling is used to monetize the so-called "free" services, there is no intention of data subjects to con-

653 Critics on the ambiguity and uncertainty of the objective assessment adopted by the EDPB's *Guidelines*, see *Engeler*, PinG, 2019, 149 (151-152); Schantz, in *Simitis, et al.*, Datenschutzrecht, Art. 6 Rn. 32; Buchner/Petri, in *Kühling/Buchner*, DSGVO/BDSG, Art. 6 Rn. 45.

654 *Indenhuck and Britz*, BB, 2019, 1091 (1094f.).

655 Vgl. Schulz, in *Gola*, DSGVO, Art. 6, Rn. 37.

656 See *Engeler*, ZD, 2018, 55 (57).

657 See EDPB, 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, para. 53 and 54.

658 *Sattler, in: Pertot, Rechte an Daten*, S. 70.

659 *Posner and Weyl*, Radical Markets: Uprooting Capitalism and Democracy for a Just Society, 213 et seq. It explains how "factories for thinking machines" work based on the neural networks.

clude such a contract for "data against services".[660] Therefore, on the flip side, it can be deduced that if the data subject is aware of the *quid pro quo* relationship between the processing of personal data and the "free" services, his or her will – be it revocable consent or binding permission – shall be respected. The EDPB's second argument is that Art. 21 (2) GDPR supports the exclusion of data licensing agreement for profiling: A special opt-out right for direct marketing indicates the cautious and restrictive mentality of the GDPR towards personal profiling.[661] However, it cannot lead to the conclusion that the data subject is prohibited to agree on behavioral advertising as remuneration. Rather, the controller who opts in this business model is subject to this special opt-out right of data subjects. Lastly, the examples and argumentation advanced in the EDPB's *Guidelines* imply another reason for deviating from the choice of the data subject, i.e., the voluntariness of data subjects is endangered due to power asymmetry since data objects always face a "take it or leave it" situation.[662]

Hence, these arguments cannot lead to a general exclusion of Art. 6 (1) (b) GDPR in scenarios of "data against service". It could be argued that if the data subject knows and requests the data processing voluntarily, even if it concerns profiling as the necessary tool for providing personalized content, which is deemed significantly risky for the rights and freedoms of data subjects, the will of that data subject may still be considered within the EDPB's framework.[663]

Therefore, the EDPB's *Guidelines* are not followed because of its flaws and more importantly, its inapplicability to merchandising.

### 3.2.2 Possible counterarguments

The most convincing argument against the relatively liberal reading of Art. 6 (1) (b) GDPR is advanced by the scholars with the mainstream opin-

660 EDPB, 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, para. 4.

661 Ibid., para. 52.

662 It revolves around "contracts for online services, which typically are not negotiated on an individual basis." Moreover, the examples it listed focus on digital service scenarios, which are often triggered by the user's consent to standard contracts unilaterally drafted by the data controller. See ibid. para. 16, and the examples.

663 Vgl. *Indenhuck and Britz,* BB, 2019, 1091 (1092).

ion. The wider reading of the ambit of Art. 6 (1) (b) GDPR would result in an escape from the consent ("*Flucht vor der Einwilligung*"),[664] because controllers as big platforms can easily apply professional contract writing skills to meet the requirement of necessity. To use an online service, internet users are used to signing the privacy policy provided by the digital service provider. Although most privacy policies today are templates written by controllers, it is easy for them to argue, with some fine-tuning, that many of the conditions are subject to negotiation with data subjects. If this argument is supported, then the anytime freely revocable consent would not be used anymore. This is the exact situation the GDPR aims to prevent by emphasizing the free revocable consent.[665]

Moreover, difficulties in assessing the mutual expectations of the parties are undeniable given the increasingly complex contract designs.[666] One would reasonably argue that even in a freely negotiated contract, the data subject does not well comprehend the purpose, content, and means of the data processing (See examples about the relationship between "idol trainees" and powerful agencies in Part II Section 3.2.2 (4)). Thus, a loophole according to the systematic interpretation of Art. 6 (1) GDPR surfaces not because the anytime revocable consent must be applied in preference,[667] but because the GDPR's objective of deploying the ready revocability of consent to protect data subjects would fall short.[668]

The emphasis on the concept of "necessary" as a normative correction (*normatives Korrektiv*)[669] according to *Bunnenberg* is a commendable solu-

664 Frenzel, in *Paal and Pauly*, DS-GVO BDSG, Art. 7, Rn. 26; Also in Langhanke and Schmidt-Kessel, 4 Journal of European Consumer and Market Law 218 (2015) (221).

665 Buchner/ Kühling, in *Kühling/Buchner*, DSGVO/BDSG, Art. 7 Rn. 39; *Tinnefeld and Conrad*, ZD, 2018, 391 (396).

666 *Heinzke and Engel*, ZD, 2020, 189 (192).

667 Buchner/Kühling, in *Kühling/Buchner*, DSGVO/BDSG, Art. 7 Rn. 16; Schulz, in *Gola*, DSGVO, Art. 6 Rn. 10; Heckmann/Paschka, in *Ehmann and Selmayr*, DS-GVO, Art. 7 Rn. 17; Plath, in *Plath*, DSGVO/BDSG, Art. 6 Rn. 5; *Piltz*, K&R, 2016, 557 (562); In this direction, see Schanz, in *Simitis, et al.*, Datenschutzrecht, Art. 6 Rn. 11 The opposite opinion, see Frenzel, in *Paal and Pauly*, DS-GVO BDSG, Art. 7 Rn. 1; *Sattler*, JZ, 2017, 1036 (1040).

668 Stemming from the purpose of emphasizing individuals' control over personal data, consent in Art. 6 (1) (a) GDPR shall be prevented from restrictive interpretation. Moreover, compared to other legitimate grounds, Art. 8 of the Charter focuses on the data subject's consent specifically.

669 Albers/Veit, in *Brink/Wolff*, BeckOK Datenschutzrecht, Art. 6 Rn. 44; A similar term "evaluative corrective" (*wertendes Korrektiv)* stems from *Bunnenberg*, Privates Datenschutzrecht: über Privatautonomie im Datenschutzrecht, S. 59.

tion because it chooses the path of data protection law rather than contract law.[670] It is more warranted compared to the EDPB's *Guidelines* as it inquires the "the motives of the parties behind the conclusion of the transaction" (*die hinter der Geschäftseingehung stehende Motivlage der Parteien*).[671] However, at the second point, the approach of absolute necessity deployed by the EDPB is directly adopted in private sector without further explanation. Free revocable consent is indeed less intrusive than a binding contract for the data subject. This is also illustrated by *the ladder of permission*, of which free revocable consent is at the bottom due to its weakest binding effect on the subject. Nonetheless, the question that the author does not address is why, in the realm of private autonomy, data subjects do not have the freedom to choose to climb one rung higher – the binding contract.

Admittedly, the principle of data minimization may play a role in interpreting the concept of "necessary",[672] but it mainly concerns the content of personal data and the necessity to process personal data at all.[673] The CJEU also adopted the approach of absolute necessity in data processing conducted by public authorities.[674] The EDPB's *Guidelines* focus merely on online services where the contracts are generally pre-drafted standard contracts that are typically signed by the users without looking. It cannot

670 The distinction between solutions based on data protection law and contract law, see *Funke,* Dogmatik und Voraussetzungen der datenschutzrechtlichen Einwilligung im Zivilrecht, , S. 271f.; The solutions on the basis of contract law centering on the consumer protection and the content control of contracts pursuant to the BGB, see Schulz, in *Gola,* DSGVO, Art. 6, Rn. 27 und 37; *Engeler,* ZD, 2018, 55 (58); *Indenhuck and Britz,* BB, 2019, 1091 (1094 f). The approval of this solution, see Albers/Veit, in *Brink/Wolff,* BeckOK Datenschutzrecht, Art. 6 Rn. 44.

671 The author describes it as the "objective purpose of the contractual relationship" in line with the EDPB's *Guidelines* though. See *Bunnenberg,* Privates Datenschutzrecht: über Privatautonomie im Datenschutzrecht, S. 58.

672 EDPB, 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, , para. 15; Roßnagel, in *Simitis, et al.,* Datenschutzrecht, Art. 5, Rn. 116.

673 "The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed". "Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means." See Recital 39 of the GDPR.

674 CJEU, Volker und Markus Schecke, Joined Cases C-92/09 and C-93/09, para. 77; CJEU, Rīgas, C-13/16, para. 30; see EDPS, Assessing the Necessity of Measures that limit the fundamental right to the protection of personal data, 7.

lead to the conclusion that the approach of absolute necessity should be followed in all types of contracts.

It is even more questionable when *Bunnenberg* finally argues that Art. 6 (1) (b) GDPR is applicable if the reliance interest of the controller overrides the interest of the data subject to revoke consent at any time.[675] In this wise, since the readily revocable consent is not reasonable for a merchandiser,[676] the data subject seems to be prohibited to choose consent in Art. 6 (1) (a) GDPR even if the controller agrees. This outcome would be unreasonable in users' merchandising scenarios. Considering the *hair salon* case, if the data subject agrees with the use of her photos on the fan page of the hair salon for some discount, would she not be allowed to withdraw her consent at any time and thus ask the controller to take down her photos? Based on the theory of *the ladder of permission*, there are a variety of conditions that need to be considered for the rightful holder to have more binding dispositional power upward, but downward extensions usually do not require justification.[677] Therefore, the assessment of the concept "necessary" presents an evident resemblance with the application of Art. 6 (1) (f) GDPR in contractual relationship (see above Chapter 3), which rests on a balance of interests instead of an advocation of personal autonomy anchored in by Art. 6 (1) (b) GDPR.

The main issue is that it seems to overlook the fundamental differences between merchandising and the model of "data against service". The EU data protection legislator tacitly acknowledges that in the context of data exploitation the data subject cannot actively choose as the choices he or she makes are predetermined by controllers. Data subjects are hence "nudged" to the lowest step of *the ladder of permission* to protect themselves, and if they want to be binding by contracts, an objective weighing of interests including the requirement of necessity is required.[678] Using the concept "necessary" to distinguish the applicable scope of consent and a

675 In the book, the author argues that Article 6(1) (b) GDPR is only applicable if the controller cannot reasonably be expected to obtain the consent of the data subject; and unreasonableness is indicated when the controller can claim a special interest in the binding nature of the legal relationship, which takes precedence over the data subject's interest in revocation in the given case. See *Bunnenberg*, Privates Datenschutzrecht: über Privatautonomie im Datenschutzrecht, S. 57.

676 Ibid., S. 59-60.

677 *Ohly*, "Volenti non fit iniuria": die Einwilligung im Privatrecht, S. 144 und 146.

678 Brinkmann, in *Gsell, Weller and Geibel*, GROSSKOMMENTAR zum Zivilrecht: BeckOGK, § 307 Datenschutzklausel Rn. 16.

contract within the scenario envisaged by the legislator may be warranted, but it would be inappropriate to use this normative correction stemming from the principle of proportionality without justification to regulate civil transactions.[679]

## 3.3 Applying Art. 6 (1) (b) GDPR to merchandising in the B2B context

### 3.3.1 Arguments and advantages of this solution

#### (1) The legal basis for this solution

It is argued here to make an exception from the leading opinion of Art. 6 (1) (b) GDPR by considering merchandising contracts in the B2B (Business to Business) context a special contract type, and as it fulfills the two requirements in the provision literally Art. 6 (1) (b) GDPR is applicable.

First of all, the application of Art. 6 (1) (b) GDPR to merchandising in the B2B context does not prevent circumvention of Art. 6 (1) (a) GDPR as the anytime revocable consent is not dodged by controllers to compromise the objective of the GDPR in protecting data subjects from data exploitation. Rather, it is to guarantee contract law is not replaced or overturned by the GDPR.[680] This reading has its support in the GDPR.[681] By advocating an understanding of the requirement of necessity "in the context of a contract", recital 44 GDPR requires the respect to autonomous contracts.[682]

Moreover, the control of data subjects over personal data is not only materialized in the free revocability of consent but also the principles of data fairness, transparency, and accountability as well as the data subject's

679 *Rüpke, Lewinski and Eckhardt,* Datenschutzrecht, S. 172-175; Schantz, in *Brink/Wolff,* BeckOK Datenschutzrecht, Art. 5, Rn. 26. The problem of applying the principle of proportionality in horizontal relationship has also been noticed by the proposer of this solution, see *Bunnenberg,* Privates Datenschutzrecht: über Privatautonomie im Datenschutzrecht, S. 55.

680 Albers/Veit, in *Brink/Wolff,* BeckOK Datenschutzrecht, Art. 6 Rn. 44.

681 It is argued that the general restriction of the applicability of Art. 6 (1) (b) GDPR in auxiliary data processing cannot find a legal basis in the GDPR. See *Indenhuck and Britz,* BB, 2019, 1091 (1095f.).

682 It states, "processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract."

rights. After all, the GDPR is not a single provision regarding lawfulness but a legal system to guarantee high-level data protection.

Thirdly, the restrictive ambit of Art. 6 (1) (b) GDPR may go too far in merchandising in the B2B context. All the opinions including the mainstream one focus on the pre-drafted standard contracts prevailing in the "data against services" model because data subjects are likely to inadvertently enter a binding relationship, and data controllers from using contracts to take (permanent) possession of personal data and make them serve their business purposes exclusively.[683] Given the fact that digital contracts in standard forms are complex, lengthy, and ubiquitous, and "the duty to read" a contract is both impractical and inefficient,[684] data subjects probably do not understand the contracts even if they try, they cannot afford the cost not to be contracting or to negotiate at every time of contracting. Thus, an exclusion of this kind of contracts from Art. 6 (1) (b) GDPR seems plausible. As reiterated, this situation differs from merchandising in the B2B context significantly.[685] Professional models and celebrities value their rights and are able to negotiate with agencies about specific terms and conditions. Some pre-drafted standard contracts exist due to efficiency,[686] but they are subject to negotiation on an individual basis.[687] When parties have freely decided the purpose, contents, and duration of the data processing, strong justification is needed to deviate from the principle of private autonomy in the civil law.

In addition, an independent commercial purpose of the controller is highlighted to support the exclusion of Art. 6 (1) (b) GDPR according to the mainstream opinion as it suggests that the data processing is unnecessary and likely to be extensive as well as unmanageable for data subjects. It makes sense in online environment, especially facing with data-driven controllers. However, in merchandising, parties' commercial

683 *Westphalen and Wendehorst*, BB, 2016, 2179 (2185).

684 *Bix*, in: *Miller and Wertheimer*, *The Ethics of Consent: Theory and Practice*, 252 (261 and 264 et seq.). It addresses that contract law generally places the burden to read the documents on the party who signs it. However, when faced with standardized forms of contracts, the traditional doctrine of consent is under "distinct challenges".

685 See Part I Section 3.2.2, Part III Section 3.2.

686 *Indenhuck and Britz*, BB, 2019, 1091 (1093f.); Albers/Veit, in *Brink/Wolff*, BeckOK Datenschutzrecht, Art. 6 Rn. 44.

687 See OLG Frankfurt, NJW-RR 2005, 1280 - Skoda-Autokids-Club, Rn. 39; *Indenhuck and Britz*, BB, 2019, 1091 (1094f.); Vgl. *Westphalen and Wendehorst*, BB, 2016, 2179 (2185f.).

purposes overlap. For instance, in the *landlady* case, the data subject would get more consideration if the controller performed more data processing. This was in line with the common desire of both of them. It would also be contrary to the data subject's commercial purpose if she revokes her commission based on the protection of the GDPR when the controller has completed the preliminary work, including optimizing photos, finding partners, and negotiating contracts, etc.

Furthermore, the characteristics of merchandising hardly raise any concern about undermining the protection for data subjects advocated by the GDPR. In merchandising, the data subjects involved are professionals who are usually not in a position with asymmetry of power or information against the controllers. The purposes and methods of data processing are transparent and fair, and the risks are also defined and relatively small.

Last but not least, while the special protection of data subjects (depicted persons) in German law cannot be used as a reason to exclude the application of the GDPR because of the accessoriness of the national law of obligations to the EU data protection law,[688] the overlaps between the two support a reasonable application of the GDPR in merchandising scenarios. The underlined rationale is that the justification for the high-level data protection at the cost of private autonomy is absent or significantly undermined in the B2B context due to the voluntariness and professionality of the data subject as well as the certainty and low risk in data processing and purpose.

(2) The EDPS' resistance towards merchandising in the B2B context?

The explicit and seemingly strongest argument of the EDPS is that "fundamental rights such as the right to the protection of personal data cannot be reduced to simple consumer interests".[689] By warning against "that people can pay with their data the same way as they do with money", the EDPB strongly criticizes the commercialization of personal data as if the

688 *Bunnenberg*, Privates Datenschutzrecht: über Privatautonomie im Datenschutzrecht, S. 23; *Peitz and Schweitzer*, NJW, 2018, 275 (275-277).

689 EDPS, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, 3.

fundamental rights were salable.[690] However, a fundamental right is not necessarily a negative right without positive components.[691]

The fundamental right to protect one's dignity is two-folded. In addition to the protection from devaluation, one shall act as he or she wishes and takes full responsibility for that decision to "be a human and respect the others as human beings" (*Sei eine Person und respektiere die anderen als Personen*)[692] unless an exception prescribed by law, or moral values applies. Thus, the fundamental right to the protection of personal data contains naturally the imperative to prevent the misuse of personal data, but one cannot conclude that enforcing the informational self-determination by disposing of one's data is prohibited in that fundamental right. The BGH has also addressed that the recognition of the pecuniary components of the right of personality is necessary to guarantee protection against commercial use.[693]

A thorough taxonomy that keeps the restrictions within the necessary limits is thus essential. The abundant jurisprudence of the KUG regarding merchandising demonstrates that a general prohibition of commercialization of personal data under all the circumstances is an excessive and unnecessary (and might also be outdated) solution to protect the free development of personality and human dignity. All in all, the nature of fundamental rights is not a reason to prohibit any means of commercializing personal data but merely the translative transfer.

### (3) The enforcement of this solution

When the data processing reveals some commercial value and is not auxiliary to the performance of the contract, it is generally excluded from the application of Art. 6 (1) b) GDPR. However, if the contract is about merchandising and the data subject is an entrepreneur who possesses the knowledge of merchandising business and makes a living on it, the data processing can invoke an exception to the teleological reduction of the applicable scope of Art. 6 (1) (b) GDPR.

---

690 Ibid.3.

691 The fundamental right to protect one's property in Art. 14 of the Charter is two-folded. One shall protect his or her property from intrusion and dispose of it as he or she wishes unless an exception is prescribed by law applies.

692 *Hegel*, Grundlinien der Philosophie des Rechts, § 36, S. 43.

693 Vgl. BGH, GRUR 2000, 709 - Marlene Dietrich, Rn. 35.

In distinguishing the B2C and B2B context, time-for-print contracts would be the borderline case. Admittedly, young models are often suffering from power asymmetry, and the anytime revocable consent is devised to reverse the inequality. However, despite the lack of negotiating power, they are clear about what they are paying for and the risks they are taking. Moreover, German courts are inclined to recognize the knowledge and decisions of young models in merchandising scenarios, i.e., to respect the rationality of the individual in the absence of clear evidence to the contrary. In the *landlady* case, the higher court in Munich did not consider that the permission to publish her nude photos of the person depicted was a youthful mistake; the court further argued that a 24-year-old is capable of making meaningful decisions about her career choice and lifestyle.[694] Even in the borderline case, the objection for the validity of a time-for-print contract revolved around the young model's level of knowledge instead of her weaker position.[695] In this respect, the borderline cases are clearly distinct from the users' merchandising scenario we have pictured. In users' merchandising, data subjects merely have an abstract yet incomplete idea of their rights and obligations – they have obtained "free" services from the controllers. Even if they are aware that their data become accessible for controllers, they do not know what consequences they might face or whether it is a good deal. In a nutshell, power asymmetry and the lack of self-sufficiency of contracting parties are not prominent in time-for-print contracts.[696]

Enlighted by some German scholars, the negotiability of the contract serves as a clear sign for the voluntariness and professionality of the data subject.[697] Merchandising contracts, albeit having models, are scrutinized, and specifically agreed upon by the data subject including the purpose, contents, duration, rights and obligations and sub-licensees or the conditions for selecting sub-licensees. In this wise, users' merchandising is in

694 The court does not consider that the age of 24 when she agreed to publish the nude photos, was too young to make a meaningful decision concerning her career choice and lifestyle. See OLG München, NJW-RR 1990, 999 - Wirtin.

695 The German court has addressed in the "stink fingers" case that the ruling might be different if the case concerns amateur models who lack enough experience. LG Frankfurt/Main, 30.05.2017 - 2-03 O 134/16 - Stinkefingers, para. 70 with further references.

696 Even the GDPR acknowledges this point as the prohibition of coupling tackling with power asymmetry is merely declarative while the duty to inform is absolute and rigorous.

697 Vgl. Albers/Veit, in *Brink/Wolff,* BeckOK Datenschutzrecht, Art. 6 Rn. 30.

general excluded from the exception because, despite it concern merchandising, the contract (the privacy policy) is usually drafted by the controller and the data subject cannot exert any influence on the text.[698] Moreover, it is possible that controllers would grant sub-licenses based on the blanket authorization. Thus, Art. 6 (1) (b) GDPR is only applicable in typical merchandising contracts between professional data subjects such as models, actors/actresses and agencies, advertisers, and manufacturers. It is further supported by the general rule in interpreting exceptions as to understand them narrowly.

(4) Well-balanced protection for both sides

Apart from providing a stable legal relationship for merchandising, well-balanced protection for all contractual parties facilitated by the application of Art. 6 (1) (b) GDPR is also undergirded by the unaffected application of national law in protecting personality interests of the person depicted (the data subject).[699] In other words, the German doctrines including the revocability of consent, the theory of purpose transfer in interpreting the contract, as well as the contractual rights and privileges of the person depicted are all applicable in assessing the validity of that contract.

As demonstrated in Part I Section 3.1.1 (2), the person depicted can revoke consent in a merchandising contract by proving a changed belief of merchandising. In addition, extraordinary opt-out rights of the person depicted, which are always included in merchandising contracts, can also lead to the termination of those contracts when a prescribed violation of the data subject's interests, rights and freedoms emerges. The data subject shall deploy these rights to terminate the legitimacy of data processing by the controller with an *ex nunc* effect. Consequently, the controller must stop data processing by taking down the advertising and delete the stored data.

Admittedly, the data subject does not have as much control over personal data under Art. 6 (1) (b) as consent in Art. 6 (1) (a) GDPR. However, it is in the interest of the data subject to recognize that the data processing is necessary for the performance of the contract. After all, the data subject seeks mainly (more) economic benefits. If he or she retains the right to

698 Such as the invitation emails and links sent by one's friends to invite the person to sign in the platform.

699 Schantz, in *Simitis, et al.,* Datenschutzrecht, Art. 6 Rn. 21.

terminate the contract at any time, very few agencies and advertisers would be willing to cooperate with the data subject. Even if some bold merchandisers exist, they will certainly pay significantly less remuneration to the data subject because of the higher risk they take. Moreover, by placing the integrity of inner beliefs at the heart of personality protection, the prohibition of assignment and the revocability of consent in merchandising scenarios strikes a fair balance between the core interests of one's personality. It is noteworthy that the untouchable human dignity and free development of personality speak for personal autonomy and the inalienability of dignity. Lastly, in case of doubt for the ambit of the data processing, the German doctrine of purpose transfer provides helpful concretization in applying the requirement of necessity. Though this concept should be interpreted autonomously at the EU level, the same origin, namely the principle of purpose limitation, and the same underlined rationale to protecting the interests of data subjects without undermining the effectiveness of their self-determination in concluding the contract both support the indirect application of the abundant German jurisprudence in interpreting and executing the EU provision. Against the merchandising background, if the means of exploitation of personal pictures are not specified in the contract – be they implicitly granted or licensed in gross – the lawful means should be the ones that are indispensable for realizing objectives outlined in the contract.

In this sense, time-for-print contracts can apply Art. 6 (1) (b) GDPR as the lawful ground for data processing as long as it is necessary to achieve the purpose of that contract. The nature of free negotiation of this kind of contracts and the professionality of both parties are strong reasons for invoking the exception for the teleological reduction. Thereby, similar results could be concluded from the application of the GDPR in the "*stink fingers*" case. The commercial exploitation of the personal data by the controller is lawful, but not the processing concerning the disgraceful presentation of the pictures.

A spin-off consequence of the recognition of merchandising contracts under the GDPR is that it paves the way for the recourse for material damages computed on the lost profits can be supported by the GDPR. Hopefully, it can remind people to start paying attention to the commercial value of data and gradually penetrate the users' merchandising.

### 3.3.2 Disadvantages and objections for this solution

#### (1) Borderless application of Art. 6 (1) (b) GDPR in sub-licensing situations

The verbatim reading of Art. 6 (1) (b) GDPR might lead to a borderless application, which would render the control of data subjects over personal data factually infeasible.

Common examples often emerge in the context of a data licensing agreement, in which the first data controller, normally a data broker, would transmit the personal data to as many controllers/sub-licensees as possible to get consideration. Thereby, the data subject's control over his or her personal data would be *de facto* deprived if the contract since the data licensing agreement is binding and thus the data subject cannot withdraw the consent; Moreover, by merely asking the first controller to take measures in a proportionate manner according to art. 17 (2) and 19 GDPR, the GDPR does not impose an absolute obligation on the first controller to notify the second and third controllers when the data subject claims rights at it. In this sense, the control of the data subject seems to stop at the first controller.[700] In addition, the obligations for providing information, no matter of the first or the second and third controllers, are limited in effectiveness as the binding nature of the contract would force the data subject to challenge the validity of the contractual obligation at first. Lastly, the omission of these obligations is hardly detrimental to the validity of the contract unless it can be proved that the data subject has exercised the right to informational self-determination in the opposite way because of a serious cognitive error.

Nevertheless, one may argue that Art. 6 (1) (b) GDPR is justified in deliberately not limiting the other party to the contract. Illustrated by the emergence and success of platforms, data subjects can use the one-stop service in platforms to complete numerous matters that previously needed to be done individually. For example, via Amazon, a consumer only signs a contract with the platform instead of signing contracts individually with the provider of the product, the courier company, etc., because the other controllers' legitimacy for processing personal data can be derived from the consumer's contract with the platform. Moreover, this interpretation would not compromise the enforcement of data subject's rights. As the concept of joint controllers has been broadly constructed by the CJEU

700 See *Sattler, in: Pertot, Rechte an Daten,* S. 69f.

since the *Fashion-ID* case, the platform can be held fully responsible according to Art. 82 (4) GDPR.[701] In this wise, it seems non- detrimental if data subjects sign the contract without reading it given some structural and cognitive problems.[702] However, this is the exact situation where data processing is accessory to the performance of the contract. Regardless, Art. 6 (1) (b) GDPR is applicable, and the prevailing opinion is what makes it possible for data subjects to be properly protected.

In summary, the concern about the borderless application of Art. 6 (1) (b) GDPR is well-founded. One can only contend that since the exception of its application is limited in the B2B context like the one in the *landlady* case, the negative consequences could be well maintained coupled with an intensified duty of information of the first controller as well as the second one. Given the self-sufficiency of the data subjects in the B2B context, the clearer the identity of the second controller is in the (context) of the contract, and the clearer the information the data subject has when making the decision, the more justified the second controller is to invoke Art. 6 (1) (b) GDPR. At least, the first controller must at first make some general references of the second and third controllers when it collects the data; when the first controller can identify the others, it should notify the data subject.[703]

(2) Under-protection for data subjects in B2C contexts

By distinguishing the B2C and B2B context and offering Art. 6 (1) (b) GDPR only in the B2C context might result in some under-protection issues for average internet users, i.e., ordinary data subjects. While it is admitted that the applicability of art. 6 (1) (b) GDPR in a B2C scenario may not be a good solution as many academics and EDPB have observed, the commercial value of their data would be acquired by controllers through consent without consideration. As *Langhanke* points out, by qualifying the privacy policy regarding data processing as consumer contracts, a review of the fairness of the content is brought to the fore.[704] For instance, the

701 CJEU, Fashion ID, C-40/17, para. 65-85.
702 *Thaler and Sunstein*, Nudge: improving decisions about health, wealth, and happiness, 19 es seq.
703 Schantz, in *Simitis, et al.*, Datenschutzrecht, Art. 6 Rn. 22.
704 Langhanke and Schmidt-Kessel, 4 Journal of European Consumer and Market Law 218 (2015) (220).

China's fastest-growing e-commerce platform, *Pingduoduo*, is embroiled in such a scandal. It encouraged users to keep inviting their friends to join *Pingduoduo* by promising monetary rewards, which could only be withdrawn when the amount reached 500 RMB. However, as the amount gets closer to 500 RMB, the reward for each invitation gets smaller and smaller, which makes it impossible for users to withdraw money *de facto*.[705] Thus, users stop sending invitations to their friends, but the commercial promotion of *Pingduoduo* is not retroactively invalidated. As a result, *Pingduoduo* gets viral in internet and data subjects get nothing.

Therefore, treating the relationship of merchandising as a synallagmatic contract, rather than a mere user's consent, allows the data subject to receive reasonable remuneration and introduces contractual rights common to merchandising contracts to fully protect the personality rights of the data subject. After all, allowing controllers to exploit the commercial value of data without consideration will lead to more exploitation.[706] Taken time-for-print contracts as examples, legal negation of the validity of such contracts due to power asymmetry and paternalistic protection for young models would not only seriously affect the informational self-determination of data subjects but also put the young models in a deadlock situation.[707] Therefore, the rightful solution that the German courts take is to assess the fairness of the reciprocal behavior between photographers and models, and thus draw boundaries for what authorization is necessary.

### (3) Art. 6 (1) (b) GDPR as a general clause for fair contracts

This solution is premised on an ideal B2B context where a certain degree of fairness (*qui dit contractuel dit juste*) is presumed.[708] Professional models

---

705 Sina finance, "在拼多多，一分钱难倒英雄汉"(In *Pingduoduo*, a hero is beaten by a penny)，at https://finance.sina.com.cn/tech/2021-06-30/doc-ikqciyzk2719869.shtml. This article articulates the logic under the promoting game set up by *Pingduoduo*. One can at first easily get bonus, but the fission form increases. Since there is always "one penny short of victory (to withdraw deposit)", one has to invite more and more people into this "infinite loop" game.

706 Bietti, 40 Pace law review 310 (2020) (378).

707 Vgl. *Ohly*, "Volenti non fit iniuria": die Einwilligung im Privatrecht, S. 79f, 160. It argues that the anytime revocable consent lay restrictions on both sides of the contract.

708 Cite from *Beale, in: de Elizalde, Uniform Rules for European Contract Law?: A Critical Assessment*, 9 (23); Originally in, *Fouillée,* La science sociale contemporaine, 410.

care about their images and are proactive in asking for information, negotiating the terms and conditions of contract, fighting for benefits, and avoiding risks. Furthermore, models as "professional players" constantly enter into the same type of contracts. They understand and have fully weighed the benefits and risks. However, as a spectrum of the self-sufficiency of data subjects in merchandising scenarios shows (Part III Section 3.2.1), the threshold for professionality of models is elusive. Length of time in practice, income and education are all difficult to use as satisfactory criteria, or they can all be used as criteria. Especially when internet influencers are increasingly coming into the playground, the line between the B2B and B2C contexts is blurring. The BGH considered Cathy Hummels who has more than 600,000 followers as entrepreneur (*Unternehmer*), but how about micro-influencers who have 10,000 followers or less, are they entrepreneurs or average internet users?

Given this, the second condition may be more decisive in enforcing this solution, namely, the negotiability of the contract. In this wise, this solution resembles the minor opinion in literature to some extent as Art. 6 (1) (b) GDPR almost becomes a general clause for fair contracts. Consequently, it suffers similar critics that the negotiability of contract can be easily circumvented by powerful controllers if they possess *de facto* dominant position, such as the scenario between "idol trainees" and powerful agencies.

Establishing a special contract type for merchandising contracts in the B2B context would address this concern. As data subjects who voluntarily and prudently choose merchandising as a career are well respected and protected under the German legal regime, a muster of merchandising contracts under German law taking the contractual right into account is expected to indicate the fairness and necessary protection for data subjects.[709] However, there is hardly a legal basis for this suggestion. Art. 6 (1) (b) GDPR, unlike other lawful grounds, does not offer discretion for the Member States.

709 *Golz and Gössling,* IPRB, 2018, 68 (72); *Beale, in: de Elizalde, Uniform Rules for European Contract Law?: A Critical Assessment,* 9 (31). Instead of focusing on merchandising, the author addresses that harmonization of contract law is more promising in B2B contexts.

### 3.4 Summary

By applying Art. 6 (1) (b) GDPR as its literal reading to merchandising contracts in the B2B context, merchandisers can rely on valid contracts with professional models to process their personal data and even grant sub-licenses for purposes of merchandising without fearing the anytime revocable consent prescribed in Art. 6 (1) (a) and 7 (3) GDPR. However, there are two detrimental objections to this approach. For one, it can be easily stretched to a general clause for fair contracts as there is hardly a legal basis to limit this approach in merchandising contracts, not to mention this type of contracts is formulated under national law. For two, there is no hard line between the B2B and B2C contexts. As KOL (Key Opinion Leaders) in social media increasingly become a profitable career, the line is more blurring.

Admittedly, the restrictive reading of the ambit of Art. 6 (1) (b) GDPR according to the mainstream opinion would stifle the private autonomy in merchandising. Moreover, even though this solution does not directly address the issue of under-protection for celebrities in unauthorized merchandising cases, the legal recognition of merchandising contracts under the GDPR can support the recourse for the lost profits by celebrities in unlawful data processing scenarios. However, this solution overlooks the users' merchandising in the B2C scenario. If contracts in this scenario are limited to merchandising and does not include direct-marketing, profiling, etc., why should there be reasons to hinder data subjects conclude a binding merchandising contract according to their will? After all, professionalism is a status that acquires by learning. The limitation of the B2B situation would thus be too conservative considering the advent of "digital natives"[710]

710 *Prensky*, On the horizon, 2001, 1. The "digital natives" refer to the generation that grew up in the Internet era; correspondingly, "digital immigrants" generally refer to those who gradually learn and use the Internet in their adulthood.

## 4. The proposal for a two-tier interpretation of consent

### 4.1 The two-tier interpretation of consent

#### 4.1.1 Introduction of this solution

##### (1) The content of this proposal

*Sattler* proposes a two-tier interpretation of consent in Art. 6 (1) (a) GDPR.[711] Consent defined in the GDPR has two forms. One is simple and unilateral and can legitimize data processing conducted by the controller according to Art. 6 (1) (a) GDPR. This consent is anytime revocable pursuant to Art. 7 (3) GDPR. The other one is a legal act that is given to establish a legal relationship, which according to Art. 6 (1) (a) shall also provide a lawful ground for data processing. However, the revocability of this consent is not subject to Art. 7 (3) GDPR but to national law regarding legal acts. In this context, the anytime revocability in Art. 7 (3) GDPR is not a mandatory condition for consent anymore.[712] Rather, data subjects can choose between anytime revocable consent and binding consent to dispose of their control over personal data according to their genuine wishes. In doing so, consent given by models in merchandising agreements is allowed to be binding but subject to revocability with due cause according to German law.

Art. 4 (11) GDPR defining consent does not require the anytime revocability. Instead, it defines consent merely as "*any freely given, specific, informed and unambiguous indication of the data subject's wishes*". According to this definition, wiggle room for the two-tier interpretation is presented. All steps in the *ladder of permissions* developed by *Ohly* can be subsumed within the consent since they meet the conditions prescribed in Art. 4 (11) GDPR. In other words, consent, following the definition in the GDPR, could be simple, unliteral consent that is readily revocable, a binding contractual permission, or even an assignment of right if it does not contradict to other provisions of the GDPR.[713] Thus, in *Sattler's* words,

---

711 See *Sattler*, JZ, 2017, 1036 (1043f); *Sattler, in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance – Contract Law 2.0?*, 225 (243 et seq.); In this direction, see *Sattler*, in: *Bakhoum, Personal Data in Competition, Consumer Protection and IP Law - Towards a Holistic Approach?* , 27 (43 et seq.).

712 *Sattler*, JZ, 2017, 1036 (1044).

713 Ibid., 1043.

Art. 4 (11) GDPR "provides the minimum standard" for consent – the so-called "safety net" (*Sicherheitsnetz*). Consent below the net, which is, for instance, presented in a pre-ticked box, or under huge pressure, is not valid self-determination under the GDPR, whereas consent above this net can have multiple variants.[714]

The dual objectives pursued by the GDPR speak stronger for this interpretation. While the protection of natural persons with regard to the processing of personal data is guaranteed by fundamental rights and freedoms (Art. 1 (2) GDPR), it shall not be the reason to restrict or prohibit the free movement of personal data within the Union (Art. 1 (3) GDPR). Against this backdrop, the freedom of contract as a fundamental freedom in the Union shall not only play a role within the framework of balancing interests regarding the protection, but shall also be considered as an indispensable tool to facilitate the free movement of personal data.[715]

To strike a fair balance of the fundamental rights, namely between the right to the protection of personal data (Art. 8 of the Charter), and private autonomy (Art. 1 of the Charter) and the freedoms to conduct business (Art. 16 of the Charter) in light of the dual objectives of the GDPR, a teleological reduction of the applicable scope of Art. 7 (3) GDPR is argued to facilitate the two-tier interpretation for consent.[716] Anytime revocability is confined within the simple and unilateral consent residing on the lowest layer in the *ladder of permissions*. Thus, it is the least binding disposition for the data subject, which, on the flip side, presents the disposition that best reflects the strong control of the data subject over personal data. In consent above this layer, such as the contractual permission, Art. 7 (3) GDPR is inapplicable. Hence, Art. 7 (3) GDPR is principally optional according to data subjects' wishes.[717]

(2) Its enforcement

According to the two-tier interpretation of consent, Art. 6 (1) (a) GDPR can legitimize data processing of the data controller by following the true will of the data subject, be it a simple consent that reflects a strong will

714 Ibid.
715 Ibid., 1044; CJEU, AGET Iraklis, C-201/15, para. 66 f.; CJEU, Sky Austria, C-283/11, para. 42 ff.
716 *Sattler*, JZ, 2017, 1036 (1046).
717 Ibid., 1044.

to control, or an expression of will that creates an obligation. Art. 6 (1) (b) GDPR is still limited to accessory data processing to the contract, such as delivery and identity verification. While Art. 6 (1) (a) GDPR can be applicable in different situations, in some of which consent is freely revocable and in others not. However, the bottom line is that the consent under the GDPR must be an informed and voluntary indication of a data subject. In this sense, a pre-ticked box or a deceptive privacy policy leads to invalid consent.

Against this backdrop, consent gains flexibility, and the autonomy of data subjects is thus respected. After all, the more stringent the conditions for validity are, the more likely that the legal meaning of the consent deviates from the true will of the data subject.[718] Moreover, it would not undermine the high-level protection for data subjects provided by the GDPR by rendering consent binding in some scenarios. On the one hand, the obligation of information obliges data controllers to inform data subjects about the nature, ambit, and consequences of the consent they are giving. In the absence of clear notification of the binding effect of consent, consent should fall on the "safety net" and be deemed as an anytime revocable consent in the light of the principle of accountability.

On the other hand, the choice of the data subject – to waive Art. 7 (3) GDPR does not lead to his or her permanent subjection to data processing by the data controller. Under the GDPR, the principles of purpose limitation and data minimization confines the content, purpose, means and duration of the processing. Furthermore, the controller must stop processing and delete data when specified purpose(s) are fulfilled. Extraordinary opt-out rights are also not seldom in European contract law in open-ended contracts signed by consumers.[719] At least in Germany, the uneven protection for personality in merchandising contracts disclosed in Part I not only demands the revocability of consent but also regards the extraordinary opt-out right of the person depicted mandatory.

718 *Krönke*, Der Staat, 2016, 319 (326); Cf. *Bix, in: Miller and Wertheimer, The Ethics of Consent: Theory and Practice*, , 252 (252, 256).

719 *Gareth and Peter*, in: *Zweigert and Drobnig, International Encyclopedia of Comparative Law Online*, Vol. VII, § 15 no 30-57.

(3) Argumentation based on the (inter-)systematic interpretation

The Directive on Certain Aspects concerning Contracts for the Supply of Digital Content and Digital Services (DCSD), which had recognized the permission to access to personal data as a counter-performance for the supply of digital content/services in its draft but has deleted that expression in its final version, presents an intensive tension to the GDPR when "the consumer provides or undertakes to provide personal data to the trader" for the supply of digital content/services (Art. 3 (1) DCSD).[720] As the second sentence of Art. 3 (1) DCSD excludes its applicable scope in data processing that is exclusively to supply the digital content/service, Art. 6 (1) (b) GDPR shall not serve as the lawful ground for this situation. Consequently, since the GDPR prevails in any case (Art. 3 (8) and Art. 16 (2) DCSD), consent for data processing given by consumers for receiving the digital content/service is anytime revocable according to Art. 7 (3) GDPR if consent is understood narrowly.[721]

This *status quo* is not beneficial for consumers. Firstly, although the contract between the trader and the consumer who provides personal data subject is concluded and effective but hardly enforceable; though it has been argued that a special opt-out right for consumers is not quite unusual in the EU,[722] a right to withdraw at any time without reason and for an unlimited period of time will dissuade many traders who long for a binding and enforceable legal status.[723] Moreover, the unprotected status for traders who supply digital contents/services would encourage them to exploit to collect and use the data as quickly as possible to recover costs/profit before consumers terminates the contract.[724] Considering the obligations of traders after the termination of such contracts (Art. 16 (3) DSCD), data processing that particularly raises GDPR concerns, such as the inte-

720 Recitals 13, 14, 37, 42, and 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). 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.; Recital 24 of Directive (EU) 2019/770.

721 *Sattler, in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance – Contract Law 2.0?*, 225 (232).

722 Langhanke and Schmidt-Kessel, 4 Journal of European Consumer and Market Law 218 (2015) (222).

723 In contrast with natural obligation that often takes places in business regarding lottery and gambling. See *Schulze*, Die Naturalobligation, S. 6.

724 Vgl. *Sattler, in: Pertot, Rechte an Daten*, 49 (80).

gration and analysis of consumers' personal data to generate new data (profiling, personality analysis, etc.) seem to be inevitable.[725] Furthermore, the right to receive a proportionate reduction in the price when the digital content/service is defective is only applicable for consumers who provide money against the supply of the digital content/service according to Art. 14 (4) DCSD. If the "counter-performance" is personal data, the consumer has only the remedy of termination according to Art. 7 (3) GDPR.[726] Lastly, as the consequence of the termination of contracts has been left to national law according to recital 40 of the DCSD, a forum-shopping for traders due to varied judgments in national courts is likely to take place.[727]

Therefore, if the two-tier interpretation for consent is adopted to enable a binding relationship between the trader who supply the digital content/service and the consumer who provide personal data as consideration, the strong consumer protection stipulated in the DCSD can apply indiscriminately in scenarios where "counter-performance" is personal data provided by consumers to solve the discrepancy brought up by the different treatments between the "counter-performance" in manners of money and data.[728]

(4) Questioning the unlimited data paternalism in private sector

Moreover, *Sattler* focuses on the lack of sufficient justification regarding the omnibus approach taken by the GDPR of treating the public and

725 Art. 16 (3) DSCD allow traders to continue their data processing when the condition prescribed in paragraph (a) (b) (c) and (d) is met alternatively. For instance, the trader can still process data that has been aggregated with other data by the trader and cannot be disaggregated or only with disproportionate efforts (Art. 16 (3) (c) DSCD).

726 Admittedly, the threshold for exercising that right appears to be lower than in the case where the consideration is monetary. As Art. 14 (6) DCSD requires that consumers can only terminate the contract "if the lack of conformity is not minor", and Art. 7 (3) GDPR requires the withdrawal to be free, consumers can thus terminate the contract concerning personal data based on minor inconformity. See *Sattler, in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance – Contract Law 2.0?*, 225 (232).

727 Vgl. Ibid., 237-238.

728 Also addressed by *Sattler*, it is indeed difficult for courts to calculate the amount compensation because the value of personal data is unknown and probably trivial for individual data. See ibid., 232.

private sector alike.[729] For public authorities, all is prohibited unless permitted by law, while for private parties all is permitted unless prohibited by law.[730] The informational self-determination emerged exclusively from the confrontation between individual rights and public power,[731] which needs to be adjusted when it is applied between civil subjects.[732] The justification for data paternalism reflected in the GDPR is more warranted and appreciated when more serious asymmetries of information and power exist between data controllers and data subjects,[733] and it is also acknowledgeable that some private controllers who have massive amounts of data and powerful data processing technologies have already become comparable to public power.[734] This condition is also reflected from the perspective of the EU data protection law. The e-Privacy Directive merely foresaw the possibility to withdraw consent for specific personal data such as location data,[735] as it takes advantages of data subjects due to their bounded recognition to force them to conclude a contract of personal filing when they just want to chat with friends. Moreover, as the BVerfG keenly observed, the more powerful the data controller is and the more control it has that rivals public power, the more justified is the application of the GDPR to it.[736] In the other way round, it is hence questionable whether this direct vertical application of the data paternalism – "the encroachment on the scope of protection of the data subject's general freedom of action" at the cost of "the data controller's freedom of occupation" in private sector – is justified.[737]

729 See *Sattler, in: Bakhoum, Personal Data in Competition, Consumer Protection and IP Law - Towards a Holistic Approach?* , 27 (34 et seq.); *Sattler,* JZ, 2017, 1036 (1042).
730 *Sattler, in: Bakhoum, Personal Data in Competition, Consumer Protection and IP Law - Towards a Holistic Approach?* , 27 (36).
731 BVerfG, NJW 1984, 419 - Volkszählung.
732 For instance,BGH, NJW 2009, 2888 - Spickmich, Rn. 31f.; *Di Fabio,* Safeguarding fundamental rights in digital systems, S. 90.
733 *Hermstrüwer,* Informationelle Selbstgefährdung, S. 227 ff.
734 *Bull,* Sinn und Unsinn des Datenschutzes, S. 6; Bundestag, Grundfragen des Datenschutzes, Drs. VI/3826 S. 138
735 See Article 6.3 and 9.3-4 of the 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 (Directive on privacy and electronic communications) – the e-Privacy Directive.
736 BVerfG, GRUR 2020, 74 - Recht auf Vergessen I, para. 88; BVerfG, NJW 2011, 1201 - Fraport, para. 60.
737 *Sattler,* JZ, 2017, 1036 (1042).

It questions (*hinterfragt*) the overly extensive application of the paternalistic measures in the GDPR.[738] Without going too deeper and further from the topic of merchandising in this dissertation, the observation revolves around the German experience in regulating the commercialization of personal images. As briefly introduced in Part III Sections 3.1.3 and 3.2.2, one of the main arguments for data paternalism is ill-grounded in merchandising as the models with expertise and equal status voluntarily and deliberately choose a lifestyle that is consistent with their long-term preference. Thus, the financial disadvantages faced by young models are frivolous in warranting a vigorous limitation on the effectiveness of consent. Moreover, the soft-licensing model in Germany also guarantees the inseparability of personal data from the data subject, which reflects the imperative of untouchable human dignity and the principle of freedom. Additionally, protection stemming from German jurisprudence and practice, which also acquires acknowledgment in law, is more suitable and useful for models in merchandising to protect their interests compared to the protective measures in the GDPR. Therefore, the fundamental differences between merchandising and data processing concerned by the GDPR in terms of the knowledge, professionality and power of data subjects, the means and purpose of the processing as well as the overall risks for data subjects speak strongly for cautious application of the paternalistic provisions in the GDPR in merchandising including Art. 7 (3) GDPR.

(5) Universally various connotations of consent

The counterargument that *the ladder of permissions* invoked by *Sattler* is a unique German concept that is inapplicable for interpreting an EU concept, is untenable.

Although *the ladder of permissions* is a doctrinal development under German law, its philosophical and theoretical root is in the Roman maxim *volenti non fit iniuria* (loosely translated as no wrong flows from the harm when the person harmed has consented to[739]). Not only *Kant*, but

738 See *Sattler, in: Bakhoum, Personal Data in Competition, Consumer Protection and IP Law - Towards a Holistic Approach?* , 27 (40); *Sattler*, JZ, 2017, 1036 (1045).

739 There are two ways to understand this maxim. One is to regard *volenti non fit iniuria* as a legal fiction that since a person will not harm him- or herself, what that person has consented to is not an actual harm for him- or herself. The other is to negate the unlawfulness flowing from the harm since the person harmed has accepted it. See Feinberg, 1 Canadian Journal of Philosophy 105

also *Mill* have undergirded their philosophy by this universal principle of fairness acclaiming personal autonomy and its associating requirement of self-responsibility.[740] In light of these ethical and legal ideas, consent with multiplicity originated in Greek and Roman culture soon gains wide consensus in the Western world.[741] Very close to the meaning of *the ladder of permissions*, one may use consent to create a right or entitlement or give permission or assume obligation.[742]

Gradually, consent, as a manifestation of voluntary choice, is considered the essence of contract law,[743] and the withdrawal of consent is subject to restrictions given the reasonable reliance of the counterparty triggered by the obtained consent.[744] In other words, the revocability of consent is an exception from the general of *pacta sunt servanda*. Nevertheless, the anytime revocable consent is common in medical and sexual scenarios.[745] There are several strict conditions for a valid consent underlined the principles of autonomy and self-responsibility. Being aware of the content of the consent, free to decide and able to hold independent responsibility for the consequences are the three major conditions.[746] In theory, the violation of any of these conditions would result in invalid consent, but reality is not a black-and-white world. Almost all three conditions are on a spectrum, with an almost unreachable complete satisfaction at one end

---

(1971) (107). The latter is more convincing and has been adopted here because the value judgment of denying illegality of the harm will not affect the legality of other people's justifiable defense behavior.

740 *Ohly*, "Volenti non fit iniuria": die Einwilligung im Privatrecht, 63ff.

741 *Johnston*, in: *Miller and Wertheimer*, *The Ethics of Consent*, 26 (35 et seq.).

742 *Kleinig*, in: *Miller and Wertheimer*, *The Ethics of Consent*, 4 (12).

743 Cf. *Bix*, *in: Miller and Wertheimer*, *The Ethics of Consent: Theory and Practice*, 252 (252, 257); If a party had "assumed and faithfully promised" (*assumpsit et fideliter promisit)*, then he or she has the obligation to implement order issued by the court to the enforce the contract. See *Ibbetson*, A historical introduction to the law of obligations, 131.

744 *Kleinig, in: Miller and Wertheimer*, *The Ethics of Consent*, 4 (10); Steyn, 113 The Law Quarterly Review 433 (1997) (433).

745 *Kleinig, in: Miller and Wertheimer*, *The Ethics of Consent*, 4 (10).

746 See *Beauchamp*, in: *Miller and Wertheimer*, *The Ethics of Consent*, 56 (66 et seq.). It focuses on the autonomy of consent and dissects it into intentionality, understanding and voluntariness. However, it is considered that intentionality can be reflected by understanding and voluntariness. Moreover, the self-responsibility delineates the boundaries of what can be covered by consent and what cannot. If the given person cannot take responsibility for what he or she consents to, the person shall not be allowed to give that consent. Vgl. *Mill*, On Liberty, 41; *Ohly*, "Volenti non fit iniuria": die Einwilligung im Privatrecht, 77f.

and a complete non-fulfillment at the other.[747] For instance, in medical scenarios, almost all patients do not fully understand the medical approach and accompanying risks despite the physician's lecture.[748] The financial pressure "forces" models who are new to the business to choose between not having the possibility to be photographed at all and letting high-level photographers take pictures for free. A minor shall only be held responsible for things that are at his level of perception.

Against this backdrop, it needs to make necessary concessions to the needs of protection for minors, disadvantaged party due to knowledge and negotiation power by recognizing the (anytime) revocability of consent. Thus, a broad understanding of the nature, type and consequences of consent is a legal fact that is widely accepted in the Western world. The foundation of the interpretation forwarded by German scholars is not objectionable because it is not imposing a German concept on the autonomous legal concept of the EU. In essence, the solution proposed by *Sattler* seeks to restore consent to its original nature upon certain conditions by proposing a teleological reduction of the limitation of consent added by the GDPR.

### 4.1.2 Counterarguments to this proposal

#### (1) The opinions of authorities as well as the (intra-)systematic interpretation

Above all, rendering Art. 7 (3) GDPR optional seems to contradict the historical interpretation based on the official documents in drafting the GDPR and the EDPB's understanding of consent.[749] The WP29 has advocated the "possibility to withdraw consent at any time" since the era

747 *Beauchamp, in: Miller and Wertheimer, The Ethics of Consent*, 56 (71-72). The condition of self-responsibility seems not a matter of degree as one can or cannot hold responsible, it is intricated in data processing situation since personal data are entangled and they may also contain some social value. See Part V Section 4.3.

748 *Candilis and Lidz*, in: *Miller and Wertheimer, The Ethics of Consent*, 330.

749 *Funke*, Dogmatik und Voraussetzungen der datenschutzrechtlichen Einwilligung im Zivilrecht, S. 322. It has addressed that the exception for the right of revocation, which in the end always makes the right of revocation a question of balance, was rightly deleted in the Council draft and in return supplemented by more specific exceptions,

of Directive 95/46/EC.[750] Subsequently, the free revocability of consent implied by Directive 95/46/EC has been made clear in the e-Privacy Directive. Reading from the consistent opinions issued by the WP29 and the successor EPDB, the revocability of consent serves two functions.[751] For one, it is used as an indicator for voluntariness as the withdrawal of consent shall not lead to any detrimental effect on the data subject. Moreover, the free revocability is to enhance the control of data subjects by enabling data subjects to call off data processing whenever they wish. In this wise, the limited application of anytime revocable consent in the e-Privacy Directive should be considered as an incubator for the general application of Art. 7 (3) GDPR.[752] Consequently, this unique nature of consent plays a prominent role in the GDPR is par for the course.[753]

Secondly, the anytime revocability in Art. 7 (3) GDPR as one of the rigorous conditions for valid consent is devised to guarantee high-level protection for data subjects by putting the right to determine the legality of data processing in the hands of data subjects. Based on reflections on the opinions and guidelines drafted by the authorities at the EU level, the anytime revocability of consent is indispensable. According to the EDPB, the reason why Art. 21 (1) only mentions Art. 6 (1) (e) and (f) GDPR and does not discuss consent is that withdrawal of consent has the same effect as the right to object.[754] The EDPB further contends that Art. 7 GDPR "sets out these additional conditions for valid consent", and "if the withdrawal right does not meet the GDPR requirements, then the consent mechanism of the controller does not comply with the GDPR".[755] In this wise, it seems that one cannot change the mandatory nature of conditions prescribed in Art. 7 GDPR because the GDPR does not intend to build a higher yet optional standard for consent. Therefore, many scholars also

750 WP29, Opinion 15/2011 on the definition of consent, WP187, 9.
751 Ibid., 9; EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, para. 10 and 46 et seq; WP29, Working Document on the processing of personal data relating to health in electronic health records (EHR), WP 131, 8 and 9; WP29, Opinion 8/2001 on the processing of personal data in the employment context, WP48, 3.
752 The WP 29 has suggested including "an express clause setting up the right of individuals to withdraw their consent". See WP29, Opinion 15/2011 on the definition of consent, WP187, 37.
753 EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, para. 112.
754 Ibid., para. 164.
755 Ibid., para. 103 and 116.

consider Art. 7 (3) GDPR mandatory.[756] While some scholars acknowledge the incompatibility between anytime revocability of one party and the core rule of *pacta sunt servanda* in contract law, they contend for an extremely strict and exceptional exclusion of this mandatory provision.[757] However, since their arguments primary rely on German law instead of a normative start point in the EU data protection law, the advocation for some exceptions for the anytime revocability of consent seems problematic under the GDPR.[758] Against this backdrop, the proposal of *Sattler* is warranted as its starting point is the definition of consent in Art. 4 (11) GDPR instead of national law.[759]

However, this proposal seems to contradict the intra-systematic interpretation for consent due to its conditions for validity in Art. 7 GDPR. Several counterarguments are advanced here as follows.

First, Art. 7 (1) - (4) GDPR imposes different requirements for the validity of consent, paragraph (1) demanding the active duty of proof on the part of the controller, paragraph (2) calling for clarity and independence of the statement of consent, paragraph (3) requiring the revocability of consent, and (4) providing for a prohibition on binding. It lacks sufficient evidence to claim that the paragraphs under the same provision are point-

---

756 *Voigt*, Die datenschutzrechtliche Einwilligung, S. 156; *Funke*, Dogmatik und Voraussetzungen der datenschutzrechtlichen Einwilligung im Zivilrecht, S. 322-323; *Hacker*, ZfPW, 2019, 148 (170); Stemmer, in *Brink/Wolff*, BeckOK Datenschutzrecht, Art. 7 Rn. 90; Ingold, in *Sydow*, DSGVO: Handkommentar, Art. 7 Rn. 46; Buchner/Kühling, in *Kühling/Buchner*, DSGVO/BDSG, Art. 7 Rn. 39 and 39a; Heckmann/Paschke, in *Ehmann and Selmayr*, DS-GVO, Art. 7 Rn. 93; Schantz, in *Schantz and Wolff*, Das neue Datenschutzrecht: Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis, Art. 7 Rn. 532; Langhanke and Schmidt-Kessel, 4 Journal of European Consumer and Market Law 218 (2015) (220 f.); *Metzger*, AcP, 2016, 817 (825); *Spelge*, DuD, 2016, 775 (781); *Laue, et al.*, Das neue Datenschutzrecht in der betrieblichen Praxis, § 2 Rn. 14; Däubler, in *Däubler, Wedde, Weichert and Sommer*, EU-Datenschutz-Grundverordnung und BDSG-neu : Kompaktkommentar, Art. 7 Rn. 50; *Tinnefeld and Conrad*, ZD, 2018, 391 (396).

757 Klement, in *Simitis, et al.*, Datenschutzrecht, Art. 7 Rn. 92; Schulz, in *Gola*, DSGVO, Art. 7 Rn. 57; *Specht*, JZ, 2017, 763 (769); Ronellenfitsch, Siebenundvierzigster Tätigkeitsbericht zum Datenschutz und Erster Bericht zur Informationsfreiheit, 2018, § 4.9.1.

758 For instance, scholars draw the normative grounds on the requirement of good faith (*das Gebot von Treu und Glauben*) in § 242 BGB, while the report of the Hessen Authority relies on the judgment of the German court and probably the balancing of interests according to § 241 (2) BGB.

759 In the direction, see *Funke*, Dogmatik und Voraussetzungen der datenschutzrechtlichen Einwilligung im Zivilrecht, S. 323.

ed to different types of consent (i.e., one for simple consent), and the other three for all types of consent. Secondly, the third sentence of Art. 7 (3) GDPR requires that the right to withdrawal at any time must be informed to the data subject before he or she gives consent. This indicates the revocability of consent is not an active choice of the data subject but an obligation that the controller is required by law to fulfill when it invokes consent as the lawful ground.[760] Thus, it would be a violation of Art. 7 (3) GDPR if the controller informs the data subject that the lawful ground is consent on the one hand and claims that it is irrevocable on the other hand. Thirdly, the teleological reduction of Art. 7 (3) GDPR is inconsistent with the data controller's duty to inform because Art. 13 (2) (c) GDPR requires the controller to inform the right to withdrawal at any time without exceptions. Moreover, from the perspective that the right to withdrawal belongs to the data subject's rights,[761] there are more reasons for its non-waivable nature as all data subject's rights are not optional.

(2) Challenges to its practicability

More importantly, leaving aside whether this two-tier interpretation holds up under the GDPR, it is doubtful that it helps controllers in practice. Considering the higher-tier of consent is a significant deviation from the general understanding of consent under the GDPR (based on the teleological reduction), and presents a binding effect on the data subject him- or herself, the examination of the fulfillment of the controller's duty to inform can become very strict. Taking the *company advertising* case as an example, if the controller unintentionally obscures the revocability of consent, and the data subject has been misguided by the equivocal declaration, the controller must bear the consequence that no invalid consent has been given in any sense (see Part II Section 4.2.2). Whether the controller wants to use the low-tier or high-tier consent, the data subject is likely to be misled into influencing his or her decision. More importantly, as the

760 Taeger, in *Taeger, et al.*, DSGVO - BDSG - TTDSG, Art. 7 Rn. 84.

761 Many scholars consider the revocability of consent in Art. 7 (3) GDPR an embodiment of data subject's rights in light of the right to the protection of personal data anchored in Art. 8 (1) of the Charter. See *Liedke*, Die Einwilligung im Datenschutzrecht, S. 29f.; Frenzel, in *Paal and Pauly*, DS-GVO BDSG, Art. 7 Rn. 16; Heckmann/Paschke, in *Ehmann and Selmayr*, DS-GVO, Art. 7 Rn. 86; Klement, in *Simitis, et al.*, Datenschutzrecht, Art. 7 Rn. 86; Also *Sattler*, JZ, 2017, 1036 (1004).

burden of proof is on the controller, it is difficult for the controller to prove what the data subject had in mind.

Lastly, the applicable scope of the two-tier interpretation of consent seems to be omitted in the scholarly writings. Since the proposal originated as an interrogation of the GDPR's paternalistic protection, it seems fair to assume that it implicitly applies on the premise that data subjects must be fully aware of the implications of the higher-level consent and voluntarily bound by it. However, without a clear sign as the B2B scenario would present, the cost to examine the knowledge of the data subject and to evaluate his or her voluntariness could be unbearably high.[762] Obviously, this cost would be borne by the controller based on the principle of accountability and thus a strong dissuasion for controllers to pursue the higher-level consent.

## 4.2 Conclusions

It can be distilled that the strongest arguments of the two-tier interpretation of consent under the GDPR are the omission of revocability of consent in its definition and the boundaries of data paternalism, while its weakest position is the intra-systematic interpretation and the opinions of the authorities. Moreover, the cost for compliance and the high possibility of incompliance would seriously discourage controllers from using this method, although this explanation has in their favor. It is conceivable that controllers would still stick to the anytime revocable consent and keep in developing more attractive digital services.

Nevertheless, this proposal offers an innovative perspective to conceptualize consent. In light of *the ladder of permissions*, the anytime revocability of consent is a tool to extend the disposability of rights holders under data paternalism. Otherwise, one could only choose from the two alternatives, one is the absolute maxim of *volenti non fit iniuria* at the cost of not being able to protect the weak, and the other is a complete disregard of the

762 According to some scholars, this is one of the economic reasons for adopting paternalistic laws. See Feinberg, 1 Canadian Journal of Philosophy 105 (1971) (119); Kronman, 92 The Yale Law Journal 763 (1983) (766 et seq.). Likely, it is also one of the arguments advanced by the EDPB in excluding the application of Art. 6 (1) (b) GDPR in the business model of "data against services" (see above Section 4.1.2). However, this argument would be problematic when the cost for examination is taken by the counterparty/data controllers instead of courts.

autonomy of data subjects. Thus, the GDPR does not completely deny data subjects the right to dispose of their data, but limits it to a certain extent for the reason of protecting the data subjects themselves. This motivates one to consider whether this restriction is not necessary when the data subject is capable of protecting himself/herself. In this sense, the proposal offers a liberal, ever-changing solution as data subjects mature.

## *5. The comparison of the solutions and the result*

### 5.1 Unsuitable solutions 1 and 2

By continuing the German regulation of merchandising, data subjects can obtain compensation for material damage caused by illegal merchandising and establish relatively stable cooperation with merchandisers under the legal protection catered to their practical needs. In addition, it offers future-oriented protection for data subjects in the increasingly popular users' merchandising scenarios because it is likely that as web users become more familiar with this pure merchandising (which focuses only on user recommendations instead of profiling), data subjects will no longer be disgusted or fearful of this kind of promotion using their likenesses but rather want to receive reasonable remuneration for such exploitation of their likenesses.

However, the legal basis of this solution is under severe objections from both theoretical and practical perspectives. Interpreting Art. 85 (1) GDPR as a mandate for the Member States to legislate national law to reconcile data protection and freedom of expression in purely commercial activities would result in a complete hollowing out of the GDPR's effect as a directly applicable EU Regulation. Moreover, even if Art. 85 (1) GDPR could be interpreted as a stand-alone opening clause, the significantly larger (material and territorial) applicable scope of the GDPR would lead to substantial complexity and uncertainty in legal application in Germany. The production chain of merchandising would be assessed separately. Publication and dissemination would be under the KUG, while other processing including recording, editing, transmitting, transferring, storing, and deleting under the GDPR. It would amount to an unbearable burden for merchandisers, data subjects, and courts.

Apart from the flaws in the legal basis, some advantages of this solution can also be realized without the overly stretched interpretation of Art. 85 (1) GDPR. For instance, models can claim the restitution for fictive license

fees based on the law of unjust enrichment in Germany. The binding relationship between models and merchandisers can also be facilitated by interpreting some provisions of the GDPR in a minimal way instead of limiting the applicable scope of the GDPR in general. In a nutshell, the first solution that advocates the direct application of the KUG in merchandising has obvious advantages but is largely unfeasible.

Although the GDPR does not prohibit Art. 6 (1) (f) GDPR to be applied in a contractual relationship, and the balance of interests might be in favor of the controller taking its reasonable reliance deriving from the merchandising contract into account, the solution 2 is unsuitable for unlocking the deadlock between the data subject and the controller in an authorized merchandising scenario in both theoretical and practical terms. It can provide a relatively stable position for the merchandiser premised on a valid merchandising contract, but it is only in theory.

Above all, as the final decision on the weighing of interests is in the hands of courts and not the data controller, and much less the data subject, this solution not only distorts the role of the data subject by mistakenly treating him or her as the person being decided, who is the decider for merchandising, but also ignores the triumph of individual autonomy over the paternalistic law in regulating merchandising. Moreover, the extensive use of Art. 6 (1) (f) GDPR as a "safe harbor" for merchandisers under the GDPR contradicts the function and purpose of general clauses.

In practice, this is not an optimal scenario for data controllers either. Since Art. 6 (1) (f) GDPR does not require the data subject's consent or even his or her knowledge, the compliance requirements for the controller will be relatively high. Moreover, the right to restriction can hold the processing in suspension and force the controller to take down the advertainments at any time as the balancing test puts too much uncertainty in verifying the lawfulness of merchandising. Thus, the controller would have to run its main business in a consistent and great uncertainty. At the same time, merchandising contracts are always essential to prove that the interests pursued by the controller outweigh the rights and freedoms of the data subject due to the commercial nature of merchandising. Therefore, merchandisers have nothing to gain from this solution except for the additional compliance requirements and uncertainty.

In summary, as this solution essentially puts the informational self-determination under a cloak of heteronomy simply for compliance reasons, it is more like a suboptimal solution.

## 5.2 The comparison between solution 3 and 4

Solutions 3 and 4, despite their different legal bases, share many commonalities. Both expect to find a solution to the incompatibility between the GDPR and merchandising contracts within the framework of private autonomy. More specifically, the two solutions detect the boundaries of data paternalism and find that the high-level data protection would amount to the encroachment of personal autonomy when it exceeds the boundaries. To strike a fair balance between the fundamental rights of individuals in data protection and personal autonomy, they both advocate narrowing the applicable scope of the protective provisions in the GDPR in merchandising. Therefore, both solutions are risky. A little deviation either gives rise to excessive data protection at the cost of the dysfunctionality of contract law or leads to defeating the purpose of data protection. Differentiation is thus essential for both solutions, and merchandising defined in this dissertation serves as the best practice for both solutions.

Moreover, both of them suffer from some legal flaws. Solution 3 runs counter to the (intra-)systematic interpretation of the GDPR and the opinions of the EDPB by rendering the anytime revocability of consent optional. Although the opinions of the EDPB are not decisive, they carry weight with regard to the CJEU's interpretation. Moreover, the two-tier interpretation might constitute a reformative understanding of the GDPR as it would compromise the strong control of data subjects over personal data designed by the EU legislator. On the other hand, solution 3 is also subject to dogmatical objections. Without a clear delineation of merchandising contracts in the B2B context from other contracts, it would easily be stretched to a general clause for contracts if they are fair. Moreover, it cannot answer why an equitable merchandising contract under German law could be used as a typical contract under EU law.

Despite these similarities, comparisons can be made in the following respects.

Solution 3 is limited in the B2B context, whereas the two-tier interpretation of consent is not (though it could be). At this point, solution 4 can tackle the issue of under-protection for data subjects in B2C contexts, while the users' merchandising scenario is excluded from solution 3. According to solution 4, if the controller can prove the exclusion of the anytime revocability of consent anchored in Art. 7 (3) GDPR accords to the genuine wish of the data subject, a binding relationship can be established.

In terms of implementation costs, solution 4 seems more appealing than solution 3 as it has a clear beacon, the B2B scenario whereon both

parties to the contract have some degree of self-sufficiency. In the absence of such preconditions, the cost to examine whether the data subject is genuinely willing to enter a contractual relationship is enormous, and the measures remain unknown. For instance, it is worth exploring whether a box waiting to be actively checked by the data subject – to waive the right to withdraw consent at any time – meets the requirement.[763] Even though the GDPR has passed on the cost to the controller according to the principle of accountability, the considerable cost and legal uncertainty would create a strong dissuasive effect. Consequently, instead of pursuing high-level consent, controllers would still settle with the anytime revocable one and attempt to collect as much data as possible and then analyze, exploit, and transmit personal data quickly after collection. On the flip side, the restriction of the B2B situation would be too conservative compared with solution 4. Given the history of the commercialization of portraits over the past hundred years, a similar change in perception might be appreciated in users' merchandising. If data subjects understand the methods, purposes, and risks of merchandising and can make choices after evaluation with the assistance of information and education, the restriction stemming from the boundaries of the justification of data paternalism would also be unjustified. The only justifying reason would be the cost of analysis. However, since controllers take the cost, the choice should be left with them.

However, there are two objections to this consideration. Solution 3 can also presuppose the exact prerequisites to increase clarity and reduce implementation costs as it is a general solution. Besides, as pointed out in Section 4.3.2. (3), it is difficult to delineate the B2B scenario from others. While a muster of merchandising contracts in the B2B context is expected to achieve a certain role of demonstration and instruction, it will no doubt be strained and lacking in legal grounds.

Against this backdrop, the two-tier interpretation of consent might be more future-oriented.

## 5.3 The result

The overarching applicability of the GDPR stemming from the ambitious and extensive purpose of the EU legislator inevitably permeates those

763 This paper tends to think that this is not enough. Since many people do not understand and do not use the right of withdrawal at any time, it is difficult to assume that people know what the opposite of it means.

places that already have specific legal norms,[764] such as merchandising. Without highlighting the boundaries of the justification of data paternalism within the legal framework of the GDPR, this job that must be done has been left to the CJEU. The lack of attention to those boundaries would not only deviate from the self-determination of data subjects but also lead to the "dysfunctionality" of contract law. Moreover, too much paternalism deprives data subjects of the opportunity to learn from their mistakes, when sometimes it is necessary to make some. In some scenarios, the GDPR is necessary because the price for mistakes made by data subjects is too high to bear, but in cases like the *landlady* or "*stink fingers*", mistakes are affordable for data subjects.

After the evaluation, while some solutions have more problems worth refuting, every solution is not perfect. Solutions 3 and 4 are preferable compared to solutions 1 and 2. In comparison between solutions 3 and 4, it needs to be admitted that solution 4 is more malleable, while solution 3 is relatively conservative. However, solution 4 is contrary to the interpretation of the data protection authorities at the EU level solution 3 is not. A muster of merchandising contracts in the B2B context at the EU level might alleviate their objections by providing legal certainty and reducing compliance costs. The most important components are the means, content, purpose, and the rights and privileges of the models, including the extraordinary opt-out rights. In this respect, many practice-oriented German commentaries regarding merchandising licensing contracts and contract templates are available for reference.

764 *Bull,* Sinn und Unsinn des Datenschutzes, S. 50; *Lauber-Rönsberg,* AfP, 2019, 373 (375-376).