Part II Merchandising under the GDPR

1. Introduction

After the EU data protection law emerged, a few German scholars have observed that its extensive applicability would impact merchandising.[191] This concern became evident and inevitable after the GDPR became effective. Therefore, it is time for a comprehensive discussion of how the GDPR regulates merchandising.

After a brief introduction to the GDPR and, in particular, its new features compared to previous EU data protection laws, Chapter 2 proves that the GDPR applies to merchandising cases. This may seem self-explanatory. However, as this Chapter unfolds, we can see that the GDPR's broad material and territorial scope of application also leaves some small spots. Chapters 3 and 4 discuss the application of the GDPR to unauthorized merchandising and authorized merchandising, respectively. It is to echo the structure of Part I for a more apparent contrast. More importantly, the two different forms of merchandising represent heteronomy and autonomy, respectively. A separate review of how the GDPR regulates these two modes of commercial exploitation of personal information allows a better examination of whether it achieves its dual objectives – data protection for data subjects and free flow of data (Art. 1 (2) and (3) GDPR).

Chapter 3 validates the unlawfulness of unauthorized merchandising under the GDPR and examines the possible remedies provided in the GDPR. Section 3.1 applies Art. 6 (1)(f) GDPR in unauthorized merchandising cases after a substantive interpretation of this provision using the GDPR's narrative. It accompanies an evaluation of the current approach adopted by German courts in dealing with merchandising cases.[192] Sec-

---

191 *Sattler, in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance – Contract Law 2.0?*, 225 (243 et seq.); *Schnabel*, ZUM, 2008, 657 (661).

192 This approach in merchandising cases has to be distinguished from the courts' argument in news coverage cases. In the latter context, German courts usually make it clear at the outset that because images were used for journalistic or artistic purposes, the KUG can be considered appropriate national law under Art. 85 (2) GDPR, which reconciles the freedom of expression and personal data protection because it meets the ECtHR's interpretation. See BGH, NJW 2022, 1676 - Tina Turner, Rn. 27-36; BGH, MMR 2021, 150 - Zulässigkeit einer iden-

tion 3.2 explores how the data subjects unauthorized merchandising cases would be compensated according to Art. 82 GDPR. Not only are damages caused by unlawful data processing discussed, but whether and how the data subject's rights can be used to claim damages is also analyzed. Some case studies regarding the cases mentioned in the Introduction of Part I present themselves to highlight the contrast without compromising the generalizability of the analysis.

Chapter 4 regarding authorized merchandising seeks the legal basis of merchandising contracts under the GDPR and reckons the applicability of the data subject's rights in merchandising cases. Before diving into the scrutiny of the lawful grounds in Art. 6 (1) GDPR, Section 4.1 addresses the question of whether the processing of personal images for merchandising falls under Art. 9 (1) as sensitive data. After excluding the application of Art. 9 GDPR in general, Sections 4.2 and 4.3 examine respectively the applicability and consequences of consent in Art. 6 (1) (a) and contracts in Art. 6 (1) (b) GDPR in authorized merchandising. As case law in the CEJU is not very rich, especially regarding Art. 6 (1) (b) GDPR, the analysis here is largely supported by the official documents issued by the WP29, the EDPB, and the EDPS as well as scholarly literature.

After concluding the findings in Section 4.4, the rights of data subjects in merchandising scenarios according to the GDPR are enumerated and examined for their feasibility and effectiveness in Section 4.5. Case studies are conducted alongside the discussion for clarification so that the comparison between the GDPR and German law in regulating merchandising is concrete and not devoid of content. Chapter 5 finally concludes this Part.

2. The applicability of the GDPR in merchandising

2.1 A brief introduction to the GDPR

Before diving into the overlap in the scope of application of the GDPR and the KUG in merchandising, it is necessary to review the advancements in data protection in the EU and Europe to better comprehend the substantial protection and objectives pursued by the GDPR. After all, history is a

---

tifizierenden Bildberichterstattung auf Internetseite einer Tageszeitung, Rn. 23; OLG Köln, ZUM-RD 2018, 549 - Anwendbarkeit des KUG neben der DSGVO, Rn. 9. Thus, it differs from merchandising cases defined in this dissertation, which are unrelated to news coverage or art at all.

continuous process, and by focusing on how things were formed, we can gain clarity on the things we face now.

Perceiving the threats that digitalization might pose to individual freedoms and rights, the German Federal State of Hesse issued the first personal data protection law in 1970,[193] and this wave of legal protection soon swept through Sweden, the Federal Republic of Germany, Austria, and the rest of the European Union. The Council of Europe has formulated the "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" (afterward the 108 Convention) in tandem with the OECD around 1980 to provide new *vires* to the ECHR drafted in the 1950s.[194] Although the 108 Convention is a non "self-executing" treaty,[195] its core notions including that individuals are the protected subjects of data protection law in respect of fundamental rights and freedoms, the omnibus approach to governing both public and private sectors alike,[196] as well as some key terms' definitions have profoundly influenced the subsequent legislation of the EU.[197]

By using its competence in governing the internal market,[198] the EU, in the 1990s, became the chief actor in data protection. The acute consciousness of "free flow" of personal data (within the EU) rendered the Directive 95/46 beyond a faithful transform of the 108 Convention as well as the ECHR. Consequently, this unique character, coupled with protection for fundamental rights and freedoms of natural persons, lays down the EU's dual-objectives structure for the data protection law (Art. 1 (1) and (2) of

193 Datenschutzgesetz, Hessisches Datenschutzgesetz, 1970.

194 OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, at http://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm; Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series (ETS) No. 108, Nr. 14.

195 Council of Europe, Explanatory Report to the Convention for the Protection of individuals with regard to automatic processing of personal Data, Nr. 38.

196 Simitis/Hornung/Spiecker gen. Döhmann in, *Simitis, Hornung and Döhmann*, Datenschutzrecht, Einleitung Rn. 116.

197 Art. 1 both in the 108 Convention and the Directive 95/46 state that (one of) their main purposes are to protect natural persons and respect human rights and fundamental freedoms. Art. 3 in the Directive 95/46 very much resembled Art. 3 in the 108 Convention regarding the applicable scope, the definitions as regard "personal data", "(automatic) processing, "special categories of data", etc.

198 Art. 95 EEC, now Art. 114 TFEU; The first sentence of the Preamble of the Directive 95/46; Art. 1 (2) of the Directive 95/46.

the Directive 95/46).[199] The 21st century ushered in a new phase of the EU data protection law. The right to the protection of personal data has been enshrined as a fundamental human right in Art. 8 of the Charter and granted with primary law status in the Treaty of Lisbon in 2009.[200] Using these new *vires* and under the impression of the Edward Snowden revelations, a directly applicable EU regulation,[201] namely the GDPR, replaces the Directive 95/46 aiming at full harmonization within the EU.[202]

Against this backdrop, the GDPR does not emerge *ex nihilo*.[203] Given the shortcomings of the Directive 95/46 and the existing legal fragmentation across the Member States, the GDPR, equipped with "real teeth", introduces a multitude of adjustments to expand and strengthen the EU data law substantially, especially in terms of legal provisions and execution.[204] Although there is some room to maneuver to the Member States prescribed intentionally by the GDPR,[205] they are mostly only allowed to concretize the provisions. After all, provisions and legal concepts of the GDPR are subject to autonomous interpretation by the EU. In this wise, the preliminary rulings carried out by the CJEU, as well as the Guidelines, Opinions, Recommendations, and Best Practices offered by the EDPB (previously the WP29) are of great importance in understanding the GDPR. Moreover, two chapters of the GDPR dedicate to the regulations on supervisory authorities for data protection EU-wide regarding their operating mechanism and, foremost important, consistency.[206]

The realized significant threats resulting from data technologies and ubiquitous data-harvesting practices lead to the new strategies codified in the GDPR. In addition to the expanded territorial scope,[207] strengthened

199 Subsequently, the dual-objectives structure has been almost literarily transformed in the GDPR (Art. 1(2) and (3) GDPR).
200 Art. 16 TFEU.
201 CJEU, Flaminio Costa v E.N.E.L, C-6/64; Art. 288 TFEU.
202 Rec. 3, 6, 7, 9 and 10 GDPR; Art. 99 (2) GDPR; *Schantz*, NJW, 2016, 1841.
203 *Fuster,* The Emergence of Personal Data Protection as a Fundamental Right of the EU, 3.
204 Recital 9 of the GDPR.
205 While there are more than 69 opening clauses, their scope of application is narrower, and their interpretation should be stricter and subject to final determination by the EU. Cf. *Miscenic and Hoffmann*, EU and comparative law issues and challenges series (ECLIC), 2020, 44 (50).
206 Chapter 6 "Independent supervisory authorities" and Chapter 7 "Cooperation and consistency".
207 Art. 3 GDPR

governance of data transfers,[208] new types of sensitive data,[209] and broadened data subject's rights,[210] the materialized principle of accountability and the adopted risk-based approach are highlighted advancements of the GDPR.[211] On the one hand, the principle of accountability is inevitable because it flows from the inherent task of the GDPR to cope with uncertainties,[212] such as developments of technologies, transnational and global collaboration in data processing and protection, and the vagueness between violations of data protection rules and damages to data subjects. Thus, omissions of these obligations, even without damages, could lead to exorbitant administrative fines.[213] On the other hand, the risk-based approach mitigates the disproportionate burden of accountability resulting from the broad application of conditions and strict obligations to some extent.[214] It has not just been regulated in the text of the GDPR,[215] but also applied in interpreting some terms and concepts of the GDPR, for instance, the fulfillment of the burden of proof stemming from the principle of accountability, the ambit of sensitive data, the balancing of competing interests between the data subject and controller and/or third parties in Art .6 (1) (f) GDPR.[216] Thus, large and influential data controllers are generally more obliged to adhere to the detailed and elaborate compliance rules than small and more conventional controllers whose processing is unlikely to result in a risk to the rights and freedoms of data subjects, or

208 Art. 44-49 GDPR.

209 The GDPR includes genetic data and biometric data for the purpose of uniquely identifying a natural person. See Art. 9 (1) in connection with Art. 4 (13) and (14) GDPR.

210 I.e., the GDPR has codified the right to erasure following the *Google Spain* case, now known as the "right to be forgotten" (Art. 17 GDPR), with more grounds for data subjects and an obligation for data controllers to notify every recipient. The GDPR has facilitated data subjects the right to portability (Art. 20 GDPR), the right not to be subject to a decision based solely on automated processing (Art. 22 GDPR), and the right to withdraw their consent at any time (Art. 7 (3) GDPR).

211 *Schröder*, ZD, 2019, 503; *Veil*, ZD, 2015, 347.

212 Hornung/Spiecker gen. Döhmann, in *Simitis, et al.,* Datenschutzrecht, Art. 1 Rn. 2.

213 Art. 83-84 GDPR.

214 Recital 15; *Renz and Frankenberger*, ZD, 2015, 158; *Veil,* ZD, 2015, 347.

215 For instance, Art. 24(1), 25(1), 27 (2) (a), 30 (5), 32 (1), and 35 GDPR.

216 Vgl. *Schröder,* ZD, 2019, 503 (504, 506); Vgl. Schantz, in *Brink/Wolff,* BeckOK Datenschutzrecht, Art. 5 Rn. 38.

is occasional.[217] However, the risk-based rules do not lend themselves to easy execution but require thorough guidelines.[218] In addition, the final decision for their interpretation lies in the hand of the CJEU, which leaves room for uncertainty in national courts and to legislators.

All in all, as a pivotal plank of the European Commission's Digital Single Market strategy,[219] the ambitious purpose of the GDPR coupled with its supremacy and the "one size fits all" solution might lead to a sweeping effect on national legal regimes that do not endeavor to protect personal data but are entangled with personal data, such as administrative rules about foreigners,[220] transparency of government subsidy policy,[221] schooling,[222] and, of course, merchandising. This concern and probably factual consequence give importance to this dissertation's research question: If the

---

217 Art. 30 (5) GDPR. The compliance rules include, for instance, incorporating date protection measures by design and default (Art. 24-25), keeping records of processing activities (Art. 30), conducting data protection impact assessment" (Art. 32-36), and pointing data protection officer (Art. 37-39).

218 The WP29 as well as its succeeding body, the EDPB, have issued plenty of guidelines and opinions to shed light on the operation of the principle-alike rules in the GDPR. For example, WP29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, 844/14/EN; EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 14 et seq.; EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), 5 et seq.

219 European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, COM(2015) 192 final, at http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf.

220 See CJEU, Minster voor immigratie v. M., Joined Cases C-141/12 and C-372/12, para. 48. In this case, the court considered data contained in an application for a residence permit as well as in the legal analysis of this application personal data so that it should be subjected to the EU data protection law.

221 CJEU, Volker und Markus Schecke, Joined Cases C-92/09 and C-93/09, para. 80ff. The court has invalided the respective regulations because they did not strike a fair balance between the necessity to enhance the transparency of public policy and the right to the protection of personal data and the right to privacy.

222 See CJEU, Peter Nowak, C-434/16, para. 49. In the *Nowak* case, the court found out that written answers of a candidate at an examination and any related comments made by an examiner are personal data that should be protected under the EU data protection law. It might impose schools as well as teachers with onerous compliance obligations prescribed by the GDPR and astronomical penalties. For example, the Swedish DPA has fined a municipality almost 20000 euros because it used facial recognition technology to monitor the attendance of students in school. See Facial recognition in school renders Sweden's first

GDPR is applicable in merchandising where the commercial value of personal data prevails, and private autonomy without too much paternalistic protection is acclaimed, would its regulation be appropriate and proper?

2.2 The material and territorial scope of the GDPR

Art. 4 GDPR provides 26 essential definitions for the terms including the ones that are decisive for the material applicable scope of the GDPR, namely "personal data" in Art. 4 (1) and "processing" in Art. 4 (2). One characteristic of the EU data protection law is that it chooses the term "data" commonly used in digitalization instead of "information". Contrarily, the latter is the legal term used in China and the US for their modern acts of privacy protection.[223] Data under the GDPR is understood broadly with regards to its physical form, content, properties, dimensions, and conceptual levels so that both raw and unorganized data meaning nothing to human beings as well as semantic data as in personal images taken by cameras are (personal) data in the meaning of the GDPR.[224] Nevertheless, the emphasis on digitalization should not be exaggerated since "data" and "information" have been consistently used interchangeably in the GDPR and the EU official documents.[225]

GDPR fine, EDPB, at https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_sv.

223 In China, the newly issued "Personal Information Protection Law of the People's Republic of China" (effected on 11-01-2021) chooses to use the term information, while the bill has obvious similarities to the GDPR. For instance, the definition of personal information in the Chinese law states (Art. 4 (1)), "Personal information means all kinds of information related to identified or identifiable natural persons that are electronically or otherwise recorded, excluding information that has been anonymized." In the US, the segmented privacy protection laws do not affect their unanimous choice for the term information. See for instance 114th Congress, Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015; See California Consumer Privacy Act of 2018; Ohm, 88 Southern California law review 1125 (2015) (1130 et seq.).

224 See CJEU, Rynes, C-212/13, para. 22; Karg, in *Simitis, et al.*, Datenschutzrecht, Art. 4 Rn. 26.

225 See Art. 4 (1), (13) and (15) GDPR, and Recitals 6, 26, 29, 30 and 50; WP29, Opinion 4/2007 on the concept of personal data, WP136, pp.6-8; European Commission, Commission staff working document on the free flow of data and emerging issues of the European data economy Accompanying the document Communication Building a European data economy, SWD(2017) 2 final.

The GDPR essentially mirrors the definition of "personal data" in Art. 2 (a) of the Directive 95/46/EC about "any information relating to an identified or identifiable natural person". The typical risk-based definition – the simpler it is for the data controller and any others to single the person out in terms of cost, time, and technology, the more the GDPR tends to qualify the data as personal data – conspicuously expands the scope of personal data.[226] This relatively objective assessment,[227] coupled with the principle of accountability, obliges data controllers to prove that the data cannot be attributed to a natural person, for instance, by using anonymization as a default rule.

The last key factor in specifying the applicable material of the GDPR is the term "processing" pursuant to Art. 2 (1) with the definition under Art. 4 (2) GDPR. It covers all automated operations along the value chain of data processing, from collecting, storing, and using to erasing and deleting. More importantly, the term "processing" also extends to unautomated means. Art. 2 (1) GDPR excludes wholly unautomated means from the applicability of the GDPR, for example, noting down someone's phone number on a piece of paper. This exception is overruled if this note forms part of a directory organized alphabetically. In fact, given the widespread of digital products, the CJEU has concluded that photography and surveillance of people are processing personal data.[228]

As a pioneer in protecting personal data at a high level, the EU addresses a wide territorial applicable scope in respect of international trade and borderless communication to prevent forum shopping. Highlighted in the *Google Spain* case, the general rule of the establishment principle – the choice of law depends on where an entity is established – has been expanded by interpreting "establishment" and "in the context of the activities" flexibly.[229] It is no longer contingent on whether the establishment within the EU has carried out the data processing *per se*, economical support sustains the application of the EU data protection law.[230]

Nevertheless, against the E-commerce backdrop, which enables providers without residing in any Member States to provide services for data subjects within the EU, the establishment principle cannot tackle this

226 Recital 26 of the GDPR; CJEU, Patrick Breyer v Bundesrepublik Deutschland, C-582/14, para. 44 et seq.
227 *Brink and Eckhardt*, ZD, 2015, 1.
228 CJEU, Rynes, C-212/13, para. 22-25; CJEU, Sergejs Buivids, C-345/17, para. 31-36.
229 See CJEU, Google Spain, C-131/12, para. 52, 53 and 55.
230 *Spindler*, DB, 2016, 937 (938); *Albrecht*, CR, 2016, 88 (90).

problem, no matter how far stretched. The GDPR introduces the *Marktortprinzip* (principle of the market) in Art. 3 (2) GDPR to regulate data controllers outside the EU provided on either an economic connection or influence in people inside the EU by data processing.[231] Thus, if the entities without an establishment in the EU offer goods or services to data subjects in the EU or aim to monitor EU customers' behavior in any form of web tracking, they shall obey the rules established in the GDPR and likely have to appoint a representative as a contact point for data subjects and supervisory authorities within the EU.[232] It is also noteworthy that the location of data subjects instead of their nationality is decisive for applying the GDPR. All in all, one could argue that, broadly speaking, the location of data subjects instead of the controllers is decisive for applying the GDPR.

However, the GDPR also lists four exceptions for its material applicable scope in Art. 2 (2) GDPR and mandates the Member States to make some derogations and exemptions to specific parts of the GDPR according to Art. 85 GDPR. Compared to Directive 95/46/EC, the GDPR does not grant the Member States much discretion regarding its material scope and substantive protection. On the one hand, the exceptions are constructed restrictively. For instance, while the GDPR excludes its application in data processing "by a natural person in the course of a purely personal or household activity" in Art. 2 (2) (c) GDPR, it does not affect its governance over "controllers or processors which provide the means for such personal or household activities".[233] This exception to exception puts Apps for communication and social platforms under a magnifying glass, even though they focus only on providing instant messaging dominated by data subjects, or social networking existing between "real" friends. On the other hand, the authority for interpreting the general opening clause of Art. 85 GDPR is reserved by the CJEU. Without a clear and determined answer from the CJEU, the ambit of Art. 85 GDPR is still undecided (detailed discussion see below).

231 Recital 24 GDPR; *Schantz*, NJW, 2016, 1841 (1842); *Hornung*, ZD, 2012, 99 (102).

232 Art. 27 in combination with 4 (17) GDPR.

233 Art. 2 (2) (c) GDPR in connection with Recital 18.

2.3 Questions regarding the applicability of the GDPR in merchandising

At first glance, the GDPR applies to merchandising smoothly. First, being identified is the foremost important condition for merchandising because the person depicted, usually, a celebrity, must be identified to attract consumers' attention or trigger an image transfer. Second, in the digital age, almost every link in the production chain for merchandising, ranging from taking photos, over uploading data into computers for editing, storing, printing, to manufacturing the exemplars, has been "datafied.[234] Thirdly, the exceptions provided in Art. 2 (2) GDPR are generally not applicable. There is no need to elaborate that the public nature inherent in merchandising renders the exception for personal and household activities inapplicable. Moreover, the exception for deceased people's data in recital 27 of the GDPR is not problematic for merchandising because not only must the purposes of the processing but also its contents, means, and consequences be taken into consideration to determine whether this exception is applicable; Thus, data concerning deceased persons might be relevant for their relatives.[235] Since post-mortem personality protection in Germany rooted in human dignity anchored in Art. 1 GG is maintained by one's relatives as fiduciaries,[236] and merchandising of a deceased celebrity could result in wealthy increase or lawsuits of his or her successors, living relatives of the deceased celebrity may be at least indirectly affected by the processing from the GDPR's perspective.[237] It is hence suggested for data

234 This word is *borrowed* from Lupton and Williamson, 19 New Media & Society 780 (2017). However, sometimes purely handmade fan products exist, such as portraits of celebrities painted by street artists, etc. The GDPR is impossible to apply here because there is no data processing in the sense of GDPR. Nonetheless, this is exceptional given its negligible proportion of revenue and possible defenses for freedom of speech and art. However, as the whole production chain of fan products consists of various operations, and most of them are "datafied", the GDPR at least is partially applicable. Moreover, against the backdrop that merchandising occurs increasingly frequently and preferably on the internet, it is increasingly unproductive to focus on the exceptions.

235 *Paal and Pauly,* DS-GVO BDSG, Art. 4, Rn. 6; *Brink/Wolff,* BeckOK Datenschutzrecht, Art. 4, Rn. 5; *Voigt and Bussche,* The EU General Data Protection Regulation (GDPR): A Practical Guide, 11.

236 *Fischer,* Die Entwicklung des postmortalen Persönlichkeitsschutzes: von Bismarck bis Marlene Dietrich, 129ff.; *Gregoritza,* Die Kommerzialisierung von Persönlichkeitsrechten Verstorbener, 51ff.

237 CJEU, Volker und Markus Schecke, Joined Cases C-92/09 and C-93/09, para. 53; Karg in, *Simitis, et al.*, Datenschutzrecht, Art. 4 (1) Rn. 4; For instance, the WP 29's opinion has further argued that deaths caused by the genetic deficiency

controllers to obey the rules in the EU data protection law even when they process data about deceased people.[238]

Nevertheless, two questions remain about the applicability of the GDPR in merchandising.

2.3.1 Exceptions for the territorial applicability

Given the flourishing cultural and entertainment industry in Europe, it is common that European celebrities are invited by foreign brands to shoot advertisements either abroad or aiming at foreign markets, say, the Chinese market. It is questionable whether it falls under the scope of Art. 3 GDPR. Imagine three scenarios. One is that Thomas Müller, the famous German football player, travels to China to shoot an advertisement for a Chinese company producing running shoes. In the second scenario, Müller handles the merchandising business by himself (this is more likely for models who have just begun their careers). Instead of taking a long journey, he shoots a video and sends it to the Chinese company abroad. The last scenario is perhaps more common. Müller has authorized his merchandising rights in gross to an agency in Germany (like Nena did in the *Nena* case), which makes the commercial in tandem with the Chinese company and transfers the data to China. The advertisements in all scenarios are shown with Chinese subtitles and only broadcasted within China.

The first constellation is without a doubt ungoverned by the GDPR according to Art. 3 GDPR since the Chinese company neither has an establishment within the EU nor offers service/goods to data subjects in the Union. Even though the nationality of the data subject – Thomas Müller – is German, processing of his data taking place in a third country does not trigger the application of the GDPR because the term "data subjects who are in the Union" in Art. 3 (2) GDPR refers to the location of the data subject at the time when data processing takes place instead of the nationality or residence.[239]

---

may be considered as personal (sensitive) data about the deceased's children since such deficiencies are heritable. See WP29, Opinion 4/2007 on the concept of personal data, WP136, 22.

238 Ibid. 24.

239 See EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), 14-15.

On the contrary, the third scenario is undoubtedly regulated by the GDPR and even triggers an additional legal regime prescribed by the GDPR for data transfers. The agency in Germany and the Chinese shoemaking company are co-controllers in the sense of the GDPR since they decide together about the purpose and means of the processing of personal data. In this sense, the German agency must meet the two-tier requirement pursuant to Art. 44 GDPR. More specifically, it must at first comply with the general provisions in the GDPR as regards the general principles of processing, especially the lawfulness, rights of data subjects, etc. and the special rules for data transfers in Art. 46-50 GDPR as the designated country, China, is not "safe" according to the decision of the EU Commission to ensure an adequate level of data protection when personal data have been transferred to any country other than the EU Member States.[240]

The second scenario, however, illustrates the implementation issues resulting from the *Marktortprinzip*. Although the Chinese company does process personal data of a data subject located in the EU and arguably makes an offer for (merchandising) service to that data subject (Art. 3 (2) (a) GDPR),[241] the EU lacks the necessary grip to manage the data controller.

If the merchandising contract is not regarded as a provision of services to data subjects within the EU, it poses a risk of legal circumvention when controllers conclude contracts with data subjects separately. For instance, a US-based genetic testing company offers its services in a direct-to-consumer manner online and concludes hundreds and thousands of contracts with data subjects in the EU individually.[242] In this case, if the GDPR does not apply, the objective of the newly added *Marktortprinzip* – to prevent data controllers from circumventing the GDPR by establishing outside the EU – would be rendered futile.[243] However, if any contractual relationship leads to an application of the GDPR when one party or even a third party benefited from the contract is in the EU, even though the controller does not have the ambition to set foot in the EU market, the rigorous and extensive compliance rules outlined in the GDPR would constitute a great burden on the controller. Predictably, this will significantly increase the cost for foreigners to cooperate with EU data subjects, and ultimately dis-

240 Recital 6, 23, and 101 of the GDPR.
241 Plath, in *Plath,* DSGVO/BDSG, Art. 3 Rn. 20.
242 Mahmoud-Davis, 19 Wash. U. GLOBAL Stud. L. REV. 1 (2020) (8).
243 Schantz, in *Simitis, et al.,* Datenschutzrecht, Art. 44 Rn. 13 - 15.

courage the international corporation between EU and foreign companies, under which the EU market is not the target.

More importantly, insurmountable obstacles at the implementation level would emerge if the GDPR applied. For instance, when data transfers are involved, the controller must, besides fulfilling the general requirements in the GDPR, facilitate the EU Standard Contractual Clauses (SCC) pursuant to Art. 46 (2) (c) and (d),[244] or demonstrate conditions prescribed in Art. 49 (1) GDPR.[245] However, the functioning of these regulations is premised on that there is a data controller or a processor inside the EU. When the partner of the controller abroad is the data subject himself,[246] like in the hypothetical scenario, it lacks a grip for the GDPR to oblige the Chinese company to apply the GDPR. Consequently, the whole system runs into difficulties. After all, it is impossible to implement the GDPR abroad since the authority and investigative powers of DPAs are significantly limited.[247] Eventually, the lack of legal enforcement would lead to disregard and unawareness of the law.[248] Perceiving the dilemma, the GDPR requires companies abroad to maintain a representative in the EU (Art. 27 (1) GDPR). It could alleviate tensions between "reality" and "illusion" in enforcing rules about data protection and transfers,[249] but would eventually discourage the international corporation, in which the EU market is not the target. After all, the effectiveness of the *Marktortprinzip* relies on the absolute attractiveness of the EU market. It is questionable whether

244 Because it comes from a country that is not "safe" according to the decision of the EU Commission. Insofar, the European Commission has only considered the following countries providing an adequate level of protection as the EU, Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay. See Adequacy decisions, EU Commission, at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

245 For instance, explicit consent of the concerned data subject (Art. 49 (1) (a)), or a necessity of performing contracts (Art. 49 (1) (b)).

246 The GDPR, albeit implicitly, assumes that data subjects should not be considered controllers even though they decide the purpose and means of the processing of their data. Cf. Edwards, Finck, Veale and Zingales, Data subjects as data controllers: a Fashion(able) concept?, Internet Policy Review, at https://policyreview.info/articles/news/data-subjects-data-controllers-fashionable-concept/1400.

247 CJEU, Maximillian Schrems v Data Protection Commissioner, C-362/14, para. 43; Vgl. Schantz, in *Simitis, et al.*, Datenschutzrecht, Art. 44 Rn. 13 - 14.

248 *Veil*, Neue Zeitschrift für Verwaltungsrecht, 2018, 686 (696).

249 Cf. Kuner, 18 German Law Journal 881 (2017).

entering the EU market is still attractive to small companies after weighing the benefits and costs, especially compliance costs.

Against this backdrop, *Hornung* argues for the exclusion of the GDPR in its entirety for a one-time contract between one person inside the EU and a data controller outside the EU due to the absence of the need for protection (*Schutzbedürftigkeit*).[250] This teleological reduction in interpreting Art. 3 (2) (a) GDPR has merit because it avoids the dilemma described above. A one-time contract concerning one person inside the EU illustrates a fundamentally different picture than the one Art. 3 (2) GDPR envisaged on the internet environment where data-harvesting practices, automated profiling, and targeting advertisements overrun.[251] It is also significantly different from the genetic testing company mentioned above, which systematically and continuously processes data on many EU data subjects. Moreover, this finding is supported by the underlined rationale of Art. 27 (2) GDPR, which agrees to waive the requirement to maintain a representative in the EU, if the processing "is occasional" and "does not include, on a large scale, special categories of data", and "is unlikely to result in a risk to the rights and freedoms of natural persons".

Thus, one would argue that the GDPR does not apply to the Chinese company in the second hypothetical scenario because the personal data that the Chinese company processes are exclusively Müller's, the processing is on a small scale and occasional. Moreover, the conventional processing methods without profiling or behavioral analysis hardly present a risk to the rights and freedoms of the data subject.

2.3.2 The leeway for national laws offered by Art. 85 GDPR

The second issue is more important because its answer may lead to outright exclusion of merchandising from the scope of the GDPR, namely the leeway for national laws offered by Art. 85 GDPR. Its first paragraph states its objective and 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.*

250 Hornung, in *Simitis, et al.,* Datenschutzrecht, Art. 3 Rn. 52.
251 Recital 23 of the GDPR.

There are other provisions in the GDPR that also give judges some discretion to achieve the same objective, such as Art. 6 (1) (f), Art. 9 (2) (g), Art. 17 (3) (a), etc. However, they are much more restrictive and focused than Art. 85 GDPR. Art. 85 (2) GDPR sets out two conditions for the Member States to derogate or exempt from the application of the GDPR and specifies the provisions from which derogations or exemptions can be made. For one, derogations or exemptions must be made only for data processing for journalistic purposes or purposes of academic, artistic, or literary expression. For another, it must be "necessary to reconcile the right to the protection of personal data with the freedom of expression and information." Art. 85 (3) GDPR at last orders the Member States to notify the Commission of their derogations or exemptions without delay.

Thus, reviewing whether merchandising has journalistic purposes or purposes of academic, artistic, or literary expression is the key to determining whether Art. 85(2) GDPR is applicable. Admittedly, journalistic purposes should have a wide and contemporary meaning under the active influence of the CJEU and ECtHR as the term "citizen journalism" (*Bürgerjournalismus*) implies.[252] The critical factor is thus not the "means of transmission" but whether the statement's "purpose is to disseminate information, opinions or ideas to the public".[253] Moreover, against the backdrop that partial or total commercialization of the speaker does not naturally compromise the pursuit for public interests entailed in the activi-

252 ECtHR, Magyar Tartalomszolgáltatók/Hungary, Application No. 22947/13; CJEU, Satamedia, C-73/07, para. 56. In this case, the plaintiffs were two companies who collected and published information on the income and tax of 1.2 million natural persons in Finland, first through newspapers and later through an SMS service where people could receive tax information on another person by sending his or her name to one of the companies. After this service was prohibited by Finnish data protection authority, plaintiffs raised the lawsuit, which was subsequently referred to the CJEU by the Finnish court for an interpretation about, inter alia, processing for solely journalistic purposes. The CJEU answered that "activities may be classified as 'journalistic' if their sole object is the disclosure to the public of information, opinions or ideas, irrespective of the medium used to transmit them." *Oster,* Media Freedom as a Fundamental Right, 249 et seq.; *Weberling and Bergann*, AfP, 2019, 293 (297). The term *Bürgerjournalismus* was forwarded by the Australian DPA in its notification to the Commission to indicate an expensive reading for journalistic purposes. Österreichische Datenschutzbehörde DSB-D123.077/0003-DSB/2018 v. 13.8.2018, S. 5-6.

253 CJEU, Satamedia, C-73/07, para. 56, 61.

ties,[254] it is well argued that most cases regarding the right to one's image shall still be regulated by §§ 22, 23 KUG.[255] For instance, the platform of YouTube compensates YouTubers automatically according to the view number. This business model should not and does not undermine the journalistic purpose of a YouTuber because contributions of the processing of data in disclosure to the public of information, opinions or ideas are decisive in relation to journalistic purposes.[256] In this sense, the valid concern raised by *Ohly* that personality intrusions through acts of communication on the Internet should not be forced into the Procrustean bed of data protection[257] can be addressed since the "back door" is closed by the GDPR itself through a liberal reading of journalistic purposes in Art. 85 (2) GDPR.

Nevertheless, merchandising defined in this dissertation serves the commercial interests of merchandisers exclusively. Borderline cases such as satirical advertising and self-promotion of newspapers that contribute to the formation of public opinion are excluded. Therefore, the Member States shall not make derogation or exemption of the GDPR in merchandising cases pursuant to Art. 85 (2) GDPR.

---

254 See ibid., para. 60. "it…is not determinative as to whether an activity is undertaken solely for journalistic purposes".

255 BGH, GRUR 2021, 100 - Bildberichterstattung über ein Scheidungsverfahren, para 11; OLG Köln ZD 2018, 434 OLG Köln, ZUM-RD 2018, 549 - Anwendbarkeit des KUG neben der DSGVO; VG Hannover, 27.11.2019 - 10 A 820/19 - Fanpage einer Partei bei Facebook, para. 35; *Bienemann,* Reformbedarf des Kunsturhebergesetzes im digitalen Zeitalter, S. 245; *Gramlich and Lütke*, MMR, 2020, 662 (666); *Reuter and Schwarz*, ZUM, 2020, 31; *Lauber-Rönsberg*, AfP, 2019, 373 (375f.); *Weberling and Bergann,* AfP, 2019, 293 (295); *Krüger and Wiencke*, MMR, 2019, 76 (78); *Raji*, ZD, 2019, 61(64); *Ziebarth and Elsaß*, ZUM, 2018, 578 (585);*Hansen and Brechtel*, GRUR-Prax, 2018, 369; *Hildebrand*, ZUM, 2018, 585 (589); *Sundermann*, K&R 2018, 438 (442); *Lauber-Rönsberg and Hartlaub*, NJW, 2017, 1057 (1062); *Specht*, MMR, 2017, 577. In this sense, a notification to the Commission with the KUG should be made pursuant to Art. 85 (3) GDPR. See Specht-Riemenschneider, in *Dreier/Schulze,* Urheberrechtsgesetz, vor § 22 KUG, para. 6a.

256 See CJEU, Sergejs Buivids, C-345/17, para. 57; Vgl. Pötters, in *Gola,* DSGVO, Art. 85 Rn. 8; Buchner/Tinnefeld, in *Kühling/Buchner,* DSGVO/BDSG, Art. 85 Rn. 25; Vgl. BGH, NJW 2009, 2888 - Spickmich. para. 10; *Rombey*, ZD, 2019, 301 (303); Dix, in *Simitis, et al.,* Datenschutzrecht, Art. 85, Rn. 14; *Spindler,* DB, 2016, 937 (939).

257 *Ohly*, AfP, 2011, 428 (437).

Noteworthy, some scholarly literature argues for more discretion for national laws resorting to Art. 85 (1) GDPR.[258] This proposal may seem difficult to accept at first glance, as it is so disruptive that it could allow the Member States to adapt the entire regulation of the GDPR for reconciliation between freedom of expression and personal data protection. Out of this concern, the validity of this proposal is not explored here but placed in Part IV Solutions.

2.4 Conclusions

As merchandising involves processing of personal data as always, the GDPR is applicable. It was not a problem under Directive 95/64/EC because it provided more extensive discretion for the Member States and the BDSG gave precedence to the KUG according to the principle of *lex speicilas*. However, after the GDPR came into effect in May 2018, German legislators have been evasive on this issue in sharp contrast to the heated academic debate. Moreover, they have not yet notified the Commission about the KUG but merely the state laws in Germany on press privilege pursuant to Art. 85 (3) GDPR.[259]

The expanded territorial applicability of the GDPR is problematic. Stemming from the political imperative anchored in the Charter, the EU data protection law is purported to permeate legal orders worldwide with the influence of the EU (market).[260] This goal premises that data controllers/processors are located or represented in the EU. When models are represented by themselves instead of agencies and cooperate with foreign companies outside the EU, the GDPR faces significant implementation difficulties. Though a teleological reduction of Art. 3 (2) GDPR is forwarded

---

258 For instance, *Bienemann*, Reformbedarf des Kunsturhebergesetzes im digitalen Zeitalter, S. 71f.; *Lauber-Rönsberg,* AfP, 2019, 373 (377); *Krüger and Wiencke*, MMR, 2019, 76 (78); *Ziebarth and Elsaß,* ZUM, 2018, 578 (581f.); *Lauber-Rönsberg and Hartlaub,* NJW, 2017, 1057 (1062); *Specht,* MMR, 2017, 577.

259 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.

260 Reidenberg, 52 STAN. L. REV. 1315 (2000) (1347).

when an offshore company concludes a one-time contract with one certain data subject in the EU, it does not prejudice the general applicability of the GDPR in merchandising because these are rare cases as models are usually represented by local agencies which account for the responsibilities assigned by the GDPR.

Moreover, merchandising – using one's likeness to influence consumers' decisions via image-transfer or attention-grabbing – does not fall under the scope of Art. 85 (2) GDPR because neither is it intended to nor factually does it contribute to a debate of general interest in society or aesthetical expression.[261] The controversy around the nature of Art. 85 (1) GDPR may bring some problems for the application of the GDPR in merchandising, but they are dealt with late. Therefore, the GDPR takes precedence over the KUG in merchandising due to the primacy of the EU law.

3. Unauthorized merchandising under the GDPR

3.1 The unlawfulness of unauthorized merchandising cases under the GDPR

3.1.1 Applying Art. 6 (1) (f) GDPR in unauthorized merchandising cases

(1) The principle of accountability regarding the "test grid" of Art. 6 (1) (f) GDPR

Before starting the analysis of the substance of Art. 6 (1) (f) GDPR, the principle of accountability proclaimed in Art. 5 (2) GDPR must be mentioned first. It consolidates two requests for data controllers. They shall not only be held responsible for fulfilling the GDPR-compliance obligations but, more importantly, be able to demonstrate that they have fulfilled the obligations.[262] As failure to comply with the principle leads to an upgraded administrative penalty according to Art. 83 (5) (a) GDPR, the principle raises the awareness (and cost) of compliance for data controllers and reduces the burden on oversight authorities.[263] In addition, controllers bear (civil) liability if "it is not in any way responsible for the event giving rise to the damage" (Art. 82 (3) GDPR). It is hence necessary for them to keep

261 *Tavanti*, RDV, 2016, 295 (233).
262 Vgl. Herbst, in *Kühling/Buchner,* DSGVO/BDSG, Art. 5 Rn. 77.
263 Vgl. Schantz, in *Brink/Wolff,* BeckOK Datenschutzrecht, Art. 5 Rn. 38-39.

proper documentation regarding data processing. Against this backdrop, controllers in unauthorized merchandising cases must demonstrate the lawfulness of data processing before or at least at the timepoint they begin to process the personal data according to the principle of accountability. Otherwise, even if their processing is legal, they may still face administrative penalties.

One may wonder how far the controller should go to demonstrate its compliance because, unlike consent, the GDPR does not specify the conditions for other legitimate grounds in Art. 6 (1) GDPR. The risk-based approach may be relevant here in assessing the burden of proof. The greater the impact of data processing on the rights and freedoms of the data subject, the more careful and cautious the controller should be in weighing interests in light of Art. 24 GDPR. It also echoes the requirement of the GDPR that the controller shall hire professionals to weigh the interests of both parties if data processing poses significant risks.[264] In this sense, if the data processing is rather conventional and brings minor risks on the rights and freedoms of the data subject, such as the bakery in the corner issuing membership cards, it may be sufficient for the controller to demonstrate that he has recognized the impinged rights and freedoms of the data subject, but the legitimate interest he pursued prevails. Although it appears from the wording of Art. 6 (1) (f) GDPR that the data subject should demonstrate that his or her interest overwhelms, but according to the principle of accountability and the wording of Art. 21 (1) GDPR,[265] the mainstream opinion still holds that the controller must provide documentation about the balancing of interests.[266]

Art. 6 (1) GDPR requires that data controllers must have a lawful ground to process personal data. The most relevant one in unauthorized merchandising cases is the alternative (f) since the data subject (the person depicted) has not given consent. Art. 6 (1) (f) GDPR reads,

---

264 Art. 37-39 GDPR require data controllers to designate a data protection officer to, for instance, monitor compliance with this Regulation in some events.

265 If the lawful ground for processing is Art. 6 (1) (f) GDPR, Art. 21 (1) GDPR obliges the controller to stop processing when the data subject claims the right to object, "unless **the controller demonstrates** compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject" (stressed by the author).

266 See Schantz, in *Simitis, et al.*, Datenschutzrecht, Art. 6 Rn. 87; *Robrahn and Bremert*, ZD, 2018, 291 (294); *Voigt and Bussche,* The EU General Data Protection Regulation (GDPR): A Practical Guide, 31.

> *processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*

It provides a "test grid" (*Prüfraster*) that contains three cumulative conditions for lawful data processing:

1) legitimate interests pursued by the controller or by a third party through the processing of personal data, and
2) the necessity between the processing and the pursuit of the legitimate interests, and
3) legitimate interests in (1) outweighing the interests or fundamental rights and freedoms of the data subject harmed by data processing.

It is largely agreed upon in literature and courts that the legitimate interests of controllers should be widely understood in light of recital 47 of the GDPR and the working papers of the WP29.[267] The commercial interests in promoting business pursued by merchandisers are protected by the fundamental freedom to conduct a business anchored in Art. 16 of the Charter and partially by the freedom to choose an occupation and right to engage in work in Art. 15 of the Charter. These interests are generally legitimate under the GDPR.[268]

Admittedly, public figures may contain some information that is interesting to the public. The "infotainment" is also covered by the freedom of expression irrespective of editorial control,[269] as who would not be interested to see Naomi Campbell's popping out to the shops for a bottle of milk,[270] to know celebrities' lifestyles,[271] or to judge the solidarity between members of royal families.[272] After all, deeming the curiosity about

---

267 See WP29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, 844/14/EN, 25-26.

268 Vgl. Ehmann, in *Simitis, et al.*, Datenschutzrecht, Anhang 3 zu Art. 6 Rn. 25.

269 BVerfG, GRUR 2000, 446 - Caroline von Monaco II, para. 58; BVerfG, NJW 2001, 1921 - Prinz Ernst August von Hannover, the 4th Guideline; BVerfG, NJW 2006, 2836 - Luftaufnahmen von Prominentenvillen II.

270 Naomi Campbell v MGN Limited House of Lords, 6 May 2004 [2004] UKHL 22, para. 154.

271 BGH, GRUR 2007, 527 - Winterurlaub, para. 26; BGH, GRUR 2009, 584 - Enkel von Fürst Rainier; BGH, GRUR 2008, 1024 - Shopping mit der Putzfrau auf Mallorca, para. 20; ECtHR, Zu Guttenberg v. Germany, Application No. 14047/16, para. 13,

272 BGH, GRUR 2007, 523 - Abgestuftes Schutzkonzept I, para. 14.

celebrities' privacy inferior seems rather condescending.[273] However, informational value lacks in merchandising cases because controllers neither make contribution to a debate on matters of general interest nor intend to.[274]

(2) The necessity between data processing and the pursuit of the interests

The term "necessary" in Art. 6 (1) (f) GDPR deserves more attention since it is one of the gatekeepers to prevent the balancing of interest from becoming an "argumentative Façade" for data controllers.[275] Stemming from the principle of data minimization in Art. 5 (1) (b) GDPR and the jurisprudence of the CJEU, the majority opinion in the literature understands the term "necessary" as no less intensive data processing possible to achieve the legitimate interests to a similar extent.[276] In this wise, one must scrutinize the contents, means, and duration of the specific processing operations.

From a practical perspective, identification is the key to image transfer or attention grabbing in celebrity merchandising. In addition, dentification of ordinary people is also necessary for in users' merchandising that enables the advertising to spread in a ripple pattern and possibly go viral via interactions with "friends". Moreover, there is no need to distinct celebrity merchandising from users' merchandising in assessing the necessity in Art. 6 (1) (f) GDPR. The emergence of internet influencers whose job is to make other people interested in their images and thus influence followers' patterns of consumption,[277] blurs the distinction between celebrities and non-celebrities to some extent as many microcelebrities are

273 ECtHR, von Hannover v Germany (no 2), Application No. 40660/08 and 60641/08, § 109; Vgl. *Ohly,* GRUR Int, 2004, 902 (911).

274 ECtHR, von Hannover v Germany (no 2), Application No. 40660/08 and 60641/08, § 109, with further references.

275 Frenzel, in *Paal and Pauly,* DS-GVO BDSG, Art. 6 Rn. 26.

276 Recital 39 of the GDPR; CJEU, Volker und Markus Schecke, Joined Cases C-92/09 and C-93/09, para. 74, 76, 77; CJEU, Digital Rights Ireland and Others, Joined Cases C-293/12 and C-594/12, para. 56; Roßnagel, Pfitzmann and Garstka, Modernisierung des Datenschutzrechts, 2001, S. 101; *Roßnagel*, ZD, 2018, 339 (344); *Robrahn and Bremert,* ZD, 2018, 291 (292); Plath, in *Plath,* DSGVO/BDSG, Art. 6 Rn. 17, 56; Buchner/Petri, in *Kühling/Buchner,* DSGVO/BDSG, Art. 6 Rn. 147a.

277 OLG München, 25.6.2020 – 29 U 2333/19 - Blauer Plüschelefant, 1. Guideline.

active online.[278] There are too many factors to assess publicity, such as the number of followers, the degree of internet influences' liquidity, and the impact of the platform. After all, it is not only impractical but also presents an antiquated understanding of merchandising in the online environment.

More importantly, by denying the necessity in merchandising cases from the outset, pictures on the internet for commercial interests would need to be pixeled in general unless controllers have obtained consent of the data subjects or a public interest according to Art. 6 (1) (e) GDPR exists. Consent would be inflated.[279] It would behoove controllers to obtain blanket consent from data subjects for any subsequent processing to avoid violation of the GDPR.[280] A more liberal proposition is argued in merchandising cases that public exposures of clearly identifiable photos/videos are usually necessary to promoting and advertising one's legitimate business. It does not mean that the court's conclusion that consent must be obtained for ads involving ordinary people is incorrect. Rather, the lawfulness of data processing in the case should not be rejected at the requirement of necessity.

(3) The interfered interests of data subjects

The interests or fundamental rights and freedoms of data subjects must also be understood broadly to ensure a high level of data protection for data subjects (recital 6 GDPR).[281] Possible interfered interests, rights and

278 Microcelebrities are "ordinary Internet users who accumulate a relatively large following on blogs and social media through the textual and visual narration of their personal lives and lifestyles……and monetize their following by integrating "advertorials" into their blogs or social media posts and making physical paid-guest appearances at events." See Abidin, 2 Social Media + Society 3 (2016).

279 Vgl. *Engeler*, PinG, 2019, 149 (152).

280 Thinking about the emails sent by LinkedIn, Instagram, and so on, they all use their users' images and names for promotion and advertainments. This practice is in fact appalling to many users even though it appears that they have given their consent. See lawsuits in this regard, Fraley v. Facebook, Inc. 830 F. Supp. 2d 785, 808 (N.D. Cal. 2011); Perkins v. LinkedIn Corp. 53 F. Supp. 3d 1190 (2014); Parker v. Hey, Inc. Case No. CGC-17-556257, 2017 Cal. Super. LEXIS 609. Given the fact that people usually give their consent without reading the terms due to limited capacity of time and cognition, and other structural problems. Without citing many, see Solove, 126 Harvard Law Review 1880 (2013), 1883-1889.

281 Schantz, in *Simitis, et al.,* Datenschutzrecht, Art. 6 Rn. 101.

freedoms in unauthorized merchandising are the data subject's fundamental rights to privacy according to Art. 7 of the Charter and Art. 8 ECHR as a result of exposure (*die Bloßstellung*) to the public,[282] and the right to the protection of personal data enshrined in Art. 8 of the Charter as the control of the data subject over personal data would be essentially deprived.[283] Moreover, it is uncontested that celebrities' images have substantial goodwill if they participate personally in merchandising business.[284] Thus, the commercial interests embodied in their icons should also be protected by the fundamental freedom to conduct a business anchored in Art. 16 of the Charter.

Therefore, even though the privacy of celebrities is not interfered with by merchandising, the commercial interests embedded in their control over images can be included t into the equation that awaits balancing against the commercial interests pursued by the controller.

(4) The balancing of conflicting interests

Some constructive methods for interests-balancing have been proposed in literature.[285] The distilled guideline is that the more interests and rights in terms of quantity and quality are impaired by data processing, the more substantial the legitimate interests pursued by the controller must be to sustain the processing.[286] More specifically, one should apply an overall assessment by taking the expressive contents of the personal data, the nature of the data controller, the purpose, means, consequences as well as

282 Nemitz, in *Ehmann and Selmayr*, DS-GVO, Art. 82 Rn. 13; See, *Bieker and Bremert*, ZD, 2020, 7 (10).

283 Schantz, in *Simitis, et al.*, Datenschutzrecht, Art. 6 Rn. 101.

284 Goodwill is presented when a distinctive connection between the goods or services provided by the depicted person and his or her indicia has been established in the mind of the purchasing public. See Robyn Rihanna Fenty v Arcadia Group Brands Ltd (T/A Topshop) [2015] EWCA Civ 3.

285 For instance, *Bieker* and *Bremert* made contributions to identifying the fundamental rights and freedoms of individuals that may be hindered and threatened at different stages of data processing, and how the risks manifest. See *Bieker and Bremert*, ZD, 2020, 7 (8); *Herfurth* forwarded a "3x5 – model" in the form of a matrix that comprehensively lists 15 essential criteria for measuring the riskiness of data processing operations. See *Herfurth*, ZD, 2018, 514 (515).

286 See *Herfurth*, ZD, 2018, 514 (515); See Schantz, in *Simitis, et al.*, Datenschutzrecht, Art. 6 Rn. 105f.

the impacts of the processing into account. Among the factors, the means and purpose of the data processing are foremost important.[287]

In addition, it must examine the role played by online communication as to whether it establishes a "more or less detailed profile" of the data subject,[288] or leads to *de facto* uncontrollability and incalculably high risk of recombination and long-term storage of personal data as *VG Hannover* stressed.[289]

On the one hand, Internet communication allows information to spread faster and wider. At almost zero-cost, information can be accessed, copied, extracted (from the original context), redistributed and stored. It is almost impossible for data subjects to make information that is already on the web disappear.[290] As the BVerfG proposed almost half a century ago, unlimited use, and storage of personal data posed high risks of profiling and making everyone a "hollow man" based on the construction of integrated information systems (*Aufbau integrierter Informationssysteme*).[291] On the other hand, risks posed by data technologies such as big data must be distinguished from the ones brought up by the internet as a means of communication.[292] If the view adopted by the *VG Hannover* is followed, then risk impact assessments and other higher requirements in the GDPR would become a routine for controllers who use the internet as a mean of communication. Consequently, risk impact assessments would be reduced to a dead letter because the risks posed by the Internet are abstract and general,[293] and most data controllers would shed online communication because of the high cost of compliance.

Thus, the internet can quantitatively magnify the impact on the rights and freedoms of data subjects but not necessarily triggers the so-called big

287 Buchner/Petri, in *Kühling/Buchner*, DSGVO/BDSG, Art. 6 Rn. 152.
288 See CJEU, Google Spain, C-131/12, para. 37.
289 Ibid., para. 87; BGH, GRUR 2014, 1228 - Ärztebewertungsportal, para.40; BVerfG, GRUR 2020, 74 - Recht auf Vergessen I, para. 147; VG Hannover, 27.11.2019 - 10 A 820/19 - Fanpage einer Partei bei Facebook, para. 36; Schantz, in *Simitis, et al.*, Datenschutzrecht, Art. 6 Rn. 107.
290 Not only is the effectiveness of de-searching results limited to the EU (CJEU, Google LLC v CNIL, C-507/17), but the media blitz would also make it more likely that what the data subject wants to be forgotten remains in the web forever.
291 BVerfG, NJW 1984, 419 - Volkszählung, para. 159.
292 Ibid., para. 91.
293 BVerfG, GRUR 2020, 74 - Recht auf Vergessen I, para. 104.

data risks for data subjects.[294] This understanding is also in the line with the CJEU. In both the *Google Spain* case and *GC* case, the Court found the structured overview of one's information enabled by the list of results based on name searches, instead of the online communication, particularly risky for the freedoms and rights of individuals because it can thereby "establish a more or less detailed profile of him."[295] Therefore, the CJEU's argument in the *Google Spain* case that the commercial interests of data controllers are generally inferior to the right of privacy and the right to the protection of personal data of data subjects cannot be directly applied here because that case was involved with an additional risk for a "more and less detailed profile" of the data subject.

As the notion of "reasonable expectations" adopted by the GDPR requires a mixed subjective and objective standard,[296] it invites an evaluation from the social perspective that enables a certain margin of appreciation for the Member States in this regard.[297] Noteworthy, the "reasonable expectations" in the GDPR has to be differentiated from the notion "reasonable expectation of privacy" referred by the ECtHR in a series of privacy cases.[298] Whereas the latter serves to delineate the protective scope of Art. 8 ECHR from the public sphere,[299] the GDPR's notion is merely one criterion to weigh against the interests pursued by the data controller.[300]

---

294 OLG München, NJW 1982, 244 - Löschung von Negativmerkmalen einer Kartei, 245.

295 CJEU, Google Spain, C-131/12, para. 35; CJEU, GC and Others, C-136/17, para. 36.

296 Schulz, in *Gola*, DSGVO, Art. 6 Rn. 57; *Tavanti*, RDV, 2016, 295 (299).

297 Vgl. Schantz, in *Simitis, et al.*, Datenschutzrecht, Art. 6 Rn. 108.

298 See ECtHR, von Hannover v. Germany, Application No. 59320/00, para. 51; ECtHR, Halford v. the United Kingdom, Application No. 20605/92, para. 45. This consideration is also valid in the German judiciary. See BGH, GRUR 2021, 100 - Bildberichterstattung über ein Scheidungsverfahren. The plaintiff has been photographed during her divorce lawsuit in front of the court building. The BGH relied on the term "the reasonable expectation of privacy" to argue for the protection of personality rights.

299 See the concurring opinions of Judge Cabral Barreto and Judge Zupančič in the case of ECtHR, von Hannover v. Germany, Application No. 59320/00; ECtHR, Copland v the United Kingdom, Application no. 62617/00, para. 42; ECtHR, Peev v. Bulgaria, Application no. 64209/01, para. 37 et seq.

300 The 4th sentence of recital 47 of the GDPR, "[a]t any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place"; WP29,

In balancing the interests specified above, courts could argue through a "German lens" (*Deutsche Brille*)[301] by using the notion of "reasonable expectations" to introduce the national law. In merchandising, the German judiciary has been reinforcing the perception that merchandising requires permission from the person depicted irrespective of his or her social role ever since the *Paul Dahlke* case. This practice not only shapes the commercial practice of merchandising but also profoundly affects the "reasonable expectations" of the German people and the public. Consequently, a data subject should not reasonably expect that his or her data would be processed for advertising purposes if a contractual relationship between him/her and the controller is absent. This conclusion raises a weighty indication that the interests of the data subject outweigh the legitimate interests of the controller.[302]

Thus, one can reasonably argue that the interests, and rights of data subjects in unauthorized merchandising cases in general outweigh the data controller's legitimate advertising interests in accord with the reasonable exceptions of data subjects irrespective of their social roles. As some German courts have already dealt with merchandising under the GDPR, it is imperative to review the judgments and the new "harmony approach" adopted by courts.

3.1.2 Case analysis of Art. 6 (1) (f) GDPR

(1) Evaluation of the German decisions

i. Lack of legal basis

After the GDPR came effective, German courts have already delivered some judgments about merchandising cases but surprisingly, they have not referred any cases to the CJEU yet.[303] Noteworthy, the courts have developed a quasi "harmony approach", i.e., since the result of applying

---

Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, 844/14/EN, 33, 40, 60 and 63.

301 *Kühling*, NJW, 2020, 275 (278).

302 Vgl. Heberlein, in *Ehmann and Selmayr*, DS-GVO, Art. 6 Rn. 28; Albers/Veit, in *Brink/Wolff*, BeckOK Datenschutzrecht, Art. 6 Rn. 53.

303 OVG Niedersachsen, MMR 2021, 593 - Veröffentlichung eines Fotos auf einer Facebook Fanpage; LG Frankfurt am Main, 3.09.2018 - 2-03 O 283/18 - Friseursalon,.

§§ 22 and 23 KUG would be the same as the application of Art. 6 (1) (f) GDPR there is no need to solve the concurrence issue of the KUG and the GDPR. However, this approach is questionable in many respects.

Above all, the direct application of §§ 22 and 23 KUG is only permissible if the GDPR allows the Member States to make derogations or exemptions from the GDPR in scenarios regarding commercial data processing. In these cases, while the courts admitted that merchandising was not covered by Art. 85 (2) GDPR, they applied §§ 22 and 23 KUG directly without stating any legal basis. Though Art. 85 (1) GDPR could arguably be an independent opening clause that would delegate competence to the Member States, the courts left this controversy open.[304] Therefore, the courts implied Art. 85 (1) GDPR as an independent opening clause without giving any conclusive opinion.[305] As it is not *acte clair*, the validity of this premise should be brought up to the CJEU. In any case, it is not appropriate to imply the application of Art. 85 (1) GDPR vaguely as now.

ii. Some main requirements in the GDPR omitted

Some main requirements in the GDPR were left out in the judgments because the courts mainly relied on the KUG. For instance, the requirement of the GDPR for the controller to demonstrate that he has fulfilled the obligations according to Art. 6 (1) (f) GDPR was fully omitted by the court in the *hair salon* case.[306] Furthermore, the review of the "test grid" stipulated in Art. 6 (1) (f) GDPR is overly simplistic as the court resorted to the German jurisprudence on the KUG in balancing the conflicting interests, even though it later stated that this analysis could provide effective assistance in understanding Art. 6 (1) (f) GDPR. For instance, the court jumped to the conclusion that the fundamental rights and freedoms of the data subject outweighed the interests of the data controller, and thus the processing was unlawful only after its examination of the unlawfulness of the publication under the German legal regime.[307]

---

304 OVG Niedersachsen, MMR 2021, 593 - Veröffentlichung eines Fotos auf einer Facebook Fanpage, Rn. 42f.; LG Frankfurt am Main, 3.09.2018 - 2-03 O 283/18 - Friseursalon, para. 30.

305 The same conclusion, see *Jangl*, ZUM, 2021, 103 (106).

306 LG Frankfurt am Main, 3.09.2018 - 2-03 O 283/18 - Friseursalon.

307 The court argued that, on the one hand, the video clip did not belong to contemporary history and probably with some privacy implications, and on the

iii. Inaccurate understanding of the terminology in the GDPR

Because of the over-reliance on the case law of the KUG, courts lacked the incentive to adopt and learn the GDPR's narrative. Some understandings of the terminology in the GDPR is inaccurate, such as the direct marketing purpose and the necessity between the data processing and the purposes. More importantly, the rights and civil remedies prescribed in the GDPR were completely ignored, even though the courts validated the unlawfulness of the data processing under the GDPR. Only the injunctive relief according to §§ 823 and 1004 BGB were confirmed.[308]

For instance, *VG Hannover* in a case concerning advertising on a fan page considered that a less intrusive means existed for merchandising purposes, i.e., pixilation or a mosaic depiction of one's facial features.[309] A possible reason might be that blurring of the data subject in the advertisement would not dismiss its authenticity or creditability. However, this idea is objectionable in several aspects as argued in Section 3.1.1 (2). The main flaw of the court's argument is that it did not compare the data processing with the subjective purpose of the controller in the case but rather assumed an objective purpose instead. This renders this conclusion conservative. Both the *VG Hannover* and its higher instance probably recognized the weakness of this argument by not stopping here but discussing the balancing of interests further.[310]

---

other, the publication was in a purely commercial context, which rendered the consent of the person depicted indispensable. Ibid., para. 57.

308 It can be argued that plaintiffs only claimed remedies in the BGB against the unlawful data processing, so the court did not need to review the rights under the GDPR, such as the right to information. However, *Hoeren* suggests that an elaboration for the right to information and its exception would be needed because the court tried to argue that the consent, even if existed, was invalid since the obligation to inform the data subject has not been fully fulfilled. See *Hoeren*, ZD, 2018, 587 (588).

309 In that case, a member of a political party published several meeting photos on his fan page on Facebook to promote the achievements of his party in local affairs. In some photos of the gathering, the data subjects could be identified and thus sought help from the local DPA to ask that member of the political party (the data controller) to remove the photos. The *VG Hannover* has addressed that the identification of the data subjects was not necessary for the promotional purposes pursued by the controller. See VG Hannover, 27.11.2019 - 10 A 820/19 - Fanpage einer Partei bei Facebook, para. 50.

310 Ibid., para. 51f.; OVG Niedersachsen, MMR 2021, 593 - Veröffentlichung eines Fotos auf einer Facebook Fanpage, para. 27f.

In addition, the court in the *hair salon* case wrongfully qualified the data processing by the hair salon as direct marketing. Consequently, the impinged interests and rights of the data subject, and eventually, the balance between the countervalues from both sides, were incorrect. Direct marketing describes a series of means of marketing that directly communicates with customers who have been selected in advance.[311] In other words, it focuses on the relationship between the advertising company and the targeted consumers, whose preferences and behaviors are generally tracked and profiled via cookies, like-buttons on social platforms, etc.[312] Thus, the GDPR attaches great importance to the impact and threat of direct marketing on the rights and freedoms of data subjects and obliges data controllers an unconditional duty to stop processing for direct marketing when the data subject claims the right to object in Art. 21 (2) and (3) GDPR.[313] However, in the *hair salon* case, the dispute revolved around the advertiser and the person depicted instead of being targeted by the advertising. Although the advertisement on the company's fan page enabled the company to directly communicate with customers who have already "befriended" the company, it was merchandising instead of direct marketing.

Therefore, it was incorrect for the court to argue that the interest pursued by the controller was legitimate because the data processing was direct marketing with reference to recital 47 of the GDPR. A more detrimental result was that this incorrect qualification unduly exaggerated the impact of typical merchandising for the data subject because it fabricated the risks triggered by tracking and profiling. It would further exert influence on the balance of interests required by Art. 6 (1) (f) GDPR. Practically, the wrong qualification for direct marketing would also lead to a peculiar consequence. The data controller who chooses the Internet

311 The definition of direct marketing, see *Dallmer*, in: *Dallmer*, *Das Handbuch Direct Marketing & More*, S. 7-8.

312 Recitals 41, 42, 43,45, Art. 13 (1), (2) and (4) of the ePrivacy Directive; Art. 4 (3) (f) and recital 32 of the Proposal for the ePrivacy Regulation; Vgl. Ehmann, in *Simitis, et al.*, Datenschutzrecht, Anhang 3 zu Art. 6 Rn. 18; Also in this direction, Martini, in *Paal and Pauly*, DS-GVO BDSG, Art. 21 Rn .47ff. It excludes the online display of advertisements; Vgl. *Barth*, Der Kampf um die Werbung im Internet, S. 208.

313 While Art. 21 (1) GDPR requires other indicators such as balancing of interests or "profiling" to sustain an objection, Art. 21 (2) states that "the data subject shall have the right to object at any time" to direct marketing. Vgl. *Spindler/Schuster*, Recht der elektronischen Medien, Art. 21 Rn. 4 and 9.

as the communication tool must cease the advertisements immediately as the data subject claims the right to object according to Art. 21 (3) GDPR, whereas the controller who uses television/magazine – the seemingly outdated communication tools – does not have to.

Moreover, the court did not explain the term "necessary" either.[314] Since the court misidentified the interest pursued by the controller in the case, the measurement of necessity between its operations and the pursuit of the legitimate interest would be incorrect either. However, according to the court's logic, the court should not be skeptical about the requirement of necessity as the hair salon processed the plaintiff's data for direct marketing. As argued by some scholars, in pursuit of direct marketing, obtaining the addresses of customers (data subjects), be them physical or online, are necessary, while other personal indicia, such as age, sex, and consumer preference would be arguable.[315] Following this line, processing of data subjects' likenesses for publicity was completely unnecessary for direct marketing. Thus, the assessment of the court should stop here because the conditions prescribed in Art. 6 (1) (f) GDPR are cumulative.

Without specifying the infringed interests or fundamental rights and freedoms of the data subject, the court simply relied upon the notion of "reasonable expectations" in recital 47 of the GDPR to argue that the interests of the data subject outweighed those of the controller. It seems convincing that "it is contrary to the reasonable expectations of a customer in a hair salon that the visit is recorded and used for advertising on the internet".[316] However, the court seemed to misconstrue the "reasonable expectations" in the GDPR and the notion "reasonable expectation of privacy" referred by the ECtHR.

All in all, the approach adopted by German courts in applying Art. 6 (1) (f) GDPR to merchandising cases has some critical flaws besides its lack of justification. The overlooked principle of accountability, the wrongful understanding of direct marketing, and the overly abbreviated application of Art. 6 (1) (f) GDPR intertwined with too many national initiatives increase the risk of being challenged by the CJEU significantly. In other words, using the GDPR's narrative in applying it should be borne in mind to preclude forming a self-contained German system.

---

314 LG Frankfurt am Main, 3.09.2018 - 2-03 O 283/18 - Friseursalon, para. 58.
315 Vgl. Ehmann, in *Simitis, et al.*, Datenschutzrecht, Anhang 3 zu Art. 6 Rn. 29.
316 LG Frankfurt am Main, 3.09.2018 - 2-03 O 283/18 - Friseursalon, para. 58.

(2) To apply Art. 6 (1) (f) GDPR rightfully

Case studies of Art. 6 (1) (f) GDPR present here to make the comparison between the regulation of the GDPR and the German legal regime in merchandising more vivid and concrete.

At the outset, the court should examine whether the controller has provided documentation to prove that he has properly followed the "test grid" of Art. 6 (1) (f) GDPR to demonstrate the lawfulness of its data processing. An omission of this obligation would constitute a violation of the principle of accountability in Art. 5 (2) GDPR and lead to fines. In this wise, before data processing, the controller has to list the legitimate interest in advertising his business, and the interests, rights and freedom of the data subject, which were likely to be harmed by the data processing. Then, he should weigh the conflicting interests and demonstrate that his legitimate interests prevail. In the *clickbait* case, it could be argued that as the controller believed that certain public interests in knowing the information existed in addition to the commercial interest, he was convinced that the data processing was legitimate according to Art. 6 (1) (f) GDPR.

Against this background, one can focus on the substantial issues regarding Art. 6 (1) (f) GDPR. After denying the public interests of the clickbait, it is recommended for the court to specify the impinged interests and rights of the data subject due to the processing. While the control over personal data was deprived by the unlawful data processing, damages resulting in intrusions into privacy were not visible in this case. The *hair salon* case needs to be mentioned here for comparison. On the contrary, ideal interests like the mental distress suffered by the long-term display of the video online and the intrusion into privacy were prominent whereas commercial interests were not mentioned by the data subject.[317] This difference may make an impact on the remedies. These interests, as argued above, should be considered in balancing the interests, or precisely, to examine the weighing of interests conducted on the initiative of the data controller.

Noteworthy, unlike direct marketing, making advertainments online available does not amount to a game-changer that introduces a different or upgraded form of personality infringement. While the commercial purpose and online communication for merchandising do not have an impact on the data subject as significant as other purposes such as profiling and

317 One could also argue that the data subject was embarrassed by the fact of having hair extended, but the data subject did not address this issue.

scoring, the right to the protection for personal data enshrined in Art. 8 of the Charter is infringed not insignificantly since the data subjects were deprived of control over personal data and the informational self-determination from the outset. In other words, online communication was able to cause quantitative, not qualitative changes compared to merchandising in TV or magazines in both cases. Thus, the main competing values in the *hair salon* case were commercial interests in promoting the business on the one side,[318] and the rights to privacy according to Art. 7 of the Charter and Art. 8 ECHR, and the right to the protection for personal data enshrined in Art. 8 of the Charter on the other side. In the *clickbait* case, the most impinged right was the right to informational self-determination regarding the commercial interests in personal data.

Moreover, against the prevalent new logic of merchandising in social platforms, identifying ordinary people is necessary for advertisers who would like to make customers become advertisers. The necessity of being identified is unequivocally clear in the *clickbait* case. In balancing the interests, the German jurisprudence in merchandising scenarios is referential as the "reasonable expectations" of the data subjects mandates. In the *hair salon* case, by comparing the "reasonable expectations" of a consumer for having a service in a hair salon with the fact in the case, one can argue that the privacy of the data subject has been largely invaded according to the theory of sphere (*die Sphärentheorie*). It thus triggered *prima facie* protection against intrusion since having a hair extension is normally a private matter for a person.[319] Nevertheless, this case reminds one of users' merchandising on social platforms. As ordinary internet users are increasingly participating in exploiting their likenesses to promote or endorse local bistros or public events, it is possible that data subjects would not feel mentally disturbed by such merchandising. In other words, data subjects' "reasonable expectations" are prone to changes over time. It motivates one to wonder whether data subjects in similar cases to the *hair salon* case would increasingly become like the moderator in the *clickbait* case. Nevertheless, it would not compromise the argument's validity here in light of the "reasonable expectations" of the data subject because they would expect to be compensated from merchandising.

---

318 It could be argued that the video clip in the *hair salon* case might have some informational value if it shared some knowledge about hair extension. However, it was not obvious in the case.

319 Götting, in *Götting/Schertz/Seitz,* Handbuch Persönlichkeitsrecht, § 1 Rn. 5; For an elaboration about the theory of sphere see *Degenhart*, JuS, 1992, 361.

Therefore, the data processing in the *hair salon* case and the *clickbait* case were both unlawful in strict accordance with the GDPR. It is consistent with the conclusion of the previous analysis of the framework of Art. 6 (1) (f) GDPR in unauthorized merchandising in general.

3.2 Civil damages under the GDPR

3.2.1 Art. 82 GDPR as the legal basis

(1) Statutory conditions and contested application in Germany

Given the primacy of EU law, Art. 82 GDPR that mandates an independent civil liability for data controllers (and processors) based on violations against GDPR's provisions shall directly apply in the Member States.[320] According to its first paragraph,[321] infringement, material or non-material damages, and the causality between the infringement and damages are the conditions to sustain a claim.[322] It is uniformly agreed that infringements refer not only to violations of the legality of data processing (Art. 6 and 9 GDPR) but also the principles, the data subject's rights, and the obligations of data controllers, etc.[323]

The German judiciary seems to reach the consensus that damages under the GDPR should be broadly interpreted including "discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorized reversal of pseudonymization, or any other significant economic or social disadvantage" (recital 75 GDPR). Material damages refer not only to the loss of property but also to the loss of interests with property value, for instance, non-employment due to false information, credit or insurance

320 LG Karlsruhe, 02.08.2019 - 8 O 26/19 - Negative Bonitätsscore in Wirtschaftsauskunftei, para. 20; ArbG Düsseldorf, NZA-RR 2020, 409 - Unvollständige DSGVO-Auskunft, para. 104; Vgl. Frenzel, in *Paal and Pauly,* DS-GVO BDSG, Art. 82 Rn. 1; Boehm, in *Simitis, et al.*, Datenschutzrecht, Art. 82 Rn. 1.

321 "Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered."

322 Vgl. Nemitz, in *Ehmann and Selmayr,* DS-GVO, Art. 82 Rn. 7; Becher, in *Plath,* DSGVO/BDSG, Art. 82 Rn. 4.

323 Instead to cite many, see Boehm, in *Simitis, et al.*, Datenschutzrecht, Art. 82 Rn. 10.

agreements with worse conditions.[324] However, in the practice, plaintiffs are more inclined to claim for immaterial damages instead of material ones.[325] It is controversial whether fictive license fees can be deployed to compute the actual loss suffered by data subjects when their data have been exploited unlawfully by controllers.[326] While some scholars are in favor of this proposition as the commercial interests of personal data become prominent, and data subjects can benefit from these,[327] the German judiciary is equivocal in this regard.[328] In a case concerning account blocking on Facebook, the plaintiff claimed a fictive license fee as Facebook blocked her account while keeping pushing ads.[329] In her arguments, Facebook should compensate her with at least a portion of the revenue from advertising campaigns by using her data when it blocked her account. The *OLG München* rejected this claim by denying the synallagmatic relationship between the provision of services and consent given by the data subject: As Facebook violated neither the GDPR nor its contractual obligations, its use of personal data during the block was lawful.[330]

It is an innovation of the GDPR is to specify immaterial damages in the liability clause.[331] Since recital 146 of the GDPR requires a broad interpretation in terms of damage to ensure that data subjects receive "full and

---

324 See Moos/Schefzig, in *Taeger, Gabel and Arning,* DSGVO - BDSG - TTDSG, Art. 82 Rn 29; Nemitz, in *Ehmann and Selmayr,* DS-GVO, Art. 82 Rn. 17; Laue, in *Laue, Nink and Kremer,* Das neue Datenschutzrecht in der betrieblichen Praxis, § 11 Rn. 5; Gola/Piltz, in *Gola,* DSGVO, Art. 82 Rn. 11; Becker, *Plath,* DSGVO/BDSG, Art. 82 Rn. 4a; Kreße, in *Sydow,* DSGVO: Handkommentar, Art. 82 Rn. 5; Bergt, in *Kühling/Buchner,* DSGVO/BDSG, Art. 82 Rn. 19; *Neun and Lubitzsch*, BB, 2017, 2563 (2567).

325 Material damages for lost profits could be traceable when a loan was denied due to allegedly wrongful data processing. See LG Karlsruhe, 02.08.2019 - 8 O 26/19 - Negative Bonitätsscore in Wirtschaftsauskunftei, para. 18.

326 Nemitz, in *Ehmann and Selmayr,* DS-GVO, Art. 82 Rn. 17; *Herberger*, NZFam, 2021, 1088 (1092); *Strittmatter, Treiterer and Harnos*, CR, 2019, 789 (793-794).

327 *Peitz and Schweitzer*, NJW, 2018, 275; Gola/Piltz, in *Gola,* DSGVO, Art. 82 Rn. 11; Becker, in *Plath,* DSGVO/BDSG, Art. 82 Rn. 4a f. Boehm, in *Simitis, et al.,* Datenschutzrecht, Art. 82 Rn. 28. *Wybitul, et al.*, ZD, 2018, 202 (205); *Paal*, MMR, 2020, 14 (17); *Neun and Lubitzsch,* BB, 2017, 2563 (2567); Kosmides, in *Forgó, Helfrich and Schneider,* Betrieblicher Datenschutz, Teil XIII Rn. 45; *Dickmann*, r+s, 2018, 345 (351-352).

328 See the list of German judgments according to Art. 82 GDPR up to March, 2021, see *Leibold*, ZD-Akutell, 2021, VI.

329 OLG München, GRUR 2021, 1099 - Klarnamenpflicht bei Facebook, para.17f.

330 Ibid., para. 108-110.

331 Spindler, in *Spindler/Schuster,* Recht der elektronischen Medien, Art. 82 Rn. 1.

effective compensation for the damage they have suffered", the literature in Germany presents an attitude towards a more flexible interpretation for moral damages.[332] Courts also waive the German condition for serious mental damages in sustaining a non-material claim based on personality rights when the data subject claims non-material damages pursuant to Art. 82 GDPR.[333] However, the judiciary practice is contested about how specific and substantial the damages should be to get protection. For instance, some courts found the uneasy feeling and a constant state of distress non-material damages as the data subjects lost control over personal data due to data breaches or unlawfully disclosure.[334] In contrast, other courts stated that mere fear of misusing personal data after a data

---

332 Boehm, in *Simitis, et al.,* Datenschutzrecht, Art. 82 Rn. 11; Frenzel, in *Paal and Pauly,* DS-GVO BDSG, Art. 82 Rn. 10; Gola, in *Gola,* DSGVO, Art. 82 Rn. 13; Quaas, in *Brink/Wolff,* BeckOK Datenschutzrecht, Art. 82 Rn. 28; Becher, in *Plath,* DSGVO/BDSG, Art. 82 Rn. 4c; Bergt, in *Kühling/Buchner,* DSGVO/BDSG, Art. 82 Rn. 18a; *Wybitul, Haß and Albrecht*, NJW, 2018, 113 (114); *Klein*, GRUR-Prax, 2020, 433 (434 f.).

333 OLG Köln, 26.03.2020 - 15 U 193/19 - Geldentschädigung Rn. 87; LG Karlsruhe, 09.02.2021 - 4 O 67/20 - Mastercard; LG Landshut, 06.11.2020 - 51 O 513/20 - Anspruch auf Schadensersatz aus Datenschutzverletzungen; LG Mainz, 12.11.2021 - 3 O 12/20 - Schadensersatz wegen falscher Negativmeldung an Wirtschaftsauskunftei; LG Düsseldorf, ZD 2022, 48 - Bloße Verletzung keinen immateriellen Schaden; LG Essen, ZD 2022, 50 - Immaterieller Schaden, Verlust USB-Stick; LG Bonn, ZD 2021, 652 - Lange Wartezeit für Datenauskunft; LG Hamburg, K&R 2020, 769 - Verstoß gegen die DSGVO allein begründet keinen Schadensersatzanspruch; LG Lüneburg, ZD 2021, 275 – Datenübermittlung an Schufa; LG Karlsruhe, 02.08.2019 - 8 O 26/19 - Negative Bonitätsscore in Wirtschaftsauskunftei; AG Pfaffenhofen MMR 2021, 1005, - 300 EUR DSGVO-Schadensersatz für unerlaubte E-Mail; AG Hannover, ZD 2021, 176 (Ls.) - Kein Schadensersatz nach DSGVO für Bagatellverstoß; AG Diez, ZD 2019, 85 - Kein Schadensersatz nach DSGVO bei bloßen Bagatellverstößen.The opposite opinion, see OLG Dresden, MMR 2021, 575 - Posten eines Bilds mit Symbolen einer „Hassorganisation", Rn. 14; A "comparably serious mental damage" required, see LG München I ZD 2022, 52 - Voraussetzungen des Anspruchs auf immateriellen Schadensersatz nach der DSGVO, Rn. 31.

334 Courts recognize the fear of loss of control caused by a data breach or unlawfully disclosure as (moral) damages, see LG Darmstadt, 26.05.2020 - 13 O 244/19 - Schadensersatz wegen fehlgeleiteter Mail mit Bewerberdaten (the defendant inadvertently sent the email containing the plaintiff's non-sensitive personal information in the sense of the GDPR to a wrong recipient); ArbG Lübeck, 20.06.2019 - 1 Ca 538/19 - Mitarbeiterfotos im Facebook (unauthorized use of an employee photo on the company's own Facebook page); ArbG Dresden, 26.08.2020 - 13 Ca 1046/20 - unberechtigte Weitergabe von Gesundheitsdaten durch Arbeitgeber (the defendant unlawfully disclosed the plaintiff's sick leave

breach was either trivial or not concrete enough to sustain a claim.[335] In a case where the name, date of birth, gender, email address, and phone number were lost in the course of a data breach for a MasterCard, the court addressed that risks for identity theft claimed by the plaintiff were abstract and not particularly probable; the court went even further finding that even if the transaction data had been stolen, it would not have had a significant impact since the data only concerned small purchases.[336]

Nevertheless, some parallel practices are discernable in calculating the amount of non-material damages regarding certain violations, for instance, the violation of the obligation to provide information regarding data processing.[337] In two cases, in failing to respond promptly, controllers were required to pay 500 EUR after a month when data subjects claimed for the right of information, and from the 3rd month after the request, the monthly compensation upgraded to 1,000 EUR.[338] Besides, there are some similarities in quantifying the damages resulting from data breaches and failure to delete data in a timely manner. For instance, failure to withdraw photos and information from official websites within a reasonable time after the employee has left the company led to a compensation of 300 EUR.[339] This compensation upgraded to 1,000 EUR when the post

---

time); AG Pforzheim, 25.03.2020 - 13 C 160/19 - Psychotherapeut (a psychotherapist violated the GDPR by disclosing the sensitive data of a patient unlawfully).

335 See AG Frankfurt/Main, 10.07.2020 - 385 C 155/19 (70) - DSGVO-Schadensersatz setzt ernsthaften Verstoß voraus (due to an internal error, the personal data of customers being freely accessible on the Internet); AG Bochum, 11.03.2019 - 65 C 485/18 - Kein Ersatzanspruch nach DSGVO ohne konkreten Schadensnachweis (the defendant sent the judicial appointment document to another individual via unencrypted email); See LG Hamburg, K&R 2020, 769 - Verstoß gegen die DSGVO allein begründet keinen Schadensersatzanspruch (due to an error setting, the plaintiff's reservation information on the defendant's website was made available to the public for approximately 6 weeks).

336 LG Karlsruhe, 09.02.2021 - 4 O 67/20 - Mastercard.

337 It is well argued that inconsistency remains in this respect. See *Franck*, ZD, 2021, 680. This, however, makes the parallel practices more prominent.

338 ArbG Düsseldorf, NZA-RR 2020, 409 - Unvollständige DSGVO-Auskunft, followed by ArbG Neumünster, 11.08.2020 - 1 Ca 247 c/20 - Schadenersatz für verspätete Auskunft, and LAG Hamm, 11.05.2021 - 6 Sa 1260/20 - Schadensersatz bei nicht erteilter Auskunft nach DSGVO.

339 LAG Köln, 14.09.2020 - 2 Sa 358/20 - Foto des früheren Arbeitnehmers auf Webseite; ArbG Köln, 12.03.2020 - 5 Ca 4806/19 - vergessene Online-PDF-Datei.

was on Facebook.[340] For data breaches, the damage was 1,000 EUR and upgraded to 4,000 EUR when sensitive data were involved.[341]

More importantly, in none of these decisions did the courts require the plaintiffs to prove the specific number of damages they suffered. Instead, it took upon themselves the calculation of the appropriate amount. The underlined logic could be that mental damages were typical results of such torts and foreseeable for data controllers,[342] and the damages ordered by courts echoed the principle of effectiveness and dissuasiveness. These parallel practices effectively reduce the burden on data subjects to demonstrate their damages. On the contrary, there are also courts taking a strict approach to determining moral damages and causation. In this wise, data subjects suffering mental distress were unlikely to get compensated because they could not demonstrate the causality between their deteriorating position and the misbehavior of controllers as well as the justification for the amount of damages.[343] Given the difficulty for data subjects to prove the causality between infringements and damages, especially in the context of big data, it is a promising judiciary attempt to allow data subjects to receive some compensation without having to prove specific damage and causation after specific torts occurred.[344] Also, the final amount of compensation is subjected to fine tuning in light of the principle of effectiveness and dissuasiveness.

In assessing the number of damages, in particular non-material ones, scholarly literature suggests taking the factors listed in Art. 83 (2) GDPR, in particular the financial strength and subjective fault of the controller into account to ensure "full and effective" compensation.[345] If the violation

340 ArbG Lübeck, 20.06.2019 - 1 Ca 538/19 - Mitarbeiterfotos im Facebook. Compensation for 1,000 EUR was the maximal.

341 LG Darmstadt, 26.05.2020 - 13 O 244/19 - Schadensersatz wegen fehlgeleiteter Mail mit Bewerberdaten; AG Pforzheim, 25.03.2020 - 13 C 160/19 – Psychotherapeut.

342 Bergt, in *Kühling/Buchner,* DSGVO/BDSG, Art. 82 Rn. 44.

343 See LG Frankfurt/Main, 18.01.2021 - 2-30 O 147/20 - Datenleck (the court has denied the causal link between the data breach and the harassing phone calls received by the data subject thereafter); LAG Baden-Württemberg, 25.02.2021 - 17 Sa 37/20 - Kein immaterieller DSGVO-Schadensersatz bei US-Transfer (the causal link between illegal transfer of data to the United States and the damage has been denied).

344 In the same direction, *Franck,* ZD, 2021, 680 (683f.).

345 See *Wybitul, et al.,* NJW, 2018, 113 (115); *Wybitul, et al.,* ZD, 2018, 202 (205); Bergt, in *Kühling/Buchner,* DSGVO/BDSG, Art. 82 Rn. 18; Frenzel, in *Paal and Pauly,* DS-GVO BDSG, Art. 82 Rn. 10; *Kremer, Conrady and Penners*, ZD, 2021,

is caused by structural problems such as the data controller reduces the level of protection for profit, or the violation renders many people at stake, the amount of compensation should be effective and deterrent for the controller.[346] However, the function of administrative penalties must be distinguished from civil damages. It is currently under discussion whether a GDPR/EU standard for calculation is necessary.[347] Hopefully, the assessment of moral damages and causality will be clarified by the CJEU shortly since the BVerfG has forwarded a request for a preliminarily ruling.[348]

By stating that "*[a] controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage*", Art. 82 (3) GDPR asserts a presumption of fault instead of a liability without fault.[349] However, it is questionable how a data controller can be exempt from liability because it must be "not in any way responsible". On the one hand, the occurrence of damages cannot prove the liability. On the other, the data subject cannot be required to demonstrate where the controller has not done enough to claim damages.[350] It would be a clear violation against *lex non cogit and impossibilia* since data subjects cannot know the factual and supposed technical and organizational measures taken by the controller. Rather, the controller bears the burden to demonstrate that it has implemented appropriate technical and organizational measures to prevent the risks that are likely to arise by taking "into account the nature, scope, context, and purposes of processing" according to the risk-based approach according to Art. 24 (1) GDPR. This requirement is somewhat abstract and difficult to provide effective practical guidance in the absence of detailed industry standards. As a result, some controllers have turned to the argument that there is no causal relationship between the violation and the damages.[351] As this is the point that the data subject needs to prove according to the

---

128 (131); *Paal*, MMR, 2020, 14 (17); Holländer, in *Brink/Wolff*, BeckOK Datenschutzrecht, Art. 83 Rn. 31.

346 Becker, in *Plath*, DSGVO/BDSG, Art. 82 Rn. 4 d).

347 *Wybitul, et al.*, ZD, 2018, 202 (206).

348 BVerfG, NJW 2021, 1005 - DSGVO-Schadensersatzanspruch.

349 Boehm, in *Simitis, et al.*, Datenschutzrecht, Art. 82 Rn. 6.

350 A German court held that the principle of accountability is only applicable when the data controller is being challenged by a data protection authority instead of a data subject for the fulfillment of Art. 24 (1) GDPR. See OLG Stuttgart, 31.03.2021 - 9 U 34/21 - Mastercard-Priceless-Datenleck, para. 56.

351 LAG Baden-Württemberg, 25.02.2021 - 17 Sa 37/20 - Kein immaterieller DSGVO-Schadensersatz bei US-Transfer (the causal link between illegal transfer of data to the United States and the damage has been denied).

general rule on the allocation of the burden of proof and it is difficult,[352] the attempt mentioned above makes more sense to provide some standard compensation after specific violations occurred.

(2) Evaluation

Art. 82 GDPR is envisaged to allow data subjects easier access to recourse through the explicit provisions for moral damages and the reversed burden of proof in lability. Reading in entirety with the compliance rules in the GDPR, Art. 82 GDPR expands the scope of claims that data subjects can make. Controllers must strictly adhere to the GDPR's rules to avoid possible civil liabilities because an objective violation can trigger the claim of Art. 82 (1) GDPR for data subjects in the first place. However, the lack of an EU standard in interpreting the damages, causality and quantifying compensation undermines the practical importance of Art. 82 GDPR. The execution of Art. 82 GDPR remains ambiguous and contested to some extent in Germany.

It is thus not a surprise that the German judiciary is inclined to grant national remedies even though infringements of the GDPR have been established.[353] Admittedly, plaintiffs also tend to invoke the GDPR to prove illegality but assert damages under German law based on §§ 823, 1004 BGB in connection with §§ 22 and 23 KUG. The supremacy of the GDPR over national laws requires the application of Art. 82 GDPR provided on a violation of the GDPR.

As current cases mostly focus on moral damages, and so does the scholarly literature,[354] it is a pity that the *OLG München* forewent an opportunity to explore the attribution of the economic benefits of personal data. In

352 The causality between material damages and infringements is difficult to prove, not to mention the non-material ones. See *Paal,* MMR, 2020, 14 (17); Gola/Piltz, in *Gola,* DSGVO, Art. 82 Rn. 11; *Neun and Lubitzsch*, BB, 2017, 2563 (2567); *Dickmann*, r+s, 2018, 345 (351-352).

353 OVG Niedersachsen, MMR 2021, 593 - Veröffentlichung eines Fotos auf einer Facebook Fanpage; LG Frankfurt am Main, 3.09.2018 - 2-03 O 283/18 - Friseursalon; OLG Köln, ZUM-RD 2018, 549 - Anwendbarkeit des KUG neben der DSGVO.

354 There are more articles focusing on moral damages since it is the first time the EU data protection law entitled natural persons to compensation for moral damage. Even when material damages are mentioned in the articles, the examples and calculations are rather brief. Vgl. *Geissler and Ströbel*, NJW, 2019, 3414 (3415). Nevertheless, a noteworthy elaboration on the importance and connota-

that case, the underlying business logic of social platforms revolves around the commercial interests of personal data.[355] Thus, even though Facebook did not guarantee the continuity of its services in its privacy policy (which is certainly not an appropriate place to stipulate), it seemed to have some validity to claim for restitution based on the unlawful appropriation by continuously using data processing to push ads for revenue when it did not provide the service.

It is also interesting to note that civil damages are virtually trivial compared to the sky-high fines issued by data protection authorities. In an Austrian case, the Austrian Post was fined 18 million euros by the Austrian Data Protection Authority for unlawful processing of sensitive data (political orientation) of Austrian citizens.[356] On the contrary, the controller was liable to the infringed data subject for 800 euros.[357] Admittedly, the legal mechanisms and purposes of administrative penalties and civil damages are distinctly different and cannot be compared directly. Nevertheless, the principle of effectiveness and dissuasiveness also steers the measurement of damages to render infringements no longer profitable for controllers.[358] More importantly, generous civil compensation can incentivize data subjects to proactively exercise their rights under the GDPR. Such a huge discrepancy between administrative penalties and civil damages undermines the proactive pursuit of legal remedies by data subjects and shift all the responsibility of vetting and prosecuting to the data protection supervisory authority. It would be a huge waste of public power and tax as it can be solved entirely by data subjects on their initiative. After all, the huge administrative costs, and the use of enforcement in the "whack a mole" style are questionable.

All in all, by facilitating a more data subjects-friendly recourse mechanism, Art. 82 GDPR provides an impetus for enhanced protection for data subjects but is in dire need of guidance at the EU level. The motivation

---

tions of material damage see *Dickmann*, r+s, 2018, 345 (348f.); *Strittmatter, et al.*, CR, 2019, 789 (792).

355 The data controller generates revenue from processing personal data for ad distribution, which subsidizes the "free" social services it offers, and the "free" social services, in return, provide a constant flow of personal data.

356 See Datenschutzbehörde, Strafverfahren gegen Österreichische Post AG, OTS0095, at https://www.ots.at/presseaussendung/OTS_20191029_OTS0095/strafverfahren-gegen-oesterreichische-post-ag.

357 OGH Wien, ZD 2019, 72.

358 Boehm, in *Simitis, et al.*, Datenschutzrecht, Art. 82 Rn. 26; *Schantz*, NJW, 2016, 1841 (1847); *Strittmatter, et al.*, CR, 2019, 789 (791).

of data subjects to protect themselves proactively is, however, weakened by the contested application of Art. 82 GDPR and the ambiguity of the attribution of commercial interests contained in personal data.

3.2.2 Remedies for data subjects in unauthorized merchandising cases

(1) Infringements of Art. 6 (1) (f) GDPR

As explored above, unauthorized merchandising generally violates Art. 6 (1) (f) GDPR as the interests and rights of data subjects outweigh the data controller's legitimate advertising interests. Thus, data subjects only have to demonstrate damages resulting from the unlawful data processing in order to claim remedies based on Art. 82 GDPR. According to the scholarly literature and judgments in Germany, damages must be genuine and substantial. A not yet materialized risk does not suffice.

In merchandising cases, moral damages are hardly conceivable as German jurisprudence consistently addresses: No privacy infringement but free-riding on publicity. As the right to one's image confers both moral and property interests embodied in the autonomous decision of one's portrait to the person depicted, the typical remedy is restitution for the fictive license fee that the person would have received if his images had been used lawfully. Through the lens of the GDPR, moral damages of data subjects in typical merchandising cases are not visible either. Moreover, an actual financial loss of data subjects such as the diminished market value of their image and publicity due to the illegal data processing is, if any, difficult to prove. In fact, data subjects in merchandising cases are cut off from the value chain of data processing without any legal basis, and the commercial interests resulting from the processing flow to the controller exclusively. Therefore, the decisive question is whether data subjects can claim material damages drawn on the analogy with fictive license fees under the GDPR.

Though material damages are widely understood, and some scholars suggest an analogy with fictive license fees,[359] one may claim damages computed on the fictive license fee in a comparable situation upon two conditions. First, the EU personal data protection law attributes the commercial interests encompassed in personal data to data subjects. Second, a

359 Nemitz, in *Ehmann and Selmayr*, DS-GVO, Art. 82 Rn. 17; *Herberger*, NZFam, 2021, 1088 (1092); *Strittmatter, et al.*, CR, 2019, 789 (793-794).

market of commercial exploitation of personal data is recognized, at least, not objected to by law. The latter also supports the causality between the damage and infringement. If one cannot prove that he was able to get remuneration without the illegal data processing, then he cannot claim compensation.[360] Moreover, a lawful market is indispensable because the value of the commercial interests is a fact and determined by the market. Without a market, it is difficult to calculate the damage.

While the GDPR is elusive regarding the first condition,[361] it is arguable whether a market for personal data is admissible as the EDPB frowns upon it. The opinion of the EDPB, albeit not decisive at all, is referential in interpreting the GDPR. If the GDPR were to adopt the EDPB's opinion and prohibit any form of commercialization of personal data, the fact that a lawful market for licensing portraits exists in Germany (and possibly in all the Member States) should not be able to be an argument against it. Recital 146 GDPR would not serve as an argument either as it addresses that national law of the Member State could be applied in apportioning responsibility between joint controllers instead of quantifying (material) damages. Thus, both conditions are in question. A combination of Art. 6 (1) (f) GDPR and §§ 812 and 818 II BGB is not possible either, if the commercial interests embodied by the right to informational self-determination are not attributed to data subjects under the regime of the EU data protection law.

Therefore, besides the costs of establishing the infringements of the GDPR, expenses for inquiry, attorney's fees, and litigation costs,[362] it is questionable whether data subjects in merchandising cases can be well compensated. The real issues are whether the GDPR protects the pecuniary interests encompassed by personal data and whether the market for exploiting personal data is not legally objectionable.

---

360 In this direction, Moos/Schefzig, in *Taeger, et al.*, DSGVO - BDSG - TTDSG, Art. 82 Rn. 30.

361 Duch-Brown, Martens and Mueller-Langer, The economics of ownership, access and trade in digital data, 2017, 17, arguing that "the GDPR de facto (but not *de jure*) assigns property rights on personal data to the data controller, however limited they may be due to his fiduciary role."

362 ArbG Dresden, 26.08.2020 - 13 Ca 1046/20 - unberechtigte Weitergabe von Gesundheitsdaten durch Arbeitgeber; LG Darmstadt, 26.05.2020 - 13 O 244/19 - Schadensersatz wegen fehlgeleiteter Mail mit Bewerberdate; *Wybitul, et al.*, NJW, 2018, 113 (114); Laue, in *Laue, et al.*, Das neue Datenschutzrecht in der betrieblichen Praxis, § 11 Rn. 5; *Neun and Lubitzsch*, BB, 2017, 2563 (2567); *Wybitul, et al.*, ZD, 2018, 202 (205); Bergt, in *Kühling/Buchner*, DSGVO/BDSG, Art. 82 Rn. 19.

However, when mental damages are present in unauthorized merchandising cases, the outcome is very different. Data subjects also have to demonstrate that some concrete mental damages have resulted from the unlawful data processing in claiming moral damages under Art. 82 GDPR. It should include all damages that occur in all phases of data processing including recording, uploading, and possibly long-term storage of personal data. Taking the *hair salon* case as an instance, the filming of the hair extension constituted annoying harassment, and the online publication making her non-public information to the public presented a server intrusion into her privacy and caused fear and distress. Since the video clip was uploaded on Facebook and was visible to all, the data subject could not control or even know who knew her personal information.

Moreover, one may wonder whether data subjects could claim more moral damages if online communication takes place since it would render control over personal data virtually impossible. It seems reasonable to contend that the possibility of uncontrollability, (re)combination, and re(use) resulting from the free accessibility would escalate moral damages.[363] However, this argument would make large moral compensation a routine consequence of illegal online communication irrespective of other factors. In other words, such a risk in online communication always exists and it is too general and abstract (see 3.2.1). Therefore, it is suggested here to judge the magnitude of the impact in terms of the number of times the video is played and retweeted. The greater the number of plays and retweets is, the higher the degree of moral damage is, and the less likely it is that the data subject will make the information disappear from the web altogether. At the same time, this criterion is consistent with the principle of accountability. On the one hand, the controller wants the promotional video to be widely disseminated and thus always takes active measures to increase its spread. On the other hand, the controller is also capable of taking technical measures to restrict the spread of the video, such as rendering it visible only to friends, prohibiting downloads, etc. Hence, data subjects have to substantialize the exacerbated risks due to the online communication by demonstrating, for instance, the mass distribution of the video, the futility of stopping it.

In assessing the amount of damages, one can deploy the factors listed in Art. 83 (2) GDPR as suggested by some scholars and courts. It may seem contradictory to the role of civil damages, which is designed to fill damages rather than condemnation and punishment. However, the principle

363 *Korch*, NJW, 2021, 978 (979).

of effectiveness and dissuasiveness stipulated in the GDPR has to be noted here. Some fine-tuning of the number of damages is suggested taking account of the controller's financial strength because it is a prominent indicator of the dissemination range and influence. As noted above, some German courts held that an employer who forgot to delete an employee's data from a website after the employee left the company needed to pay damages of 300 to 1,000 euros. The difference in amount was largely dependent on the content of the data (whether the profile was detailed or not) and the extent of dissemination (on an intranet or Facebook).[364]

In this line, moral damages for more than 1,000 euros seem reasonable in unauthorized merchandising cases like the *hair salon* case. Firstly, the unlawful uploaded video was a severe invasion of the privacy of the data subject. Secondly, the controller has done nothing to limit the dissemination of the video on Facebook that was accessible by everyone. If data subjects want more compensation because they are concerned about further misuse resulting from the online communication, they must demonstrate the actual moral injury in a concrete way than just raising the concern. This also applies to the situation where they want to claim grave damages due to the loss of control over personal data.

(2) Infringements of the principles of data processing?

As the first material rule in the GDPR, Art. 5 sets out the basic requirements for data processing in response to the objectives of the Regulation. Art. 83 (5)(a) GDPR provides that a violation of the principles constitutes a ground for escalating administrative penalties to address the importance of these fundamental rules. However, since the manifestation of Art. 5 GDPR is in the form of principles, its general and abstract formulation coupled with flexible, yet ambiguous terms do not lend the principles to easy execution.[365] It creates difficulties in determining infringement and the ensuing damages. For instance, how to assess "fairness"? To what

364 While ArbG Lübeck has considered compensation of 1,000 EUR appropriate (the upper limit) when an employer uploaded a photo of an employee on Facebook without authorization, LAG Köln has implied that 300 EUR was a little too much for a university that did not take down an employee's resume in a timely manner after the end of employment. See ArbG Lübeck, 20.06.2019 - 1 Ca 538/19 - Mitarbeiterfotos im Facebook; LAG Köln, 14.09.2020 - 2 Sa 358/20 - Foto des früheren Arbeitnehmers auf Webseite.

365 *Roßnagel*, ZD, 2018, 339 (342).

extent are the amount, content, and storage of personal data "adequate" and "necessary" for processing under the data minimization and storage limitation principles?

Nevertheless, principles have been substantialized in the following provisions of the GDPR. As the first and probably the most important principle in Art. 5 (1) GDPR, the principle of lawful processing has been materialized in Art. 6 (1) GDPR and Art. 9 GDPR when it involves the processing of sensitive data. The intricate and all-embracing principle of fairness is guaranteed in numerous rules of the GDPR. For instance, it constitutes the core justification for the necessity test embedded in Art. 6 (1)(b) GDPR, which would otherwise be free of restriction due to freedom of contracts. In light of the principle of fairness, the EDPB requires "a combined, fact-based assessment of the processing for the objective pursued" by the contractual service instead of a subjective and contractual terms-based assessment.[366] Besides, even though the consent is obtained lawfully according to Art. 6 (1) (a) and 7 GDPR, the principle of fairness warns against the abuse of consent by data controllers since it has an independent meaning of the principle of legality to avoid redundancy.[367] The principle of transparency is embodied in the right to information in Art. 12, 13, 14, and 15 GDPR as well as the specific requirements for the validity of consent in Art. 7 (1) and (2) GDPR. Art. 25 and 32 GDPR are manifestations of data integrity and confidentiality principles. This principle requires controllers to conduct adequate technical and organizational management commensurate with the damage and risk it incurs.[368] The principle of accountability in Art. 5 (2) GDPR guides the understanding of Art. 25 (privacy design and default), 30 (records of processing activities), and 35 GDPR (data protection impact assessments) as well as at the same time relies on them to be more feasible for controllers.

Since civil damages under the GDPR require the existence of an infringement and substantial harm according to Art. 82 GDPR, decisive issues remain whether the conduct of the data controller constitutes a violation of provisions of the GDPR and whether such a violation causes damages. In this sense, the examination of a violation against principles still relies on the scrutiny of the terms in which they have been specified

366 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, 4 and 8.

367 See Herbst, in *Kühling/Buchner*, DSGVO/BDSG, Art. 5 Rn. 17.

368 Art 25 (1) and 32 (1) GDPR.

in most cases. It is noteworthy that the principle of accountability can serve as a basis for infringement for providing specific obligations for controllers.[369] Nevertheless, it is questionable whether failure in keeping proper documentation would cause damages to the data subject. Thus, without dismissing the mandatory nature of the principles of the GDPR,[370] civil damages stemming from a violation against principles are normally difficult to establish in terms of proving infringements and damages.

(3) Infringements of the data subject's rights

The data subject's rights granted by the GDPR from Art. 12 to 22 are remarkable. On the one hand, they are not limited by a pre-existing relationship of rights and obligations between the data subject and controller. By making the rights flow with personal data, any data controller that processes the personal data is obliged to respond to the data subject's rights. On the other hand, the rights are not "absolute" rights in the sense that controllers must fulfill any claim forwarded by a data subject. Some conditions must be met for a data subject to claim the rights. For instance, an alternative in Art. 17 (1) must present for the data subject to claim the right to be forgotten rather than the controller needing to delete all traces of the data subject on the network at any time as some media touted.[371] Moreover, there are exceptions for controllers to not to enforce the claim of data subjects. In terms of the right to be forgotten, the freedom of expression and information is a good cause to continue processing personal data.[372] Nonetheless, controllers must be responsive when a data subject raises a claim based on the GDPR according to Art. 12 (1) GDPR stemming from the principles of transparency and accountability.[373]

---

369 *Alexy,* Theorie der Grundrechte, S. 74.

370 *Roßnagel,* ZD, 2018, 339 (344).

371 Art. 18 (1), 20 (1) and (2), 21 (1) and (2), and 22 (1) GDPR all set specific conditions for claiming the right to restriction of processing, data portability, object, and not to be subject to automated individual decision-making, including profiling.

372 Exceptions are also available in Art. 13 (4), 15 (4), 17 (3), 20 (4), 21 (6) and 22 (2) GDPR for the respective data subject's right.

373 Art. 12 (1) GDPR reads, "the controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

i. The right to information

Art. 12 GDPR requires data controllers to provide information concerning data processing considering the principle of transparency. Accordingly, data subjects are harnessed with the right to information anchored in Art. 13 and 14 GDPR. The CJEU regards the provision of information by controllers as a prerequisite for the legality of data processing.[374] Otherwise, the possibility for a data subject to control personal data would be deprived from the outset. This standpoint is convincing because an autonomous decision (consent or concluding a contract) rests on transparent, and sufficient information, and errors or incompleteness of information would affect the validity of that decision.[375] More convincingly, the right to information is an enabling right that facilitates other data subject's rights and ultimately the control over personal data by the data subject.

In unauthorized merchandising, controllers usually do not notify the data subject, but there may be a difference in where they get the personal data from. For instance, in the *hair salon* case, the controller collected the data directly from the data subject, and thus it should provide the information "at the time when personal data are obtained" (Art. 13 (1) GDPR). In the *clickbait* case, the controller who did not obtain the data directly from the data subject should conduct its obligation to inform "at the latest when the personal data are first disclosed" on the internet according to Art. 14 (3)(c) GDPR. This would have no effect on the outcome of the infringement but only on the legal basis.

When controllers fail to fulfill the obligation to inform promptly, they may invoke the exceptions in Art. 13 (4) or 14 (5) (a) GDPR to exempt from this obligation if the data subjects have already possessed the relevant information including their contact information and the description of the content, purpose, manner, and consequences of data processing. This excuse remains doubtful if controllers fail to prove that the data subject

---

The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means."

374 CJEU, Bara and Others, C-201/14, para.43.

375 Vgl. Dix, in *Simitis, et al.*, Datenschutzrecht, Art. 13 Rn. 26; Bäcker, in *Kühling/Buchner*, DSGVO/BDSG, Art. 14 Rn. 44.

has the information stemming from the principle of accountability.[376] Moreover, data subjects in unauthorized merchandising are probably unaware of all the information listed in Art. 13 (1) and Art. 14 GDPR. More specifically, controllers would certainly fail to inform the lawful basis for data processing, and, if the lawful basis is Art. 6 (1) (f) GDPR, the legitimate interests pursued by the controllers according to Art. 13 (1) (c) and (d), and 14 (1) (c) and (2) (b) GDPR. In addition, notification regarding storage, further exploitation of personal data as well as available remedies for data subjects according to Art. 13 (2) and 14 (2) GDPR are probably also omitted here. Another excuse claimed by a German court – disproportionate effort in providing information in recital 62 of the GDPR – is not applicable anyway.[377] Hence, controllers in unauthorized merchandising cases would violate the right to information according to Art. 13 or 14 GDPR significantly.

Damages might be alleviated by an active and timely response to the data subject's request according to Art. 12 (3) in combination with 15 GDPR. As noted in Section 3.2.2, German courts only hold controllers liable for damages when they have not responded to the data subject's request for more than a month. Against the backdrop that the omission of the obligation for information by controllers amounts to significant disadvantages for data subjects, damages of 500 to 1,000 EUR per month are also discernable from the practice.[378] The underlined rationale is self-explanatory. Without prompt and duly notification, data subjects would not be able to invoke protections provided by the GDPR to defend human rights. More importantly, in the cases, data subjects did not prove the damages and causality besides the fact that they made a request.

It is the starting point for a data subject to control personal data by knowing which personal data is processed how by whom, and for what purposes. Hence, the review of the controller's compliance with the obligation for information should be rigorous. As an enabling right, damages

376 Dix, in *Simitis, et al.*, Datenschutzrecht, Art. 13 Rn. 22. It argues that every exception for the data subject's right should be proved by the controller who would like to invoke the exception.

377 LG Heidelberg, 21.02.2020 - 4 O 6/19 - Kein DSGVO-Auskunftsanspruch bei zu hohem Aufwand. In this case, the information was not necessary since it was already 10 years old.

378 ArbG Düsseldorf, NZA-RR 2020, 409 - Unvollständige DSGVO-Auskunft; ArbG Neumünster, 11.08.2020 - 1 Ca 247 c/20 - Schadenersatz für verspätete Auskunft; LAG Hamm, 11.05.2021 - 6 Sa 1260/20 - Schadensersatz bei nicht erteilter Auskunft nach DSGVO.

resulting from infringements thereof are difficult to calculate. In this sense, the parallel practices of German courts in ruling the damages are beneficial in urging controllers to actively provide information. It is thus also welcomed in merchandising cases where controllers deliberately fail to provide the necessary information without any legitimate reasons such as impairment to trade secrets or intellectual property.[379] Since damages are only awarded after one month, data subjects are recommended to claim the right to information as soon as possible.

ii. The right to object

Art. 21 GDPR provides the right to object allowing the data subject to object to the processing of personal data based on Art. 6 (1) (f) GDPR at any time "on grounds relating to his or her particular situation". When receiving the claim of this right, the controller shall stop the contested processing and delete the personal data according to Art. 17 (1) (c) GDPR unless it can demonstrate "compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject".[380] If the verification about the legitimate grounds of the controller is pending, the controller shall nevertheless restrict data processing pursuant to Art. 18 (1) (d) GDPR.

It is questionable whether a data subject can object to unlawful processing based on Art. 21 (1) GDPR. On the one hand, the wording of Art. 21 (1) GDPR seems to suggest that this right is only applicable in scenarios of lawful processing. The obligation for demonstrating personal or special reasons by data subjects to contest the processing is suitable for scenarios where a data controller processes a large volume of data and evaluates competing interests in a general and abstract manner. Therefore, the "corrective function" served by Art. 21 (1) GDPR helps the controller to value the particular situation of a data subject and thus promises data subjects comprehensive protection.[381] More importantly, the data subject should seek remedies instead of the right to object when his or her data has been unlawfully processed.[382]

---

379 Recital 63 GDPR.
380 Vgl. Caspar, in *Simitis, et al.*, Datenschutzrecht, Art. 21 Rn. 19.
381 Braun, in *Ehmann and Selmayr,* DS-GVO, Art. 21 Rn. 10; Martini, in *Paal and Pauly,* DS-GVO BDSG, Art. 21 Rn. 30.
382 Herbst, in *Kühling/Buchner,* DSGVO/BDSG, Art. 21 Rn. 15.

On the other hand, some scholars contend that this consideration restricts the applicable scope of the right to object too much.[383] Recital 69 indicates that "a data subject should, nevertheless, be entitled to object to the processing where personal data might lawfully be processed". The "corrective function" of this right should thus not prejudice its applicability in unlawful processing. In addition, it expects too much of normal people by requiring them to first judge (rightfully) the lawfulness of data processing and then to select the correct data subject's right.[384] In this sense, the "grounds relating to his or her particular situation" should be regarded as no more than a procedure condition.[385]

Following this seemingly mainstream opinion, data subjects in unauthorized merchandising cases can claim the right to object with reference to some personal reasons, such as invasion of privacy and encroachment on goodwill. Consequently, as they fail to demonstrate compelling legitimate grounds for the processing, controllers ought to stop processing. When this right is claimed together with the right to be forgotten discussed below, controllers in unauthorized merchandising cases shall delete the personal data that they collected immediately.

iii. The right to erasure (to be forgotten)

The right to be forgotten emerged in the high-profile *Google Spain* case and became famous even before it has been codified in the GDPR. It originates in the right to erasure in Art. 17 GDPR and is characterized by the deletion of personal data or blocking access to them.[386] As envisaged by the Council,[387] the right to be forgotten was born to be a data subject's right with great adaptability and many manifestations in the digital age.[388] The right to erasure needs to be fulfilled if the processing is unlawful

383 *Spindler/Schuster,* Recht der elektronischen Medien, Art. 21 Rn. 5.
384 Martini, in *Paal and Pauly,* DS-GVO BDSG, Art. 21 Rn. 21f.
385 Caspar, in *Simitis, et al.*, Datenschutzrecht, Art. 21 Rn. 7.
386 Dix, in *Simitis, et al.,* Datenschutzrecht, Art. 17 Rn. 5.
387 Council of the EU, Position of the Council at first reading with a view to the adoption of the General Data Protection Regulation, 5419/1/16 REV 1 ADD 1, 16.
388 As the right to be delisted by search engines, see CJEU, Google Spain, C-131/12, para. 88; CJEU, GC and Others, C-136/17, para. 52. As the right to request pseudonymization in news reports, web archives, Dix, in *Simitis, et al.,* Datenschutzrecht, Art. 17 Rn. 35

(Art. 17 (1) (d) GDPR) unless the controller can demonstrate that the processing is necessary "for exercising the right of freedom of expression and information" pursuant to Art. 17 (3) (a) GDPR.

The data subjects in unauthorized merchandising cases so far have not claimed this right in Germany. Instead, they requested the controllers to take down the personal picture/the video clip from the internet relying on German law (§§ 1004, 823 BGB and the KUG). The injunction here is very similar to the right to be forgotten in the GDPR's narrative because they both intend to block access to personal data in the internet environment.

If controllers stop the data processing without delay, the data subject cannot claim damages because there is no infringement of the right to be forgotten. Although since it has already made the personal data public, the controller shall inform other controllers who are processing the personal data, this obligation is on the condition of reasonableness pursuant to Art. 17 (2) GDPR.[389] However, if controllers refuse to stop the data processing and continue for a rather long time, they are liable for damages resulting from the infringement since the processing of personal data by no means contributes to public debate in merchandising scenarios. The decisive question for claiming Art. 82 GDPR is, once again, contingent on whether the data subject has suffered damages from the omission of this obligation. The data subject has to prove that due to the refusal, additional damages occur. Therefore, it is recommended that data subjects monitor the number of times a video is played and retransmitted in real time after they claimed the right to be forgotten.

It is highly recommended for data subjects to claim the right to erasure according to Art. 17 (1) (c) in combination with the right to object under Art. 21 (1) GDPR right after they discover the violation. In this way, controllers shall cease the processing and take down the personal data right after it receives the claim and would be liable for damages resulting from any omissions.

389 It reads, "the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data".

iv. Other rights?

The other data subject's rights including the right to rectification, the right to restriction of processing, and the right to data portability are either inapplicable or ill-suited for unauthorized merchandising cases.

The right to rectification in Art. 16 GDPR grants the data subject the right to rectify inaccurate personal data concerning him or her against the controller. Moreover, "the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement." Taking the *clickbait* case as an example, the right to rectification would not be supported since the commercial exploitation of the data subject's data concerned speculation aiming at attracting internet flow instead of misrepresentation. However, the right to rectification would be applicable if the advertising concerns a depiction in false light or a wrongful endorsement since the personal data/information is inaccurate.

It is, nonetheless, questionable whether this right is suitable for these kinds of unauthorized merchandising cases. A counterargument or a supplementary statement indicating the inaccuracy of the advertisement and requesting the rectification would be ineffective unless it has been made public. However, in this wise, the controller would get nothing but more exposure. The claim of the right to rectification would hence eventually encourage merchandising involving false light and wrongful endorsements. The right to restriction of processing in Art. 18 (1) GDPR is nonapplicable here because it purports to provide a middle ground for a *temporary truce* between the data subject and the controller where there is a dispute. According to Art. 18 (2) GDPR, the data controller can still process personal data within a minimum degree including storing when the data subject claims the right to restriction. Yet, the illegality of unauthorized merchandising is so obvious that the data subject needs not put up with data processing anymore despite the minimum degree but can simply claim the right to object and to erasure.

While it seems that a data subject might benefit from the right to data portability in Art. 20 GDPR in merchandising cases because he or she may ask the controller to transmit all personal data to a competitor of the controller in order to get higher remuneration, it is legally infeasible according to the conditions listed in Art. 20 (1) GDPR (discussed in the next Part regarding authorized merchandising). Furthermore, the right to data portability is useless in prohibiting data processing of the controller

since it is an independent right from the right to object and to be forgotten pursuant to Art. 20 (3) GDPR.[390]

3.3 Preliminary conclusions

Unauthorized merchandising is unlawful according to Art. 6 (1) (f) GDPR. The pure commercial interests pursued by the controller, albeit legitimate, still need to yield to the right to informational self-determination in accord with the reasonable exceptions of data subjects irrespective of their social roles. However, the current "harmony approach" in merchandising cases adopted by some German courts is flawed. For one, the direct reliance on the jurisprudence of the KUG needs a clear legal basis in the GDPR. As the reasonable expectations of the data subject would be the appropriated one, German courts should not apply §§ 22 and 23 KUG at the beginning in the ruling. For another, by resorting to the jurisprudence of the KUG German courts tend to ignore the specificity of the provisions in the GDPR, such as the principle of accountability and the "test grid" of Art. 6 (1) (f) GDPR. Furthermore, adopting the narrative of the EU data proception law does not mean quoting terms from the GDPR in any case. Exploration of their correct meaning, such as direct marketing, is indispensable to avoid exaggeration of the risks and harms of data processing in online communication.

Both advantages and disadvantages of the strict accordance with Art. 82 GDPR are highlighted in unauthorized merchandising cases. On the one hand, Art. 82 GDPR provides an impetus for enhanced protection for data subjects by facilitating a more data subjects-friendly recourse mechanism. For one, the principle of accountability and the data subject's rights increase the obligations of controllers both qualitatively and quantitatively. For another, Art. 82 GDPR not only expands the scope of damages but also indicates a high level of compensation following the principle of effectiveness and dissuasiveness. Yet the contested practice of assessing the damages undermines the importance of Art. 82 GDPR for data protection. The tendency towards some standard compensation for some typical infringements of the GDPR, such as infringements to the right to information, is beneficial for data subjects and expected to be recognized at the EU level.

On the other, the equivocal attitude of the GDPR towards the attribution of the commercial interests contained in personal data significantly

390 Vgl. Dix, in *Simitis, et al.,* Datenschutzrecht, Art. 20 Rn. 16.

devalues the material damages that the data subject can claim. Furthermore, the strong resistance of the EDPS towards the idea that personal data can be commercialized makes it more difficult to calculate the amount of compensation even when a data market exists factually. In this sense, the material damages cover the expenses for inquiry, evidence collection, and litigation but probably not the commercial interests contained in personal data exploited unlawfully by the controller according to Art. 82 (1) GDPR. Therefore, if the data subject suffers moral damages from the data processing, it is more likely he or she would be better-off at a smaller cost than the data subject who suffers merely material damages in merchandising. In this wise, faced with unauthorized merchandising, average data subjects would get more compensation than celebrities because the latter usually do not feel morally violated, unlike the former.

As a result, celebrities who are used to merchandising probably cannot be compensated properly under the GDPR, and there is a high probability that they will even receive nothing, even though their data are worth more proved by the established merchandising market.

4. Authorized merchandising under the GDPR

4.1 The applicability of Art. 9 GDPR in merchandising cases?

4.1.1 Specific protection for sensitive data

(1) The statutory requirements in Art. 9 GDPR

Rooted in Convention 108,[391] the GDPR distinguishes between (normal) personal data and "special categories of personal data" (sensitive data) and, in general, prohibits the processing of the latter from the outset (Art. 9 (1) GDPR).[392] Data controllers are allowed to process sensitive data if they meet one of the specific requirements listed in Art. 9 (2) GDPR as well as other requirements in the GDPR "in particular as regards the conditions for lawful processing".[393]

---

391 Art. 6 in Convention 108.

392 Art. 9 GDPR is born out of Art. 8 of the Directive 95/46.

393 Recital 51 of the GDPR clarifies the relation between Art. 9 (2) and 6 (1) GDPR by stating that "in addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular

Seemingly, conditions for processing sensitive data are more rigorous than normal personal data. For instance, Art. 9 (2) GDPR lacks a general clause like Art. 6 (1) (f) that allows private entities to process personal data for compelling legitimate interests after a balancing test.[394] A free pass deriving from contracts between data subjects and controllers under Art. 6 (1) (b) GDPR is also absent in Art. 9 (2) GDPR. Moreover, Art. 9 (2) (a) GDPR imposes higher requirements for the validity of consent. Besides the principle of lawfulness, obligations imposed on data controllers who systematically process sensitive data are intensified in quality and quantity. For instance, regulation of automated individual decision-making processing is stricter when sensitive data are involved (Art. 22 (4)), the obligation to conduct data protection impact assessments is seemingly mandatory (Art. 35 (3) (b)), and, of course, penalties for violations are aggravated (Art. 84 (5) (a)).

This higher-standard protection flows from the acknowledgment that processing of sensitive data is more likely to create substantial risks to fundamental rights and freedoms of individuals.[395] An expansion of the types of sensitive data is thus foreseeable as data technology advances.[396] For instance, genetic data is evaluated as sensitive data per se in Art. 8 of Directive 95/46 after more than a decade of Convention 108, while biometric data emerge in the list of sensitive data in Art. 9 (1) GDPR after another decade of Directive 95/46.

To strike a balance between flexibility and certainty, types of sensitive data prescribed in the EU data protection law are, albeit exhaustive, with elusive boundaries. It leads to the question of whether personal photos are considered sensitive data since sensitive information about the person

---

as regards the conditions for lawful processing." The opposing view advocates an exclusion of the application of Art. 6 (1) GDPR based on the principle lex speicilas, see Kampert, in *Sydow,* DSGVO: Handkommentar, Art. 9 Rn. 1.

394 Although Art. 9 (2) (g) provides an open-ended clause irrespective of fields, it specifically requires that the purpose of processing must be of public interest. Thus, it is in general inapplicable for private data controllers. Vgl. Weichert, in *Kühling/Buchner,* DSGVO/BDSG, Art. 9 Rn. 89.

395 The first sentence of recital 51 of the GDPR states, "Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms"; Petri, in *Simitis, et al.*, Datenschutzrecht, Art. 9 Rn. 1.

396 Cullagh, 2 Journal of International Commercial Law and Technology 190 (2007) (191).

depicted, including race (mental or physical), health status, etc., can be inferred from one's facial and physical appearance.

Two categories of sensitive data are contained in Art. 9 (1) GDPR. One refers to genetic and biometric data resulting from specific technical processing, which are per se sensitive data.[397] The other describes "data sources", from which sensitive information about racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, health, sex life, or sexual orientation can be inferred directly or indirectly, independently or in combination.[398] For instance, one's dressing accessories such as kippah, hijab or glasses, one's behaviors including participating in political, religious or LGBT social movements, or engaging in extreme sports are not informative about health or religious beliefs per se, but rather are considered sensitive data because they can reveal such information.[399]

Personal pictures are not biometric data in the first category. Although Art. 4 (14) GDPR lists "facial images" as an example of biometric data, they are not personal photos taken by normal cameras but rather special photos generated through a specific technical means in the sense of Art. 4 (14) GDPR, such as the facial image used in ID cards, passports, etc.[400] However, a personal photo can still be considered sensitive data in the second category if sensitive information about the person depicted can be revealed by his or her facial or physical features or even the context in the photo.[401]

---

397 *Weichert, DuD, 2017, 538 (540).*

398 Some scholars argue that the data "concerning" health, sex life, or sexual orientation builds another category of sensitive data, or is subjected to the same category of biometric data because it also refers to data that directly shows that information. See *Schneider*, ZD 2017, 303 (304); Albers/Veit, in *Brink/Wolff*, BeckOK Datenschutzrecht, Art. 9 Rn. 19. However, the definition of these data provided in Art. 4 (15) eliminates the semantic distinction between the terms "concerning" and "revealing". See *Matejek and Mäusezahl*, ZD, 2019, 551 (553); *Schneider/Schindler*, ZD, 2018, 463 (467); Ernst, in *Paal and Pauly,* DS-GVO BDSG, Art. 4 Rn. 109; Schulz, in *Gola,* DSGVO, Art. 9 Rn. 14; Schild, in *Brink/Wolff,* BeckOK Datenschutzrecht, Art. 4 Rn. 143.

399 *Reuter*, ZD, 2018, 564 (565); *Schneider/Schindler,* ZD, 2018, 463 (466f.).

400 Recital 51 of the GDPR; See Perti, in *Simitis, et al.,* Datenschutzrecht, Art. 4 Nr. 14 Rn. 9; *Klein,* Personenbilder im Spannungsfeld von Datenschutzgrundverordnung und Kunsturhebergesetz, S. 5.

401 WP29, Advice paper on special categories of data ("sensitive data"), Ref. Ares (2011)444105, 8.

(2) the academic controversy over the criteria

Scholarly literature agrees on a case-by-case analysis about the sensitivity of a photo.[402] However, the pivotal question lies in the details of the judgment inquiring about which factors play a role in concrete cases. Some scholars focus on the subjective purpose (*Auswertungsabsicht*) of data controllers.[403] According to this subjective approach, personal photographs are only regarded as sensitive data if the controller's purpose is to analyze sensitive information from them. However, in the view of the proponents of an objective evaluation, personal photographs reflecting facial features are normally considered sensitive data because they are objectively capable of revealing sensitive information.[404]

(3) Evaluation

Advantages and flaws in both propositions are evident. The subjective approach can effectively exclude data processing that poses no particular risk for data subjects by examining the purpose of the processing. At the same time, it lacks prominent legal support and is difficult to assess.[405] The objective approach enables the GDPR to intervene at an early stage, which is in line with the intention of the EU data protection law. From its inception, the EU data protection law has been cast widely to cope with technologies.[406] However, stemming from the blurred boundaries of "data sources", the objective approach would extend too far that it virtually provides a borderless pool so that non-sensitive data can trigger the stringent precautionary measures and renders the distinction between sensitive data and normal data obsolete.[407]

Based on the characteristics of data processing, the purpose of the data controller should not be excluded from assessing the capabilities of data processing in any case. One's skin color revealing the race is a thinking process conducted by human beings, which is not processing in the sense

402 *Matejek and Mäusezahl,* ZD, 2019, 551 (552).
403 Schulz, in *Gola,* DSGVO, Art. 9 Rn. 13; *Matejek and Mäusezahl,* ZD, 2019, 551 (552).
404 Schiff, in *Ehmann and Selmayr,* DS-GVO, Art. 9 Rn. 10.
405 Perti, in *Simitis, et al.,* Datenschutzrecht, Art. 9 Rn. 12.
406 Erdos, 26 International Journal of Law and Information Technology 189 (2018) (194).
407 *Matejek and Mäusezahl,* ZD, 2019, 551 (552).

of the GDPR. Data and processing cannot be conceptualized separately. A machine cannot "see" through pictures unless it has been mandated to and provided with the necessary assistance of manual tagging and persistent "learning". In other words, a machine, or an Artificial intelligence (AI) system can only identify and record the "hidden" sensitive information from the photo when it is programmed to do so.[408] The objective approach ignores the gap between data processing and human cognition.[409] Thus, the purpose of data processing cannot be left aside to determine whether the "data sources" are sensitive or not. It is true that "there is no trivial data", but this statement has a premise, namely, data processing technologies are making it easier and easier to analyze, integrate and store data, thereby significantly increasing the risk of people being exposed to unrestricted data collection.[410] Therefore, an overall assessment not only regarding data but also taking account of the context including the purposes, means, and impact of the processing is warranted.[411]

While the GDPR places great importance on the objective factors in terms of data processing technologies,[412] official documents of the EU data protection law and its legal resources consistently emphasize the rationale

---

408 Opposite opinion See *Reuter,* ZD, 2018, 564 (565). She argues that surveillance footage should be generally categorized as sensitive data. An introduction to how AI systems work through combining large sets of data with intelligent, iterative processing algorithms, See *Posner and Weyl,* Radical Markets: Uprooting Capitalism and Democracy for a Just Society, 214 et seq.

409 Vgl. *Bull,* Sinn und Unsinn des Datenschutzes, S. 13; *Lenk,* Der Staat am Draht, S. 33f.

410 BVerfG, NJW 1984, 419 - Volkszählung, para. 159.

411 Some scholars support a more radical teleological reduction by retrieving the fundamental rights and freedoms that provide the basis for the stringent protection for specific sensitive data. Thereby, the ambit of sensitive data would not extend too far. For instance, *Petri* suggests limiting the racial and ethnic origins in Art. 9 (1) GDPR in ethnic and racial minorities, such as Eskimo, to respond and guarantee its breeding human right against discrimination. See Petri, in *Simitis, et al.,* Datenschutzrecht, Art. 9 Rn. 16. This approach is not followed based on three main reasons among others. First, no official documents indicate such restrictive understanding that would substantially undermine the effectiveness of the GDPR. Secondly, this view is likely overly conservative, since profiling, social-sorting, and discrimination in employment, admissions, and price are not only among minorities. Finally, it does not solve the core issue in Art. 9 (1) GDPR, which revolves around a general understating of a whole category of data, namely the "sources data".

412 See Recital 26 of the GDPR: "To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for

under the specific protection of sensitive data: processing thereof poses significant risks and harms to the fundamental rights and freedoms of individuals.[413] On the one hand, since the development of data analytical technology is still in an embryonic stage, and even data controllers might not be fully aware of the capabilities of data processing technologies, their purposes could be elusive and thus the nature of personal data provides a definite and fixed criterion for judgment. On the other hand, the GDPR is not concerned with the protection of sensitive data per se, but with the impacts of data processing on human beings. This rationale is reflected more evidently in the risk-based rules in the GDPR, which directly employ the risk brought up by data processing as a benchmark to increasing the controller's responsibility instead of using the term sensitive data per se.[414] Thus, the category of sensitive is a sign of the existence of high risk, and if in fact the processing of sensitive data does not entail high risk, then exclusion becomes necessary.[415]

4.1.2 Conclusions

Here argues for a subjective approach to Art. 9 (1) GDPR. As the concern arising from the difficulty of determining the purpose of data controllers is

---

identification, taking into consideration the available technology at the time of the processing and technological developments."

413 WP29, Advice paper on special categories of data ("sensitive data"), Ref. Ares (2011)444105*; Council of Europe, Explanatory Report to the Convention for the Protection of individuals with regard to automatic processing of personal Data, Nr. 38, para. 43, "while the risk that data processing is harmful to persons generally depends not on the contents of the data but on the context in which they are used, there are exceptional cases where the processing of certain categories of data is as such likely to lead to encroachments on individual rights and interests"; OECD, The Explanatory Report The explanatory memorandum of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, No. 50 - 51, "the Expert Group discussed a number of sensitivity criteria, such as the risk of discrimination, but has not found it possible to define any set of data which are universally regarded as sensitive".*

414 For instance, Art. 24 (1), 25, 32, 33 and 35 (1) GDPR.

415 *Spies, ZD, 2020, 117; Fazlioglu, 46 Fordham Urban Law Journal 271 (2019); Ohm, 88 Southern California law review 1125 (2015); Simitis, Revisiting Sensitive Data, 1999;* Weichert, in *Kühling/Buchner,* DSGVO/BDSG, Art. 9 Rn. 23; Schulz, in *Gola,* DSGVO, Art. 9 Rn. 13; Different opinion See Schiff, in *Ehmann and Selmayr,* DS-GVO, Art. 9 Rn. 13, with a mere focus on the data per se.

not unreasonable, it further argues for an emphasis on the reverse burden of proof stemming from the principle of accountability.[416]

The reverse burden of proof stemming from the principle of accountability can effectively prevent circumvention of obligations when data controllers process personal images that might pose higher risks to data subjects. Possible measures are detailed documentation proving that no sensitive data is being collected, analyzed, or stored.[417] Plausible circumstantial evidence is also supported here; For instance, the processing of sensitive data is inconsistent with the business objectives. Also, controllers must take effective measures including privacy by default or design, such as separated storage and timely deletion to prevent and forbid further processing.

The subjective approach of Art. 9 (1) GDPR with an emphasis on the reverse burden of proof is already reflected in some German cases. In one case, the judgment excluded the surveillance footage from sensitive data despite the personal data recorded by the camera being at a high resolution and could reveal racial and ethnic origin (skin color, hair). The argument was that the controller was not interested in collecting the special category of personal data.[418] The other case was about a data controller who owns an online pharmacy. The court ruled that the controller must prove that it had neither the purpose nor the ability to process sensitive data to exclude the application of Art. 9 GDPR.[419]

In merchandising cases, the data processing regarding personal portraits generally attracts attention and resonates with consumers instead of collecting and analyzing sensitive information of the person depicted. As discussed in Part II Section 3.1.2 (1), the difference between merchandising and direct marketing is evident: photos are used to increase publicity, while the data processing concerned by the GDPR is purported to generate

---

416 The emphasis on the reverse burden of proof is often ignored, see *Schneider/Schindler,* ZD, 2018, 463 (467f.); Vgl. BVerfG, NJW 2008, 1505 - Automatisierte Kennzeichenerfassung, para. 66; Weichert, in *Kühling/Buchner,* DSGVO/BDSG, Art. 9 Rn. 22f.; *Matejek and Mäusezahl,* ZD, 2019, 551 (553).

417 For instance, Art. 24 GDPR orders the controllers to take reasonable and proportionate responsibilities when they adopt some new data technology aiming at analyzing data subjects, and creating significant risks for individuals. Vgl. *Veil,* ZD, 2015, 347.

418 VG Mainz, ZD 2021, 336 - DSGVO bei Kameras am Monitor, 337.

419 LG Dessau-Roßlau (3. Zivilkammer), GRUR-RS 2018, 14272 - Speicherung personenbezogener Daten beim Vertrieb apothekenpflichtiger Arzneimittel über Handelsplattform, para. 40f.

more information from photos. Taking the *landlady* case as an example, the magazine used erotic photos of the model to increase sales. Racial information may be inferable, but the magazine is not aimed at or even interested in this sensitive information.[420] It would not collect, analyze, or store sensitive information. Interestingly, despite the photos in the *landlady* case being pornographic and might be sensitive in daily life, they were hardly considered sensitive in Art. 9 (1) GDPR because they were staged photos and related to occupation.[421] Conversely, information regarding consumption of these magazines is likely sensitive data because it might tell one's sexual orientation.[422]

Following the subjective approach of Art. 9 (1) GDPR with an emphasis on the reverse burden of proof, merchandisers can exclude the application of Art. 9 GDPR by demonstrating that no sensitive information about the data subject's race, ethnic origin, or health status that could be revealed from the stage photos is processed in the sense of the GDPR. Feasible measures include detailed documentation concerning the content, means of processing, and business purpose. However, if the controller cannot convincingly prove that it does not process such information, or that sensitive information is already recorded, then it must find a legitimate justification from Art. 9 (2) GDPR.

For instance, when a party member uploaded pictures onto his fan page showing the data subjects' appearance in a political campaign, the *VG Hannover* should scrutinize the data processing under Art. 9 GDPR since the data subjects' political attribute was directly recorded online.[423] It also holds in users' merchandising scenarios concerning feedbacks of pregnancy products and drugs. As a result, when sensitive information is explicitly processed – collected, stored, made available online – in the meaning of the GDPR, Art. 9 GDPR and other relevant precautionary obligations should be applied to provide a high-level protection for individuals

420 In the same direction, see Schulz, in *Gola,* DSGVO, Art. 9 Rn. 15, stating that the processing of food and drinks in delivery services does not possess the intention to evaluate one's eating habit and drug addictions.

421 *Ehmann*, ZD, 2020, 65 (68).

422 Weichert, in *Kühling/Buchner,* DSGVO/BDSG, Art. 9 Rn. 42; Schiff, in, *Ehmann and Selmayr,* DS-GVO, Art. 9 Rn. 31; The opposite opinion without reason see, Schulz, in *Gola,* DSGVO, Art. 9 Rn. 14. Probably because a data processing operation or a clear intention to process such information lacks here.

423 Schnabel has expressed his concern for merchandising under the GDPR by forwarding a similar hypothetical case. See *Schnabel,* ZUM, 2008, 657 (661).

since the processing thereof is risk-prone as regards fundamental rights and freedoms of individuals.

4.2 Consent as the lawful ground for data processing under the GDPR

4.2.1 The collision of norms (Normenkollision) between the GDPR and the KUG

Although both the KUG and the GDPR use consent (*Einwilligung*) as a legitimate basis for merchandising/data processing, their understanding of consent diverges significantly. Under the KUG, consent can indicate non-binding acts of friendship (*Gefälligkeiten*) and binding promises in synallagmatic contracts.[424] As shown in Part I Section 3.1, German jurisprudence generally considers consent in a merchandising contract a legal act that cannot be withdrawn freely. Consent in the GDPR, however, is deemed to be freely revocable. Consent of the GDPR is only one connotation of consent according to German doctrine, and thus it cannot replace the various senses of consent under the KUG.

The supremacy of the EU law only indicates a precedence of the GDPR over the KUG when their application overlaps. Therefore, there is no basis for a comprehensive substitution of legal concepts.[425] In other words, the indication of the depicted person's wish needs to be judged according to the specific scenario, and the GDPR is authorized to determine whether such a disposal of personal data is permitted or not. After all, life is not performed according to the law; on the contrary, law needs to be adjusted to the needs of reality. Furthermore, the GDPR also agrees to determine whether the definition of consent is met based on the true meaning of the data subject, rather than focusing only on the term consent as such. According to the definition of consent in Art. 4 (11) GDPR, consent can be presented in various manifestations, such as a statement, a clear affirmative action, or a signed agreement. Thus, even if the data subject does not use the word consent, it does not automatically lead to the conclusion that

424 *Dasch,* Die Einwilligung zum Eingriff in das Recht am eigenen Bild, 68f.; Specht, in *Dreier/Schulze,* Urheberrechtsgesetz, § 22 KUG Rn. 19a.

425 About the collision of norms, see *Bienemann,* Reformbedarf des Kunsturhebergesetzes im digitalen Zeitalter, S. 103f.; Specht, in *Dreier/Schulze,* Urheberrechtsgesetz, Art. 22 KUG Rn. 16a und 35.

their intention to allow the data controller to process personal data is not revocable at any time in the sense of the GDPR.

Finally, this finding does not discriminate against the interests of the data subject because the controller bears the burden to inform the data subject about the legal consequence of her or his action according to the principle of accountability. In case of doubt, the data controller must demonstrate that the data subject wants to and agrees to conclude a contract rather than giving consent. Furthermore, the GDPR considers that contracts can only provide legitimacy for necessary data processing. If it goes beyond what is necessary, then the data subject can revoke their consent at any time.

4.2.2 Consent as the lawful ground in merchandising

(1) Conditions for the validity of consent and the consequence of omissions

As the "central hinge" of private data protection law,[426] consent is the "indication of the data subject's wishes", which can be given by "a statement or by a clear affirmative action" according to Art. 4 (11) GDPR. In this sense, consent is a unilateral declaration of the data subject that legitimizes the data processing conducted by the controller.

The GDPR imposes stringent requirements on consent to ensure that the data subject genuinely executes the right of informational self-determination.[427] Art. 4 (11) GDPR requires consent to be "freely given, specific, informed, and unambiguous". While Art. 7 (2), recitals 32 and 42 prescribe detailed conditions for "specific" and "unambiguous", Art. 13 (1) and (2) GDPR have listed the information the controller shall provide when it collects the personal data from the data subject directly to facilitate the requirement of "informed". Furthermore, Art. 7 (3) GDPR requires that consent must be freely revocable. The free revocability of consent is one of the major innovations in the EU data protection law to make data controllers always walk on thin ice. Data subjects can thus "vote with their feet" and render future processing operations unlawful.

Moreover, it can also mitigate the adverse consequences of wrong choices to some extent because data subjects can withdraw consent freely when

426 Vgl. Stemmer, in *Brink/Wolff*, BeckOK Datenschutzrecht, Art. 7 Rn. 19.
427 Buchner/Petri, in *Kühling/Buchner*, DSGVO/BDSG, Art. 6 Rn. 17.

they become aware of their cognitive deficiencies. It means that the revocability of consent must be free from negative consequences for the data subject and can be executed anytime. Some scholars argue it is because of the bound cognition of human beings, especially in the face of big data but refuse to confine its application within this scenario.[428] While the cognitive problems might constitute partly the justification, it is still necessary to look at the source of law. Art. 8 of the Charter places high value on data subjects' the control over personal data. Thereby, the free revocability of consent is devised to render the lawfulness of data processing entirely contingent on data subjects' willingness in permitting or objecting data processing.

The GDPR ensures the voluntariness of consent through the so-called prohibition of coupling (*Kopplungsverbot*) in Art. 7 (4) GDPR. It requires that the performance of a contract, especially the provision of a service, should not depend on the consent to which the data processing is not necessary for the provision of that service. For instance, if an App for flashlight makes the consent to read the data subject's contact book indispensable for using that app, it violates the prohibition of coupling. However, it is rightfully argued the name of the prohibition is exaggerated because Art. 7 (4) GDPR only requires taking "utmost account" instead of prohibiting coupling entirely.[429] As suggested by recital 43, the coupling issue acquires more attention when there is structural inequality between the data subject and controller because it is more likely that the data subject would fail to express his or her genuine wishes due to dependency on the service.

Seemingly clear, these requirements are particularly problematic in practice, coupled with the legal consequence.[430] Art. 7 GDPR is of particular importance in evaluating the consequences for failing to meet the conditions for valid consent because it prescribes the conditions and the consequence flowing from a violation – (partial) invalidation of the consent according to Art. 7 (2) GDPR.[431] The prevailing view in the academic community argues for differentiation according to the type of the omitted

428 Ibid., Rn. 34 und 38.

429 Vgl. *Engeler*, ZD, 2018, 55 (58f.); Schulz, in *Gola,* DSGVO, Art. 7 Rn. 26; *Sattler,* in: *Pertot, Rechte an Daten*, 49 (75). However, some judiciary judgments tend to recognize an absolute prohibition of coupling, See OGH Wien, ZD 2019, 72, Rn. 47; *Pertot*, Zeitschrift für das Privatrecht der Europäischen Union, 2019, 54.

430 *Brink/Wolff,* BeckOK Datenschutzrecht, Rn. 94.

431 Stemmer, in ibid.Art. 7 Rn. 93.

information.[432] If the missing information is so important that it would affect the right to self-determination of the data subject seriously, then consent is invalid. Otherwise, invalidation of consent is uncalled for because it exceeds the protective purpose of Art. 7 (2) GDPR since the data subject would exercise the informational self-determination in the same way. Nevertheless, it must be distinguished from the possible administrative fines for controllers due to incompliance.

Among all, two requirements are deserving special attention in the context of merchandising. One is the voluntariness of data subjects, and the other is the omission of the notification about the revocability of consent.

Some indicators address the voluntariness of consent under the GDPR including the pre-relationship between the data subject and controller,[433] the consequence for refusing to consent,[434] and the notification of the anytime revocability of consent.[435] For instance, if the data subject is dependent on the controller or the data processing conducted by the controller as in an employment relationship, the controller must formulate the declaration in a written and independent form from the employment contract to facilitate the evaluation of the voluntary nature of consent.[436] Moreover, the controller shall prove that consent is not coerced in any sense if a structural inequity exists.[437]

The most decisive indicator is that there is no adverse consequence for refusing to consent.[438] Some scholars further demand that there should not be any beneficial consequences either.[439] However, this approach is too

---

432 Buchner/Kühling, in *Kühling/Buchner,* DSGVO/BDSG, Art. 7 Rn. 59; Schiff, in *Ehmann and Selmayr,* DS-GVO, Art, 7 Rn. 58; *Ernst*, ZD, 2017, 110 (112).

433 Recital 43 GDPR; *Gola and Schulz*, RDV, 2013, 1(6); *Pötters*, RDV, 2015, 10 (15).

434 See WP29, Guidelines on consent under Regulation 2016/679, 17/EN, 7.

435 WP29, Opinion 8/2001 on the processing of personal data in the employment context, WP48, 3.

436 Ibid., 3. It makes a strict distinction between data processing that is necessary for the establishment, continuation, and termination of the employment relationship and confines consent solely to the latter scenario.

437 It is noteworthy that the provision was originally envisaged in Art. 7(4) GDPR-E that consent is *per se* invalid if there is a "significant imbalance" between the data subject and the controller, such as in an employment relationship. However, this *proviso* has been deleted because the EU Parliament feared that this exclusion would be too broad. See European Commission, Proposal for a General Data Protection Regulation, COM(2012) 11 final, recital 34.

438 See WP29, Guidelines on consent under Regulation 2016/679, 17/EN, 7. It gives an example that the employees who refuse to consent are provided with necessary assistance so that their work would not be affected.

439 *Ernst*, ZD, 2017, 110 (112).

general to agree with. Admittedly, it might make sense when the benefit is career-related such as promotions. But monetary consideration for merchandising in a situation like the *company-advertising* case is reasonable and cannot be used as a reason to deny voluntariness. Otherwise, it virtually demands that all employees be completely altruistic for the company's commercial interests in merchandising scenario. Lastly, the WP29 also emphasizes the notification of the anytime revocability of consent to sustain "a genuine free choice" of an employee.[440] All in all, the more prominent the structural inequity between the data subject and controller is, the more additional measures the controller needs to take to demonstrate the voluntary nature of the data subject.[441]

It is questionable whether the omission of the notification about the revocability shall lead to the invalidation of consent. Some scholars find the compulsory notification incompatible with everyday life scenarios. They argue that it seems preposterous that a photographer must have a sign on him stating all necessary information about data processing and the revocability of consent to take pictures at a party.[442] This argument has some merit because the context of data processing imaged by the GDPR is most likely to be data processing in a network environment where anytime revocable consent has substantial practical implications. Foremost importantly, data subjects relying on consent shall no longer be intimidated by the complexity and length of the privacy policy drafted by controllers, as they can withdraw consent whenever they change their minds. However, this counterargument seems superfluous.

In practice, official organizers acquire attendees' consent in advance for data processing (for taking photographs) in writing with the information including the purpose, means of processing, and revocability of consent. Admittedly, this is a change based on the GDPR compliance requirements, but such a change is progress in light of the data protection law and does not give rise to peculiar consequences. Moreover, the household exception in the GDPR is applicable to private parties. Secondly, according to the

---

440 WP29, Opinion 8/2001 on the processing of personal data in the employment context, WP48, 3.

441 It is noteworthy that the provision was originally envisaged in Art. 7(4) GDPR-E that consent is *per se* invalid if there is a "significant imbalance" between the data subject and the controller, such as in an employment relationship. This *proviso* has been deleted because the EU Parliament feared that this exclusion would be too broad. See European Commission, Proposal for a General Data Protection Regulation, COM(2012) 11 final, recital 34.

442 The instance and the argument for the incompatibility, see *Ernst*, ZD, 2020, 383.

explicit wording of Art. 7 (3) GDPR, the notification regarding the revocability of consent must be "prior to giving consent".[443] While it has been argued that the information about the revocability of the consent is only needed when it is necessary "to ensure fair and transparent processing" according to Art. 13 (2) (c) GDPR,[444] this interpretation is uneasy to apply due to tautology and the inherent abstractness of the concept of "fair". Moreover, Art. 13 (2) (c) GDPR puts more emphasis on the notification about the *ex-nunc* effect of a withdrawn consent instead of the notification about the revocability per se. Finally, limiting the scope of the GDPR to the online environment or large data controllers lacks a legal basis.

Furthermore, it is essential to notice that either the consent can be withdrawn at any time or withdrawal is allowed (similar to a binding contract). When the revocability of consent is informed, the data subject can exert his or her control over the operations of data processing; when the binding nature of the contract is made clear, it warns the data subject to think carefully before he or she gives a binding commitment. Against this backdrop, without any reference to the revocability of consent, the data subject is deprived of either the control over personal data or the opportunity to think carefully. Given the imbalance of power in employment relationships, there is a clear risk that the data subject would be hoodwinked into a situation where they thought the consent was revocable at any time, but it is not in reality. Consequently, the central factor of the judgment regarding the consequence of failing to notify the revocability is contingent on whether the omission has led the data subject to a wrongful perception that ultimately affects the execution of the right to informational self-determination.

(2) Applying Art. 6 (1) (a) GDPR in authorized merchandising cases

i. Merchandising contracts no longer binding

The most obvious and troublesome issue in merchandising is the free revocability of consent anchored in Art. 7 (3) GDPR. In this sense, mer-

443 Vgl. Stemmer, in *Brink/Wolff*, BeckOK Datenschutzrecht, Art. 7 Rn. 55.
444 Kamlah, in *Plath*, DSGVO/BDSG, Art. 13 Rn. 16.

chandising contracts are no longer binding since data subjects can revoke consent at any time and must be exempt from liability.[445]

When controllers remain equivocal about the revocability of consent by neither excluding nor including it in merchandising cases, it constitutes a violation of Art. 7 (3) GDPR, and the legal consequence of this violation is dependent on how serious the self-determination of the data subject is harmed. While one would argue that since a data subject signs such a contract while mistakenly thinking it was "binding", the data subject would have carefully examined the situation before making the decision. If the voluntariness of the choice can be established, the fundamental right of the data subject in Art. 8 of the Charter to make informed decisions about data processing did not seem to be undermined. In short, a violation existed but no harm was done. However, this argument is ill-grounded. Consent is known to enhance control of the data subject as it makes the legality of data processing always dependent on the willingness of the data subject. The data subject can revoke consent anytime and renders data processing void *ex nunc.* Without notification, the data controller "tricked" the data subject into a situation where they wrongly relinquished the control they could have achieved during the processing. Even though the data subject has carefully considered his choice, depriving the right to withdrawal under the guise of a contract was illegal from the outset. In other words, upon deliberate silence, the controller misguided the data subject from the choice that is beneficial for him but undesirable for the controller.

The notification is even more indispensable as the anytime revocability of consent is a rather innovative concept forwarded by the EU data protection. Furthermore, as disclosed in Part I Section 3.1, consent in merchandising scenarios may be binding in Germany. The German court has rejected the data subject's request for withdrawal of consent resorting to balancing interests under § 241 BGB.[446] It was the exact opposite of the GDPR, according to which the execution of the withdrawal of consent should not be contingent on a balancing of interests,[447] and be as simple as the grant of consent and at any time freely (Art. 7 (3) GDPR). Thus,

---

445 *Westphalen and Wendehorst*, BB, 2016, 2179 (2185f.) Langhanke and Schmidt-Kessel, 4 Journal of European Consumer and Market Law 218 (2015) (221f.); *Sattler*, JZ, 2017, 1036 (1038f. und 1043f.); *Specht*, JZ, 2017, 763 (766ff.).

446 BAG, GRUR 2015, 922 - Veröffentlichung von Arbeitnehmer-Bildnissen zu Werbezwecken, Rn. 38

447 Vgl. Klement, in *Simitis, et al.*, Datenschutzrecht, Art. 7 Rn. 91, mentioning the exact case here and arguing for a different result than the BAG; *Spelge*,

the emphasis on the duty to inform stemming from the principle of transparency according to the GDPR is indispensable to implementing the high-level protection for personal data.

Without highlighting the notification of the unique characteristic of consent under the GDPR, it virtually allows the controller to benefit from its ambiguity. Even though the controller fails to address the revocability of consent, the controller could argue that no confusion has been aroused by its omission as long as the data subject claims revocability. As a result, the controller can enjoy a *de facto* stable position as if it relied on a contract. Lastly, it is the controller's burden to prove that the data subject is not confused by its wrongdoings, which could hardly be met in this situation because the data subject suffered from confusion. Thus, the declaration given by the data subject is likely invalid when the controller fails to notify the revocability of consent at the outset in merchandising cases, and the data processing is thus unlawful according to Art. 7 (2) and (3) GDPR.[448]

ii. Agency-merchandising contracts at issue

Besides, it is arguable whether consent given by a model in an agency-merchandising contract can legitimize merchandising by companies who have not negotiated with the model but the agency. Regarding the data protection law, it concerns the ambit of consent: Can consent be declared to one controller extent to data processing conducted by third controllers who may or may not be explicitly mentioned in the consent?

Under the GDPR, companies who process the personal data to advertise their products are not processors who outright implement the agency's instructions (Art. 4 (8) GDPR). Instead, they are joint controllers with the agency because they make joint decisions with the agency about when, how, and for what purpose to process the personal data of the data subject (Art. 4 (7) GDPR). Thus, third controllers also need to rely on Art. 6 (1)

DuD, 2016, 775 (781); Laue, in *Laue, et al.,* Das neue Datenschutzrecht in der betrieblichen Praxis, § 2 Rn. 14.

448 Art. 88 GDPR provides the margin of appreciation for the Member States in the employment context, but it aims to "ensure the protection of the rights and freedoms in respect of the processing of employees' data". Thus, rules reducing the controller's (employer's) duty to inform do not suit the purpose of Art. 88 GDPR. Vgl. Riesenhuber, in *Brink/Wolff,* BeckOK Datenschutzrecht, Art. 88 Rn. 1.

(a) GDPR, though they are usually not explicitly mentioned in the consent according to an agency-merchandising contract.

On the one hand, the wording of Art. 6 (1) (a) GDPR – the "data subject has given consent to the processing of his or her data for one or more specific purposes" – suggests that the recipient of the consent is not necessarily the controller. This neglect of the recipient is not a mistake of legislators for several reasons. Firstly, Art. 22 (2) (a) GDPR that explicitly requires the counterparties indicates that legislators do give clarity when they need to limit the boundaries of lawful grounds.[449] Secondly, Art. 9 (2) (e) GDPR even provides that active and manifest disclosure by the data subject is a legitimate reason for any controller to process sensitive data. Therefore, the specification of identities of third controllers in merchandising cases is not decisive for them to invoke the consent stated in agency-merchandising contracts according to the verbatim reading of Art. 6 (1) (a) GDPR. On the other hand, this reading would lead to a borderless application of Art. 6 (1) (a) GDPR because the possibility of not knowing the identity of third controllers is not surreal. This fear is even more justified in scenarios of processing sensitive data as any controller can invoke Art. 9 (2) (e) GDPR to justify their processing.

The wording of Art. 6 (1) (a) GDPR leaves room for its application of third controllers. However, the high-level data protection objective may need to be achieved by implementing a relatively strict interpretation of the consent in light of the principles of transparency and data minimization in the GDPR. Therefore, how the consent is drafted in an agency-merchandising contract is vital. Above all, the consent must specify that the data subject agrees to further data processing in terms of collecting, editing, granting sub-licenses, and transmitting for advertising, endorsement, etc., for business partners according to the agency's arrangement. Moreover, to prove that the processing does not exceed the ambit of the consent, try to clarify the business partners if possible, or state the type and area if not. For instance, in the *landlady* case where an agency-merchandising contract was concerned, the data subject gave explicit consent to processing her images by magazines without their identities being determined. Furthermore, she considered the identity information unimportant by stating on the telephone that she was willing to authorize any publications as long as the remuneration reached a certain threshold. In other words, the data subject actively and voluntarily gave up the right to information granted by the

449 Art. 22 (2) (a) GDPR specifies "a contract between the data subject and a data controller".

GDPR to some extent. Though the act was invalid under the GDPR as data subject's rights are not waivable,[450] one could argue that as a professional model, the data subject had a general understanding of the identities of third controllers in the industry. Thus, the lack of such information would not affect her exercise of the right to informational self-determination.

Nevertheless, it is highly recommended and almost imperative for the agency and third controllers to notify the data subject when personal data has been transmitted, according to Art. 14 (1), (2) and (3) (a) GDPR. Failure in the notification would constitute a violation that may not invalidate the consent but lead to an administrative fine under Art. 83 GDPR or damages according to Art. 82 GDPR.

iii. Rigorous conditions for validity of consent

The issue above implies another problem in applying Art. 6 (1) (a) GDPR in merchandising, i.e., data processing for merchandising is likely to be unlawful because of these rigorous conditions for validity prescribed by Art. 4 (11) and 7 GDPR. It holds for both merchandising contracts, namely the standard merchandising agreement and the agency-merchandising agreement.

While scholars argue that insufficient information does not automictically lead to invalidation of consent that renders the processing unlawful *ex tunc*, it is mainly contingent on the nature and content of the information omitted. Business practices do not welcome great uncertainty. Nevertheless, the omission of the obligation to provide information is not uncommon in merchandising because it is a mature business, and thus some information is self-explanatory or not crucial to both parties so that it would not be included in contracts. For instance, one may find that no information about the presentation and duration of the publication in the *landlady* case was discussed by the data subject – the model and the controller – the photographer.[451]

Similarly, in the *company-advertising* case, the content, means, and duration of data processing in the declaration drafted by the controller were stated abstractly according to Art. 13 (2) (a) and (b) GDPR, especially considering that the company's website was not online at the time of the data

450 Dix, in *Simitis, et al.*, Datenschutzrecht, Art. 12 Rn. 6.
451 OLG München, NJW-RR 1990, 999 - Wirtin.

subject's signature.[452] They were not an issue under the German law[453] but is controversial under the GDPR. It can be submitted in the *landlady* case that the insufficiency was not detrimental because the data subject implied those conditions by requesting relatively high royalties and thus would not exercise the right to information self-determination oppositely because of the lack of such information.[454] In the *company-advertising* case, the online distribution neither exceeded the scope of the declaration literally nor was beyond the reasonable expectation of the data subject. The company's promotion had clear relevance to the establishment of the company's website, and the data subject did not bring any question about the means or purposes of the data processing before, during, and after the production of the footage. Nevertheless, administrative fines are conceivable. The lack of clarity regarding data storage could arguably constitute a significant problem according to the principle of storage limitation in Art. 5 (1) (e) GDPR because an indefinite data storage increases the risk of data leakage and thereby poses significant risks to the fundamental rights and freedoms of data subjects. Art. 34 GDPR also requires a default rule on (semi-)automatic deletion of data when the processing is no longer necessary in honor of the default privacy.

iv. The voluntariness of consent given by young models?

In addition to the insufficiency of notification, the solid structural inequity between young models and powerful agencies is another issue related to the voluntariness of consent. Models are not stars when they start their ca-

452 See BAG, GRUR 2015, 922 - Veröffentlichung von Arbeitnehmer-Bildnissen zu Werbezwecken, Rn. 2.

453 For instance, it is well established in a similar case in Germany that the presentation of erotic photos should not be in a manner that would violate the personality of the model unless the model gives explicit consent. See LG Frankfurt/Main, 30.05.2017 - 2-03 O 134/16 - Stinkefingers.

454 One may argue that the storage of her data was necessary because the publication was likely to get that much remuneration. Consequently, if high payouts are only possible in the first 5 years according to the commercial practice, then the permissible duration should be limited to 5 years. Deleting the data after five years is advisable in accord with the GDPR. The ambiguity of the agreement did not lead to the invalidation of the contract because the data subject has already known the information that belongs to common knowledge in that practice, and thus the omission of such information does not affect the rational judgment of the data subject.

reers. However, like the aforementioned "*stink fingers*" case demonstrates, many young models would take (nude) photos for exposure against no remuneration. Their voluntariness in giving consent to such data processing is not beyond doubt.

It is noteworthy that models voluntarily choose the lifestyle to embrace publicity and glamour, and data processing is the inevitable cost. The necessity of data processing for merchandising precludes the application of the prohibition of coupling. Moreover, the competition among agencies and photographers is also intensive, making information asymmetry less prominent. Therefore, it argues that while the dependency of (young) models on agencies should not be underestimated, it should not be overestimated. After all, none of the data subjects challenged this point even in the "*stink fingers*" case and the *company-advertising* case where an employment relationship existed.

Nevertheless, the voluntariness of especially young models against powerful agencies in some agency-merchandising contracts requires a particular examination. As briefly mentioned in Part I Section 3.2.2 (4), the quasi "slave contracts" between young molders who are mainly teenagers and agencies speak strongly for deploying the indicators proposed above for assessing the voluntariness of an employment relationship here to ensure the voluntariness of data subjects. Therefore, it seems important for controllers to prove that no negative consequence follows the refusal of the data subject, and they have notified the revocability of consent to sustain a genuine free choice of the data subject.

However, these two indicators are hardly applicable in merchandising business because the data processing is necessary for their publicity, and once again, the revocability of consent is troublesome in merchandising.

4.2.3 Conclusions

Art. 7 and 4 (11) impose rigorous conditions for validity of consent in Art. 6 (1) (a) GDPR. It enhances the protection of data subjects coupled with the principle of accountability. Controllers must comply with the obligation to provide sufficient and precise information and enable data subjects to withdraw consent at any time. Failure to meet the conditions puts the validity of consent in question. Through the sword of Damocles hanging over controllers, the revocability of consent warns of the unstable legal status and urges controllers to safeguard the rights and interests of the data subject adequately.

Consent in Art. 6 (1) (a) GDPR can legitimize the data processing in authorized merchandising cases but raises many difficulties that seem insoluble.

The most significant one is its free revocability in Art. 7 (3) GDPR contradicts the principle of *pacta sunt servanda* in merchandising contracts. Seemingly, it might enhance the controller of the data subject over personal data by withdrawing consent anytime. It is a deterrent for data controllers as they lose the stable legal status for data processing. Merchandisers would not make significant and long-term investments, which would, in return, affect the career development of the data subject in merchandising. Moreover, merchandisers are obligated to notify the free revocability of consent before the data processing because they have to prove that the data subject was not misguided by the declaration. Otherwise, merchandisers are likely liable for seriously affecting the exercise of the right to information self-determination of the data subject. The omission of this notification would possibly render consent invalid under Art. 7 (2) and (3) GDPR.

Furthermore, the application of consent in agency-merchandising agreements is problematic. While the wording of Art. 6 (1) (b) GDPR leaves room for its application to third controllers that have not been stated in the consent, the agreements must be carefully drafted to include the further data processing into the ambit of the consent. Some ambiguity in consent regarding the duration and presentation of personal images would not be a significant problem for the legitimacy of data processing as it is not detrimental to the exercise of the right of informational self-determination of the data subject. Lastly, the indicators suggested by the WP29 to assess the voluntariness of consent can hardly be supported in merchandising cases even when a severe structural inequity between young models and powerful agencies exists.

It concludes that the consent envisioned by the GDPR brings insoluble difficulties for authorized merchandising. It not only deviates from models' expressed willingness to establish a binding contract with merchandisers but is also likely to invalidate their genuine willingness due to the strict conditions for validity. More importantly, the legal regulation of consent in the GDPR cannot effectively protect models, including the young and powerless ones, even though it advocates a high level of data protection. Nevertheless, controllers are strongly advised to specific contractual terms to avoid unnecessary legal disputes. Moreover, they must ensure that they have informed every detail listed in Art. 13 (1) and (2) GDPR to be exempt from administrative fines according to Art. 83 GDPR.

4.3 Contracts as the lawful ground?

4.3.1 Contracts as the lawful ground in merchandising

(1) The ambit of Art. 6 (1) (b) GDPR

Art. 6 (1) (b) GDPR presents a mixture of private autonomy and legal obligation.[455] Whereas contracts amount to the most critical and common manifestation of private autonomy in civil law,[456] data subjects are obliged to provide personal data for processing according to the contract. Thereby, Art. 6 (1) (b) GDPR allows the controller to obtain a stable data processing position while respecting the autonomy of the data subject's willingness.

Since Art. 6 (1) (b) GDPR legitimizes data processing that "is necessary for the performance of a contract to which the data subject is party", two requirements are imposed to limit its ambit: The necessity between the data processing and the performance of a contract, and the data subject as a party to the contract. The performance of a contract is broadly understood as including primary performance obligations, secondary contractual obligations related to the primary performance and processing in the context of the conclusion, amendment, and performance of a contract.[457] The mainstream opinion is to limit the requirement of necessity only to accessory types of data processing for the performance of a contract, such as collecting and using a buyer's address to perform a delivery service.[458] In other words, Art. 6 (1) (b) GDPR is applicable only if the data subject and

---

455 *Metzger*, AcP, 2016, 817 (825f.).

456 Buchner/Petri, in *Kühling/Buchner,* DSGVO/BDSG, Art. 6 Rn. 26.

457 Instead to cite many, see Albers/Veit, in *Brink/Wolff,* BeckOK Datenschutzrecht, Art. 6 Rn. 43

458 KG Berlin, DuD 2019, 301 - Zahlreiche Datenschutz-Klauseln von Apple rechtswidrig (303). It ruled that data processing for purposes, such as product improvement or advertising was not necessary for the performance of a contract within the meaning of Art. 6 (1) (b) GDPR; BKartA, BeckRS 2019, 4895 - Marktbeherrschung, Facebook, Rn. 671f.; *Wendehorst and Graf v. Westphalen*, NJW, 2016, 3745 (3747); *Westphalen and Wendehorst,* BB, 2016, 2179 (2184f.); *Tavanti,* RDV, 2016, 295 (296); *Bräutigam*, MMR, 2012, 635 (640); *Funke,* Dogmatik und Voraussetzungen der datenschutzrechtlichen Einwilligung im Zivilrecht, S. 271; Schantz, in *Simitis, et al.,* Datenschutzrecht, Art. 6 Rn. 32f.; Buchner/Petri, in *Kühling/Buchner,* DSGVO/BDSG, Art. 6 Rn. 39f.; Plath, in n *Plath,* DSGVO/BDSG, Art. 6 Rn. 25; Heberlein, in *Ehmann and Selmayr,* DS-GVO, Art. 6 Rn 13; Schulz, in *Gola,* DSGVO, Art. 6 Rn. 38, and especailly 40; Probably, Frenzel, in *Paal and Pauly,* DS-GVO BDSG, Art. 6 Rn. 14.

the controller have entered into or are about to enter into a contract whose primary performance is not data processing.

In this wise, Art. 6 (1) (b) GDPR is notably excluded from application in scenarios where personal data has been commercialized to some extent, such as the model of "data against service": It mainly describes the situation where data subjects allow controllers to process personal data in order to get "free" services provided by controllers with the cost of being exposed to targeted ads.[459] This conclusion is also drawn in the EPDB's *Guidelines* in interpreting the applicability of Art. 6 (1) (b) GDPR in the online environment. While the EPDB's *Guidelines* do not confine Art. 6 (1) (b) GDPR to accessory types of data processing, such as electronic archiving, collection of payments, etc., it does argue that data subjects can only give revocable consent to data-driven controllers, such as YouTube, for "free" services because their pursuit of free-of-charge does not belong to the genuine purpose of the service required by data subjects.[460]

One of the reasons argued by scholars is that since personal data is treated as quasi-consideration for the use of such service, and users may also pay monetary consideration, the choice to collect personal data is simply a choice of the controller/service provider, and is thus by no means necessary; The more far-reaching reason is the reduction of the applicable scope of Art. 6 (1) (b) GDPR is decisive to prevent circumvention of Art. 6 (1) (a) GDPR.[461]

Conceivably, if Art. 6 (1) (b) GDPR would legitimize the data processing as the primary performance of a contract, the data-driven controllers who collect and exploit personal data in large quantities would be encouraged

---

459 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. Instead to cite many, see *Schmidt*, Datenschutz als Vermögensrecht: Datenschutzrecht als Instrument des Datenhandels, 58f.; Abundant examples and analysis, see *Voigt*, Die datenschutzrechtliche Einwilligung, „Datenfinanzierte Geschäftsmodelle" (Data-financed business models), 171f.

460 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.

461 For instance, Schantz, in *Simitis, et al.*, Datenschutzrecht, Art. 6 Rn. 33; *Westphalen and Wendehorst*, BB, 2016, 2179 (2184); Langhanke and Schmidt-Kessel, 4 Journal of European Consumer and Market Law 218 (2015) (220); *Sattler*, JZ, 2017, 1036 (1040); 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).

to include the commercial use of personal data in the standard contracts drafted by themselves. Thereby, data-driven controllers, such as Facebook, Alphabet, Tiktok, Baidu, etc., could replace the anytime revocable consent with binding contracts signed by data subjects. As these controllers always present commercial purposes independent from the data subject's purpose in processing personal data, they would make the data processing stated in the contract as borderless as possible (in terms of content, manner, purpose, and time).[462] Coupled with the facts that data subjects seldom read the privacy policy provided controllers and controllers always take advantage of data subjects' inattentiveness or lack of time,[463] the high-level data protection promised by the GDPR by enhancing the control over personal data would be an illusion. Moreover, as Art. 6 (1) (b) GDPR does not require the data processing must be conducted by the controller who concluded the contract with the data subject, it is well argued that its application in contracts containing sub-licensing terms would render the lawful ground borderless.[464]

Moreover, one can make a clear distinction between the applicability of Art. 6 (1) (a) and (b) GDPR. Some scholars convincingly argue that the contract in the GDPR should also include unilateral legal acts (*einseitige Rechtsgeschäfte*), for instance, the promise of a reward for the performance of an act (*Auslobung*),[465] even though the EU legislation, ECJ decisions as well as Art. 4:102 (1) ACQP understand contract must contain an offer and an acceptance of that offer.[466] In this scenario, it seems unreasonable that the data subject, on the one hand, expressed his willingness to offer a

462 See *Westphalen and Wendehorst*, BB, 2016, 2179 (2184).

463 *Solove*, The digital person, 44 et seq.

464 See *Sattler, in: Pertot, Rechte an Daten*, S. 69f. More details about this argument see Part IV Section 4.

465 For the application in unilateral legal acts, see Schulz, in *Gola*, DSGVO, Art. 6 Rn. 29; Schantz, in *Simitis, et al.*, Datenschutzrecht, Art. 6 Rn. 16. Despite the contract being an autonomous concept, the GDPR does not impose any rules on the formulation of contracts. See Schiff, in *Ehmann and Selmayr*, DS-GVO, Art. 7 Rn. 29; *Schantz* argues that the conclusion of a contract thus has to be answered by national contract law in the absence of unified contract law at the EU level. Schantz, in *Simitis, et al.*, Datenschutzrecht, Art. 6 Rn. 21.

466 CJEU, Rudolf Gabriel, C-96/00, para. 48-49; *Schulze and Zoll*, European Contract Law, Chapter 3, para. 64-65. However, from another angle, one could argue that the declaration given by the data subject is an offer, and the contract concludes when the controller accepts the offer. See *Ohly*, "Volenti non fit iniuria": die Einwilligung im Privatrecht, S. 171f. Binding consent to a certain recipient is the same as a contract based on doctrinal arguments in German law.

reward to anyone who has achieved the result but, on the other hand, does not allow the person to carry out the corresponding data processing.[467] However, in this wise, the distinction between contract and the anytime revocable consent in Art. 6 (1) (a) in combination with Art. 7 (3) GDPR would be blurring. For this precise reason, some scholars contest this reading of the contract in Art. 6 (1) (b) GDPR,[468] but they cannot solve the aforementioned unreasonable result. If the data subject intends to improve the legal position of the public by expressing a binding will, there is little reason to deny the resulting reliance interest in holding the improved legal position.[469] The dominant opinion solves this problem. By confining Art. 6 (1) (b) GDPR within the data processing that is auxiliary to the performance of the contract, Art. 6 (1) (b) GDPR is applicable regardless of whether the contract consists of a unilateral commitment or bilateral declaration of will, as long as its primary performance is not data processing.[470]

(2) Art. 6 (1) (b) GDPR inapplicable to authorized merchandising

Merchandising contracts are, in essence, a form of commercialization of personal data. The main performance of the person depicted in that contract is to give consent under the KUG to the merchandiser regarding the exploitation against license fees. Thus, it is impossible to apply Art. 6 (1) (b) GDPR to merchandising contracts according to the mainstream opinion.[471]

---

467 Vgl. Schantz, in *Simitis, et al.*, Datenschutzrecht, Art. 6 Rn. 15; *Buchner*, Informationelle Selbstbestimmung im Privatrecht, S. 257.

468 See Buchner/Petri, in *Kühling/Buchner*, DSGVO/BDSG, Art. 6 Rn. 28.

469 Vgl. *Ohly*, "Volenti non fit iniuria": die Einwilligung im Privatrecht, S. 174.

470 Conditional denial of its application in unilateral acts, see Albers/Veit, in *Brink/Wolff*, BeckOK Datenschutzrecht, Art. 6 Rn. 42.

471 The view that Art. 6 (1) (b) GDPR cannot be applied to merchandising contracts, or at least it is highly questionable, see *Sattler, in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance – Contract Law 2.0?*, 225 (237); *Schnabel*, ZUM, 2008, 657 (661). On the contrary, *Bunnenberg* argues for an unobjectionable application of Art. 6 (1) (b) GDPR in merchandising scenarios because, under the dogmatics of the civil law, the merchandiser has a protected reliance interest in holding a binding nature and stability of the legal relationship, which overrides the data subject's interest in revocation. While this result is agreeable, it ignores the EDPS' s resistance to the commercialization of personal data and seems to omit a necessary explanation about why consideration

Nevertheless, it is important to note that the data processing for merchandising is necessary for the performance of merchandising contracts. An agency-merchandising agreement, including sub-licensing, serves as an example to examine whether the data processing meets the requirement of necessity as it is more complex and welcomed by professionals in practice.

The purposes of an agency-merchandising agreement for an average data subject are evident: to acquire (as much as possible) consideration and publicity by licensing the use of personal photos while saving the time and expense of contacting business partners. Consequently, there is no less intrusive way of processing data to achieve this purpose than concluding an agency-merchandising agreement. It also holds for exploitation of erotic photos, given that it is the exact lifestyle the data subject chooses, and erotic photos are not sensitive data from the perspective of the GDPR. Thus, the publication of normal photos would be neither the purpose of the data subject nor less intrusive from his or her perspective. After all, the publication of normal photos and erotic photos belong to different professional fields. In terms of data transmission, there is no less intrusive way either because without transmitting the data to third controllers, the contract's main purpose – receiving remuneration from publications would fall through. Moreover, a standard merchandising agreement between the model and third controllers cannot provide professional and efficient management of the personal images/data of the data subject, including sub-licensing. In short, they serve different purposes and are thus irreplaceable.

In summary, operations concerning data processing including sub-licensing and transmitting in merchandising are necessary to the performance of agency-merchandising contracts. If Art. 6 (1) (b) GDPR would apply to merchandising contracts, a more stable status for both parties than the anytime revocable consent could be provided. The form of merchandising contract does not affect its validity under the GDPR since Art. 6 (1) (b) GDPR does not restrict the form of contracts.

On the one hand, the high-level data protection envisioned by the GDPR should not be exaggerated to stifle private autonomy as the data subject in merchandising also wishes to establish a long-term and stable

---

of personality protection under German civil law can provide a basis for the interpretation of necessity under EU data protection law. See *Bunnenberg,* Privates Datenschutzrecht: über Privatautonomie im Datenschutzrecht, S. 59-60, 265-266; *Golz and Gössling*, IPRB, 2018, 68 (71f.), while no argumentation is provided.

cooperative relationship with the agency. On the other hand, the narrow ambit of Art. 6 (1) (b) GDPR would lead to a deviation from the genuine meaning of the data subject. Even in the *company-advertising* case, the declaration given by the data subject by signing his name on the name list (*Namensliste*) is intended to be binding.[472] Moreover, the wording of Art. 6 (1) (b) GDPR – "processing is necessary for the performance of a contract to which the data subject is party" – also suggests that it can legitimize data processing of third parties not mentioned in the contract.

On the other, the EDPS holds a solid resistance to commercializing personal data as it compares a market for personal data with a market for live human organs.[473] In addition, agency-merchandising agreements might increase the risk of data subjects losing control of personal data if consent is not the compulsory lawful ground for the first controller and the second controllers (sub-licensees).[474] Last but not least, if an agency-merchandising agreement qualifies the application of Art. 6 (1) (b) GDPR, the data subject needs to terminate the contract under domestic law even if he or she has not been notified about the second controllers when that contract is concluded. The strength of the protection is thus significantly weaker than the readily revocable consent. The right to object or restrict processing due to challenges to the legal basis for processing would not be very supportive either if the data processing is necessary for the performance of that contract.

Following the mainstream opinion in literature, Art. 6 (1) (b) GDPR does not apply to authorized merchandising as the main performance of merchandising contracts is data processing. Though the data processing including sub-licensing is absolutely necessary to the performance of merchandising contracts, the commercialization of personal data in light of such contracts is strongly objected to by the EDPS, and, more importantly, the relatively broad reading of Art. 6 (1) (b) GDPR would circumvent the pivotal lawful ground of consent and thereby cause data subjects to lose control of personal data.

---

472 BAG, GRUR 2015, 922 - Veröffentlichung von Arbeitnehmer-Bildnissen zu Werbezwecken, Rn. 27.

473 EDPS, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, para. 17.

474 *Sattler, in: Pertot, Rechte an Daten*, 49 (69~70); *Westphalen and Wendehorst*, BB, 2016, 2179 (2187); Wendehorst, Verbraucherrelevante Problemstellungen zu Besitz und Eigentumsverhältnissen beim Internet der Dinge, Rechtgutachten für BMJV, 201611/2016, S. 51 ff.

4.3.2 Any other possibilities to conquer the revocability of consent?

(1) Cumulation of lawful grounds

The GDPR does not oppose a cumulation of lawful grounds as Art. 6 (1) and 17 (1) (b) GDPR suggest.[475] While the WP29 rejects the idea that processing for one purpose could be based on several legal bases,[476] many scholars express opposition to this interpretation for legal and practical reasons.[477] Admittedly, the practical consequence of the free revocability of consent is prevented by other lawful grounds. It thus might be misleading to data subjects who thought they would be able to call off the processing at any time.[478] However, the GDPR prepares two cumulative measures to address this concern.

First, the duty to inform as an *ex-ante* precaution ensures that data subjects would not be misled in cases of a cumulation of lawful grounds. Furthermore, subsequent modifications/additions to legitimate grounds shall be prohibited because the data subject's informational self-determination would be compromised.[479] The duty of information is enhanced when the controller relies on both consent and Art. 6 (1) (f) GDPR to ascertain that it processes personal data even if the data subject withdraws consent. Art. 13 (1) (d) GDPR requires the data controller to name the specific legitimate interests it pursues when it rests on the balancing of interests; Art. 21 (1) grants the data subject the right to object at any time when his or her data has been processed based on Art. 6 (1) (f) GDPR. Until the controller can demonstrate an overwhelming legitimate interest, it shall suspend processing according to Art. 18 (1) (d) GDPR. This rigorous duty to inform is referential for the cumulation of consent and contract because

---

475 Art. 6 (1) states that: "Processing shall be lawful only if and to the extent that at least one of the following applies." (Stressed by the author); Art. 17 (1) (b) GDPR states that the controller shall erase personal data when the data subject withdraws consent, "and where there is no other legal ground for the processing".

476 WP29, Guidelines on consent under Regulation 2016/679, 17/EN, 22. According to it, a cumulation of lawful grounds is only possible if the data processing is carried out for several purposes.

477 Vgl. Plath, in *Plath,* DSGVO/BDSG, Art. 6 Rn. 5; Buchner/Petri, in *Kühling/Buchner,* DSGVO/BDSG, Art. 6 Rn. 22f.; Schulz, in Gola/Schulz Art. 6 Rn. 11; Albers/Veit, in *Brink/Wolff,* BeckOK Datenschutzrecht, Art. 6 Rn. 24.

478 Vgl. Buchner/Petri, in *Kühling/Buchner,* DSGVO/BDSG, Art. 6 Rn. 23.

479 See also *Krusche*, ZD, 2020, 232 (233f.).

the data subject cannot stop the processing when he or she withdraws consent either.

Imagine if a controller invokes both consent and a contract to process personal data, its instructions to the data subject need to satisfy the respective notification requirements for legitimate reasons and be unambiguous. Moreover, this duty of information must be exercised prior to the data processing, and any subsequent change is prohibited. More specifically, the controller must meet the conditions listed in Art. 7 and 4 (11) GDPR to construct the validity of consent. Therefore, to demonstrate compliance with Art. 6 (1) (b) GDPR, the fulfillment of the requirement of necessity is indispensable. Noteworthy, the requirement of necessity is not contradictory to the prohibition of coupling in Art. 7 (4) GDPR because the latter only "prohibits" the coupling of consent with unnecessary data processing in relation to the performance of a contract. Most importantly, the data subject must be notified that he or she has to effectively terminate the contract to stop the data processing due to the existence of that contract.

Second, the principles of lawfulness and accountability require data controllers to be responsible for the accuracy of their duty to inform. Therefore, if the controller asserts a contract that does not meet the requirements of the GDPR, then it needs to take responsibility for the misstatements. If the controller's declaration is mistake-free, the data subject could easily call off the data processing by withdrawing consent, but instead, he or she needs to first terminate the contract following domestic law. This mistake is not insignificant because the difficulty of exercising the control of the data subject has been significantly increased due to the controller's unintentional/intentional misinformation. Thus, it is warranted that Art. 83 (5) (a) GDPR prescribes the provision of a wrongful lawful ground as one of the circumstances for aggravated fines and probable damages.

In summary, the information provided by the controller must be extremely elucidative and comprehensive provided on a cumulation of lawful grounds. Given the heavier obligations in notification when the controller needs to process personal data based on contractual obligations, the declaration must become extremely long and complicated. It will, in return, affect the data subject's understanding of the content.[480] In

480 Solove, 126 Harvard Law Review 1880 (2013), 1885. He argues that the privacy notice is complex and needs to be explained in detail. A "visceral notice" like the powerful graphic warnings on cigarettes is likely to be inherently incompatible with privacy notices.

addition, the more legitimate reasons there are, the more likely they are to be challenged.

Therefore, contrary to what scholars envision, a cumulation of the contract and consent is not necessarily a better approach.[481] While it is acceptable in theory, it raises more obligations and concerns than what it can benefit in merchandising scenarios. Moreover, since the applicability of Art. 6 (1) (b) GDPR in merchandising contracts is under question, the notification about this lawful ground could lead to liability and fines for misleading information. If Art. 6 (1) (b) GDPR cannot be applied, it is both misinformation and a severe limitation on the right to self-determination of the data subject when the statement drafted by the controller declares that the withdrawal of consent shall not render the merchandising unlawful because the contract is still valid.[482] If Art. 6 (1) (b) GDPR is applicable in merchandising cases, the controller must be very cautious in drafting the declaration to avoid any confusion of the data subject.

It is thus advised here that data controllers choose only the legitimate reason they are most confident rather than relying solely on quantity.[483]

(2) Any other alternatives?[484]

To prevent the principle of *pacta sunt servanda* in merchandising contracts from being overridden by the anytime revocability of consent,[485] some scholars propose to treat the contracts as the legal basis for data subjects

481 Some scholars argued that it would suffice when the data subject is informed that "the processing is not prohibited when the data subject withdraws the consent because Art. 6 (1) (b) GDPR also applies in this case." See Schulz, in *Gola*, DSGVO, Art. 6 Rn. 12; Buchner/Petri, in *Kühling/Buchner*, DSGVO/BDSG, Art. 7 Rn. 39a.

482 Since the termination of the contract shall rely on national law, the "consent" (authorization) in merchandising is only revocable under exceptional circumstances with a due cause like the change of beliefs of the data subject as German courts consistently found.

483 Different opinion, see *Krusche*, ZD, 2020, 232 (234f.).

484 There are also other possibilities in interpreting Art. 6 (1) (b) GDPR by scholars and the EDPB. They are introduced and evaluated in Part IV as one of the solutions.

485 Albers/Veit, in *Brink/Wolff*, BeckOK Datenschutzrecht, Art. 6 Rn. 44; Klement, in *Simitis, et al.*, Datenschutzrecht, Art. 7 Rn. 92.

to give consent in the sense of Art. 6 (1) (a) GDPR.[486] In this wise, consent here is still anytime revocable according to Art. 7 (3) GDPR, but the withdrawal without reason could be regarded as a breach of contract and thus compensation for data controllers is possible based on the principle of fairness. In other words, the provision of consent under the data protection law, i.e., revocable consent, is a contractual obligation, and it cannot be refused without legitimate reasons.[487] However, this proposal would be a deterrent for data subjects to withdraw consent at any time, which seems to defeat the purpose of Art. 7 (3) GDPR. While one may argue that controllers would be more willing to make significant and long-term investments that are beneficial for data subjects, too, the scholars admit that their proposal presupposes strict scrutiny of the validity of contracts. Otherwise, it becomes a cover for circumventing the high-level data protection provided by the GDPR.

Another interesting opinion is to consider the lawful ground based on the balancing of interests pursuant to Art. 6 (1) (f) GDPR.[488] 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 signed by the data subject. The possibility of this alternative is explored in detail as one of the solutions in Part IV.

---

486 Vgl. 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.; *Riesenhuber*, RdA, 2011, 257

487 This consideration is very similar to how German courts and scholars understand the consent in merchandising under the KUG, namely, it is neither irrevocable nor free revocable. See Part I Section 3.1.1.

488 Enlighted by the judgments delivered in German courts. 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.

4.4 Preliminary conclusions

Personal images are not biometric data of Art. 4 (14) GDPR. Moreover, since the processing defined in the GDPR is different from human cognition, the purpose of data processing is an indispensable factor in invoking the protection for sensitive data as a machine cannot "see" through pictures unless it is programmed to do so. The processing of images for merchandising does not fall under the scope of Art. 9 GDPR according to the subjective approach of Art. 9 (1) GDPR with an emphasis on the reverse burden of proof if the data controller can demonstrate that no sensitive information about the data subject's race, ethnic origin, or health status that could be revealed from the photo is processed. Feasible measures include detailed documentation concerning the purpose, content, and means of processing as well as the business model.

The lawful grounds of consent and a contract under the GDPR are effective ways to implement private autonomy. In merchandising scenarios, the collision of norms between the GDPR and the KUG does not mean that consent in the KUG must be understood per GDPR. Rather, the indication of the depicted person needs to be judged based on facts. This finding does not unduly discriminate against the interests of the data subject because it, by virtue, respects the self-determination of the data subject, and the controller bears the burden of proof that the data subject intends to conclude a contract rather than a simple consent according to the principle of accountability. However, consent and a contract both present insoluble difficulties for authorized merchandising.

Above all, merchandising contracts are no longer binding as consent is free revocable pursuant to Art. 7 (3) GDPR. Art. 6 (1) (b) GDPR cannot legitimize the data processing that is the primary performance of the contract as in merchandising scenarios according to the prevailing opinion. Secondly, given the rigorous conditions of validity for consent in Art. 4 (11) and 7 GDPR, controllers are obliged with a strict duty of notification. Failure to meet these conditions probably results in damages and administrative fines, and if the failure seriously affects the right to informational self-determination of the data subject, the data processing would be regarded as unlawful from the outset. Furthermore, the absence of notifying the revocability of consent is argued to render the consent invalid because it leads to confusion on the part of the data subject and deprives the data subject's rights including the right to withdraw consent at any time. In addition, although the emphasis on the voluntariness of consent in light of the GDPR is warranted and welcomed, especially in case of a

severe structural inequity between young models and powerful agencies, the assessment supported by the WP29 is ill-suited in merchandising as it ignores the essence of merchandising: data processing against money and exposure.

The consequences are two folded. On the one hand, merchandisers are dissuaded from making significant and long-term investments in merchandising as their investments would not be protected anymore. On the other hand, it, in return, affects models significantly and contradicts their genuine willingness. As reiterated, both parties in authorized merchandising wish to have a binding cooperative relationship. However, it is further argued that the enhanced protection for data subjects facilitated by the rigorous conditions of validity for consent is not ideal for them, either. The outcome of applying Art. 6 (1) GDPR to the *company-advertising* and the *landlady* case is a good example. While the data processing in the former case was unlawful from the beginning despite the data subject's explicit consent to advertising for the company, the data subject in the latter would probably end up without a job because no magazine would be willing to accept the condition that all data processing regarding photos must stop immediately as soon as she withdrew consent.

Some scholars note the conflict between the principle of pacta sunt servanda and the anytime revocable consent; some suggest a combination of consent in the sense of GDPR and a contract under German law. However, despite all their apparent benefits, counterarguments abound. Among others, the most decisive ones are: the possible circumvention of the revocable consent, the accompanying compromise of the enhanced control over personal data envisaged by the GDPR, and the strong resistance of the EDPS and EDPB against the commercialization of personal data.

4.5 Data subject's rights in merchandising

4.5.1 Mandatory rights under the GDPR

The GDPR is not a single rule that determines the lawfulness of the processing. Instead, it is a complete regulatory system for compliance evaluation of the entire process of data processing. Thus, full compliance with the GDPR also requires a responsive mechanism for data subject's rights. In Chapter 3 of the GDPR, data subjects are granted numerous rights including the right to information and its associated rights (Art. 12-15), the

right to rectification (Art. 16), the right to erasure ("right to be forgotten") (Art. 17), the right to restriction of processing (Art. 18), the right to data portability (Art. 20) and the right to object (Art. 21) and not to be subject to a decision based on automated processing (Art. 22).

The right to information and its associated rights are highlighted in the GDPR because they are the foundation of transparency and guarantee the genuine execution of informational self-determination of the data subject. Based on explicit knowledge about data processing, Art. 16-22 GDPR further provide rights for data subjection to control data processing. Since the GDPR pursues dual objectives – data protection for data subjects and free flow of data (within the EU), these rights to control data processing naturally have conditions and exceptions, which have been concretized in their respective provisions and some general clauses such as Art. 85 GDPR.

Since there is no legal text in the GDPR stating that these rights are indispensable, it is questionable whether the data subject can give up the rights voluntarily or if the controller can restrict the application or execution of these rights through consent or contract.[489] The compelling consensus in the literature is that the data subject's rights are indispensable and not negotiable. Thus, any declaration given by the data subject or contractual terms suggesting a derogation or exclusion of the data subject's rights are void.[490] Justifications proceed as follows.

Above all, the rights in Chapter 3 of the GDPR are corollaries of "effective protection of personal data throughout the Union".[491] Both the rights guaranteeing transparency and ones enhancing the control of data subjects undergird the protection of personal data anchored in Art. 8 of the Charter – fair and lawful data processing with specified purposes and, in particular, the self-determination of the data subject.[492] Rendering them disposable would significantly undermine the high-level data protection enabled by the compliance rules and virtually deprive the control of data subjects over personal data.

Secondly, while the rights seem to present uneven protection towards data subjects at the expense of controllers, the GDPR provides a two-tier framework to strike a fair balance between the competing interests of the

489 Franck, in *Gola,* DSGVO, Art. 12 Rn. 31.
490 Schmidt-Wudy, in *Brink/Wolff,* BeckOK Datenschutzrecht, Art. 15 Rn. 34; Dix, in *Simitis, et al.,* Datenschutzrecht, Art. 12 Rn. 6.
491 See recital 11 of the GDPR.
492 Dix, in *Simitis, et al.,* Datenschutzrecht, Art. 12 Rn. 6.

data subject, controller, and third party.[493] In the highest tier, the opening clauses in the GDPR allow the Member States to make derogations and exemptions from Chapter 3 for some critical countervalues, such as the freedom of expression in four exclusive fields listed in Art. 85 (2) GDPR, public interests in accessing official documents pursuant to Art. 86, and public interests regarding scientific, historical research, or statistical purposes in Art. 89 (2) GDPR.

The second level involves the handling of details. For example, in Art. 12 (5) GDPR, the controller is allowed to charge a reasonable fee or refuse to act on the request if the claims from a data subject are "manifestly unfounded or excessive".[494] This provision is devised to prevent abuse of rights derived from the principle of good faith. Moreover, concerning the rights to control data processing – be it the right to erasure, objection, or portability – the GDPR sets forth detailed conditions for their validity and exceptions to mandate an interests-balancing in a case-by-case fashion. For instance, according to Art. 17 (3) (a) GDPR, the right to erasure shall not apply, if "processing is necessary for exercising the right of freedom of expression and information".

Lastly, given the conditions and exceptions of the data subject's rights, they are not "absolute" rights that the controller must satisfy if the data subject requests.[495] Rather, the GDPR emphasizes the responsiveness of the controller in compliance with the requirements forwarded by Art. 12 GDPR. Therefore, these rights have some value in upholding procedural justice for the data subject by granting them a protectable legal stand over which to exert control on personal data.[496]

To shape a data processing architecture that is fair, transparent, and compliant with fundamental rights requirements,[497] more reasons for why these rights cannot be waived by contract or consent are needed.

---

493 Vgl. *Benedikt and Kranig*, ZD, 2019, 4 (7).

494 CJEU, Google Spain, C-131/12; Dix, in *Simitis, et al.,* Datenschutzrecht, Art. 12 Rn. 30f.

495 *Gusy,* in: *Knopp and Wolff, Umwelt - Hochschule - Staat : Festschrift für Franz-Joseph Peine zum 70. Geburtstag*, 423 (432ff.). It argues that the recognition of the individual's control over personal data is partly a (mere) political postulate.

496 *Worms and Gusy*, DuD, 2012, 92.

497 *Bull,* Sinn und Unsinn des Datenschutzes, S. 6.

4.5.2 The execution of the data subject's rights

(1) The right to information and its associated rights (Art. 12-15)

The GDPR provides detailed rules to implement the principle of transparency in Art. 12-15 GDPR. A cording to Art. 12 GDPR, the data controller is obliged to provide information regarding data processing (Art. 12 (1) GDPR) and convenience and the executions of rights listed in Art. 15-22 GDPR for the data subject (Art. 12 (2) GDPR). More specifically, Art. 12 (1) GDPR specifies how to fulfill the obligation to inform, while Art. 12 (3) and (4) GDPR set the time limit for fulfilling that obligation. Under the principle of fairness, Art. 12 (5) provides exceptions where the controller may charge or refuse to provide information. The last two paragraphs of Art. 12 GDPR present expectations for "iconization" of the duty to inform.[498]

Art. 13 and 14 GDPR specify the content, manner, and time frame in which the controller shall fulfill the duty to inform when it collects data directly from the data subject or elsewhere, respectively. Mainly, the information concerns the controller's identity and contact information, data processing, including its content, means, purpose, and the remedies and rights of the data subject. Although the provision of such information is mandatory according to the principle of transparency, Art. 13 (4) and 14 (5) (a) GDPR offer a way to soften the legal consequence for omissions, if the data controller can prove that the data subject has already acquired that information. After that, the provision would no longer be necessary.

The right to access in Art. 15 GDPR guarantees the principle of transparency from the side of the data subject. Moreover, Art. 15 (3) GDPR grants data subjects the right to obtain "a copy of the personal data undergoing processing" by the controller. The relationship between this

498 Originated in the Creative Commons, the expression of icons for licensing agreements has inspired a discussion of whether and how privacy agreements can be expressed iconically (standardized) in the privacy protection field. Besides Art. 12 (7) GDPR, Recitals 60 and 166 have also encouraged attempts to iconify privacy policies at the legal level. There has also been much useful academic discussion of this issue and suggestions for iconographic standards: Edwards and Abel, The Use of Privacy Icons and Standard Contract Terms for Generating Consumer Trust and Confidence in Digital Services, CREATe Working Paper 2014/15, at https://www.create.ac.uk/publications/the-use-of-privacy-icons-and-standard-contract-terms-for-generating-consumer-trust-and-confidence-in-digital-services/.

right and the right to information is controversial because the scope of the information they request appears to be different.[499] While the right to information is concerned more about the legality of data processing, the right to obtain a copy focuses on the data possessed by the controller.[500] In qualifying the content of the right to obtain a copy, some scholars argue that the categories of information specified in Art. 15 (1) GDPR are sufficient and that no more data are needed.[501] Conversely, others attach more value on the verbatim reading of Art. 15 (3) GDPR. It indicates that personal data undergoes processing by the controller instead of the information listed in Art. 15 (1) GDPR.[502] In this regard, it is not enough for controllers to provide a copy of the data actively provided by the data subject; They also need to provide a copy of personal data collected from elsewhere and already edited with inputs of the controller, such as examination reviews, assessments by treating physicians, etc.

It is convincing that the data subject can inquire about the legality of data processing and invoke specific claims, such as the right to rectify or delete obsolete data only by knowing exactly what data is in the controller's possession. Therefore, one could argue that the principle of legitimacy is undergirded by the right to obtain a copy to a more extensive extent. The view that the right to obtain a copy is needed only for documentation for data subjects is largely dismissive of the potential of this right in enabling data subjects. Moreover, this actual reading is compatible with the exception for this right in Art. 15 (4).[503] If the content of Art. 15

499 Schmidt-Wudy, in *Brink/Wolff,* BeckOK Datenschutzrecht, Art. 15 Rn. 85; *Wybitul and Brams*, NZA, 2019, 672.

500 LAG Baden-Württemberg, NZA-RR 2019, 242 - DSGVO-Auskunftsanspruch gegen Arbeitgeber, para. 104; *Kremer*, CR, 2018, 560 (563f.); Franck, in *Gola,* DSGVO, Art. 15 Rn. 23 und 27; Bäcker, in *Kühling/Buchner,* DSGVO/BDSG, Art. 15 Rn. 40; Dix, in *Simitis, et al.,* Datenschutzrecht, Art. 15 Rn. 28; *Riemer*, ZD, 2019, 413 (414); Schmidt-Wudy, in *Brink/Wolff,* BeckOK Datenschutzrecht, Art. 15 Rn. 87.1; Paal, in *Paal and Pauly,* DS-GVO BDSG, Art. 15 Rn. 33.

501 *Dausend*, ZD, 2019, 103 (106f.); Paal, in *Paal and Pauly,* DS-GVO BDSG, Art. 15 Rn. 33 und 33a; *Wybitul and Brams,* NZA, 2019, 672 (676).

502 CJEU, YS, Joined Cases C-141/12 and C-372/12; Recital 63 of the GDPR; Franck, in *Gola,* DSGVO, Art. 15 Rn. 23; Bäcker, in *Kühling/Buchner,* DSGVO/BDSG, Art. 15 Rn. 39a.

503 Art. 15 (4) GDPR states that the right to obtain a copy "shall not adversely affect the rights and freedoms of others".

(3) GDPR is merely the categories of personal data according to Art. 15 (1) GDPR, such an extensive exception seems unconvincing.[504]

Regarding the legal consequence of failing to meet these obligations, as consistently argued above, the core issue is whether the data subject has wrongly exercised control over personal data based on misinformation. On the one hand, the right to information is the fundamental and enabling right of the data subject. In the absence of information, the data subject cannot effectively implement the right to information self-determination. On the other hand, not all lack of information would affect the data subject's execution of the right to self-determination. Therefore, one should carefully distinguish the nature of the information and check whether its absence could result in the data subject wrongly exercising control over personal data.

Against this backdrop, the controller in a merchandising case must provide information regarding its contact information, data processing, and the remedies and rights available for the data subject prior to data processing "in a concise, transparent, intelligible and easily accessible form, using clear and plain language". However, the controller does not bear the obligation to provide the data subject with the accounting since the accounting information about the distribution and revenue is in general not personal data, though the remuneration for the data subject is computed on the revenue.

In practice, it is advised to list the information prescribed in Art. 12-15 GDPR in an appendix as an indispensable component of the written merchandising contract for compliance. In addition to storing the personal data volunteered by the data subject separately (also in response to the data portability right in Art. 20 GDPR), it is recommended for merchandisers to store the final advertising artwork separately to respond to the right to obtain a copy of personal data as well. When other person's data is also included in the final presentation of the artwork, some scholars argue for pixilation of other's images in response to the right to obtain a copy.[505]

504 Vgl. Dix, in *Simitis, et al.*, Datenschutzrecht, Art. 15 Rn. 33; Vgl. *Härting*, CR, 2019, 219 (221f.).

505 Dix, in *Simitis, et al.*, Datenschutzrecht, Art. 15 Rn. 33.

(2) The right to rectification (Art. 16)

According to the first sentence of Art. 16, the data subject is entitled to request the data controller to correct inaccurate personal data. Stemming from the principle of accuracy in Art. 5 (1) (d) GDPR, the awareness of the inaccuracy does not necessarily depend on the notification of the data subject. In other words, the controller carries the duty to review its data processing operations to assure that personal data are accurate and to erase or rectify the inaccurate data without delay. Therefore, the decisive condition for claiming this right is to demonstrate that the personal data the controller processed is inaccurate. While it is the unanimous outlook in the academic literature that personal data is inaccurate if it does not correspond to reality,[506] it comes into a debate when it involves opinions and value judgments.[507] The seemingly mainstream opinion is that the pure value judgments are exempted from the obligation to rectification due to freedom of speech, but one should carefully distinguish pure value judgments and judgments based on wrong facts.[508] The right to rectification is, in any event, feasible in the latter scenario.

The second sentence of Art. 16 GDPR grants the data subject the right to have incomplete personal data completed. This right might play a crucial role in fields concerning profiling and automated decision-making, where the accuracy of the analysis is based on the integrity of personal data. In this sense, the right to complete personal data is also derived from the principle of accuracy. While it might be elusive for the data subject to sense when his or her data is incomplete, scholars tend to postulate that personal data processed by the controller is "never comprehensive", thus a risk-based approach is advocated here.[509] The more risks are posed to the rights and freedoms of the data subject by processing, the more data are needed to achieve the purpose agreed on by the data subject, and the stronger the reason is to complete personal data.

In authorized merchandising scenarios, these two rights aimed at guaranteeing the accuracy of personal data are not as useful as expected. Taking the *company-advertising* case as an example, the data subject might be able

506 Reif, in *Gola*, DSGVO, Art. 16 Rn. 11; Peuker, in *Sydow*, DSGVO: Handkommentar, Art. 16 Rn. 7; BVerwG, NVwZ 2004, 626 - Personalaktendaten; Dix, in *Simitis, et al.*, Datenschutzrecht, Art. 16 Rn. 11 f.

507 Worms, *Brink/Wolff*, BeckOK Datenschutzrecht, Art. 16 Rn. 53f.; Reif, in *Gola*, DSGVO, Art. 16 Rn. 10.

508 Dix, in *Simitis, et al.*, Datenschutzrecht, Art. 16 Rn. 14f.

509 Worms, *Brink/Wolff*, BeckOK Datenschutzrecht, Art. 16 Rn. 57.

to request the right to rectification because the video displayed on a company's website presented a false narrative of him; specifically, that he was still working for the company. Therefore, according to the rights in Art. 16 GDPR, the controller might have to pixilate his facial images, remove the video, or write a statement next to the video saying the data subject named *XX* and depicted in the video (concrete position) is no longer working here. However, even though this claim may be sustained, it does not satisfy the claim of the data subject in the case.

Firstly, even though the German court has argued that the commercial produced by the company did not necessarily generate the idea that the characters in the video were current employees,[510] it is contested here that the personal data processed in the commercial was no longer accurate after the data subject has left the company in light of the purposes of data processing when the controller has collected the personal data.[511] In other words, the controller is obliged to guarantee the accuracy of data up to update. If the purposes of producing the video were to show the friendly and family-like working atmosphere in the company, the participants should be real employees of the company. Therefore, the data subject could claim the right to rectification in the case. Secondly, one might argue that the take-down of the video would affect the rights and freedoms of the other people shown in the commercial since they choose to exercise their right to self-determination positively. However, unlike other rights such as the right to erasure, the rights to rectification and complete incomplete data do not have specific exceptions.[512] The objection based on the harmed rights and freedoms of third parties thus cannot find a legal basis in the GDPR.

Lastly, to make a counterstatement to set the record right may be influential and effective in (automated) decision-making seems absurd in merchandising scenarios. In doing so, the data subject virtually makes him highlighted in the commercial and gives more personal data to the public. All in all, the right to rectification presents a resemblance to the claims for correction, and publication of a counterstatement in Germany discussed in Part I Section 2.2.2. They are effective in protecting the person from distortion or misunderstanding but cannot be used to reduce exposure of

510 BAG, GRUR 2015, 922 - Veröffentlichung von Arbeitnehmer-Bildnissen zu Werbezwecken, Rn. 39.
511 Dix, in *Simitis, et al.*, Datenschutzrecht, Art. 16 Rn. 12.
512 Ibid., Rn. 19.

the advertisement and combat the motivation of the merchandiser to use the portrait illegally.

Nevertheless, if the data subject becomes aware of the inaccurate information before making it available to the public and exercises the right to rectification promptly, it might be useful to prevent wrongful endorsements.[513] The data subject could thus rely on this right to correct the statements about him or her in controlling the presentation of the final product. However, it is noteworthy that the right to rectification limits its application within inaccurate data per facts.

The right to rectification, albeit showing both *ex ante* and *ex post* characters, is not quite useful in merchandising cases. For one, rekindling old issues is not a desirable outcome for the data subject who would not want to draw people's attention again to the inaccurate merchandising. This holds especially true in celebrity merchandising. Moreover, this right is governed by the facts instead of the wish of the data subject. This significantly narrows the scope and effectiveness of the right to rectification from the data subject's perspective.

(3) The right to erasure (Art. 17)

The right to erasure under the GDPR is a manifestation of the principles of lawfulness and data minimization.[514] If the data processing is no longer lawful, the deletion of personal data is a proper and necessary consequence flowing from the right to protection for personal data in Art. 8 of the Charter. Reflected in the *Google Spain* case, "erasure" in the provision does not only cover physical deletion in the conventional sense but is supposed to be a term that should keep up with the technology (see the discussion in

513 An interesting case in China shows the importance of the right to rectification. The pianist Lang Lang and his wife make endorsements for milk powder coming from two brands and state that my baby only drinks XX brand of milk powder. Since this advertisement is clearly at odds with the facts, it would not have caused consumers to wonder about the creditability of this couple, if they would have noticed the tagline before the ad was released and asked for a correction.

514 Some scholars consider that this right stems from the principles of necessity and accuracy. See Dix, in *Simitis*, *et al.*, Datenschutzrecht, Art. 17 Rn. 1. However, the principle of necessity, albeit reflected in the principle of data minimization, is not explicitly anchored in the GDPR. The principle of accuracy seems remote since Art. 17 GDPR does not regard inaccurate data as a reason for deleting.

Part II Section 3.2.3 (3)). Thus, considering the technical limitations, it is conceivable to blur an actor's face to render him unrecognizable in a film or TV program, for example, since it is often impossible to delete the scene or sequences composited by several other actors/actresses.[515]

Art. 17 (1) GDPR states six alternative conditions for which the data controller shall timely delete the personal data upon the request of the data subject. The most important ones in authorized merchandising are Art. 17 (1) (b) and (d) GDPR. When the processing relies on the consent of the data subject, the controller needs to delete the data when the consent is withdrawn by the data subject according to Art. 17 (1) (b) GDPR.[516] For instance, the data subject in the *company-advertising* case could invoke Rt. 17 (1) (d) GDPR in combination with the withdrawal of consent to guarantee the right to erasure since he was confused about the binding nature of his "consent" due to the ambiguous declaration drafted by the controller.

It is thus discernable that the exercise of the right to erasure is closely linked to the legitimate grounds for data processing by the data controller. If the lawful ground is consent, a long and costly collaboration between the controller and data subject seems inconceivable. If the data subject withdraws consent, subsequent investments will cease, and previous investments made by the controller will be futile because of the *ex nunc* effect of the withdrawal of consent and the semi-automatic consequence of data deletion according to Art. 17 (1) (b) GDPR. Even though Art. 17 (3) (a) GDPR provides some relatively wide exceptions for the right to erasure, it is questionable whether the exclusive commercial interests pursued by the controller could be regarded as necessary "for exercising the right of freedom of expression and information". No contribution to public discussion or formation of public opinions has been made in typical merchandising cases such as the *landlady* case and the *company-advertising* case. In this sense, only some borderline cases mentioned in Part I Section 2.1.3, such as the *Rücktritt des Finanzministers* case, might be able to invoke this exception.

A due cause, such as a changed belief to withdraw consent to terminate the merchandising contract is required in Germany. Art. 17 (1) (a) GDPR, which requires the controller to delete the personal data that are no longer necessary in relation to the purposes for which they are processed, may

515 *Reuter and Schwarz,* ZUM, 2020, 31 (37).

516 However, this obligation can be suspended if there is another legal ground for the processing.

also be relevant when the processing exceeds the reasonable expectation of the data subject. As discussed in the *landlady* case in association with the *"stink fingers"* case, many details of merchandising may not be specified in the contract for efficiency against the background of mature business practices in the industry. Thus, some excessive processing activities like the editing in the *"stink fingers"* case, or the long-term storage of personal data can be challenged by the right to erasure according to Art. 17 (1) (a) GDPR. Noteworthy, the claim does not affect the validity of the consent but the specified processing operation(s).

In summary, the right to erasure is effectively coupled with the anytime revocable consent.

(4) The right to portability (Art. 20)

As an innovative data subject's right in the GDPR,[517] the right to portability is envisaged to be the "disruptive" right in tackling the lock-in effect of online social platforms.[518] By virtue of this right, the data subject shall request the controller to transmit personal data to data subject self (Art. 20 (1)) or directly to another controller designated by the data subject (Art. 20 (2)), unless the exception in Art. 20 (4) GDPR is applicable. The aim of the transmission directly to another controller is clear: by enabling data subjects to smoothly switch from one controller to another, a competitive environment for data controllers is encouraged for a higher protection level for personal data.[519]

Despite the seemingly strong potential, the fact is that the right to portability has many constraints apart from the exception for protection of the rights and freedoms of others. On the one hand, the right to portability merely covers the data provided by the data subject's initiative or that the controller was collected based on the open-access permitted by the data subject, namely the observation data.[520] In this wise, as long as

---

517 Vgl. *Albrecht and Jotzo,* Das neue Datenschutzrecht der EU, S. 293, 299f.

518 *Kühling and Martini*, EuZW, 2016, 448 (450); WP29, Guidelines on the right to "data portability", wp242 rev.01, 6.

519 Vgl. *Drexl,* in: *Franceschi and Schulze, Digital Revolution - New Challenges for Law: Data Protection, Artificial Intelligence, Smart Products, Blockchain Technology and Virtual Currencies*, 28.

520 WP29, Guidelines on the right to "data portability", wp242 rev.01, 9 et seq.; Dix, in *Simitis, et al.*, Datenschutzrecht, Art. 20 Rn. 8; Herbst, in *Kühling/Buchner,* DSGVO/BDSG, Art. 20 Rn. 11. Some scholars consider this theme contro-

the personal data collected by the controller are not based on consent or contract, or have been processed by the controller with inputs from other sources, and thus become the so-called "inferred data or derived data", the right to portability is no longer applicable.[521] Therefore, the ambit of the right to portability is narrower than the one of the right to obtain a copy of data in Art. 15 (3) GDPR. On the other hand, the GDPR mitigates the impact of the right to portability by introducing a "not very concrete legal concept" (*wenig konkrete Rechtsbegriff*).[522] In Art. 20 (2) GDPR, a data controller must transmit data directly to another controller only if it is technically feasible to do so.

In merchandising scenarios, while information regarding the identity of the data subject in the contract is subject to the right to portability as it is actively provided by the data subject, the photographs of the data subject taken by the controller are in question. For one, it may belong to observation data because the controller collects the data by recording only upon the authorization and cooperation of the data subject. Second, the photos require editorial processing conducted by the controller to become advertisements. Varied aesthetic assessments and alterations have been taken to serve publicity and commercial interests. Therefore, the edited data processed by the controller are more likely to be derived data rather than observed data and thus do not fall under the scope of Art. 20 GDPR.

Against the backdrop, the data subject can claim the right to portability to transmit his or her identification data and perhaps unedited photographs, but not the processed data combined with inputs from the controller. According to Art. 20 (2) GDPR, the data subject may also ask the controller to transmit those data directly to another controller designated by the data subject. However, since the pictures are taken by virtue of aesthetic assessments of the photographer, copyright would be a legitimate reason to limit any further exploitation of the photos in this scenario. Trade secrets would be perceivable if the merchandising relationship between the data subject and the controller has not been disclosed, or information about new products that are being merchandised is confidential.

---

versial and argue for a differentiation based on the type of the services, see *Strube*, ZD, 2017, 355 (359f.); *Gierschmann*, ZD, 2016, 51 (54); Kamann/Braun, in *Ehmann and Selmayr,* DS-GVO, Art. 20 Rn. 13.

521 WP29, Guidelines on the right to "data portability", wp242 rev.01, 10 et seq.

522 von Lewinski, in *Brink/Wolff,* BeckOK Datenschutzrecht, Art. 20 Rn. 88.

4.5.3 Preliminary conclusions

The data subject's rights are essential manifestations of the dual-objectives and the principles of the GDPR. They are applicable and indispensable in merchandising scenarios but not well-tailored to the data subject's expectations who opt for this lifestyle. The right to information and its associated rights in Art. 12-15 GDPR concretize the controller's obligation to inform and provide a new type of right to enable the data subject to obtain a copy of personal data undergoing processing. As cumbersome as it may seem, the merchandiser in an authorized case can meet compliance requirements through programmatic measures. It is recommended that the merchandiser stores personal data about the data subject's identity, the raw data about original photos, and the data of the final advertising image separately, as well as keep proper documentation.

The right to rectification in Art. 16 GDPR is not valuable in merchandising cases because the data subject must prove inaccuracy in data processing. Thus, the data subject cannot require the data controller to modify the data following his or her preferences. An *ex post* claim of this right would again draw people's attention to the wrongful merchandising, whereas an *ex ante* claim would be hardly needed because the presentation of the data subject's likeness is supposed to be appealing as a device for attention-grabbing and image-transfer. The right to erasure in Art. 17 GDPR is a corollary of unlawful or unnecessary data processing stemming from the principles of lawfulness and data minimization. Therefore, as data processing for merchandising relies on the anytime revocable consent of the data subject, this right is impactful in eliminating records of the data processing. The data subject may claim the right to portability in Art. 20 (1) GDPR to transmit the identification data and raw data for photographs, but not the data concerning edited photos, information relating to the merchandiser, or the goods/services being advertised. The data subject may also ask the controller to transmit these personal data to another controller designated, but any further use of the original photographs is prohibited due to copyright. Trade secrets would be a possible objection if information about the cooperation or new products has not been disclosed yet.

5. Conclusions

Following the subjective approach of Art. 9 (1) GDPR with an emphasis on the reverse burden of proof, merchandisers who use personal photos

as a device for attention-grabbing or image-transferring can be excluded from Art. 9 GDPR by demonstrating that no sensitive information is being processed under the GDPR. The underlined rationale here is that merchandising differs from the data processing concerned by the GDPR because merchandising is to increase publicity of the data subject and ultimately the goods/service advertised by the data subject. In contrast, data processing aims to extract more information from the photo.

Nevertheless, the high-level data protection facilitated by rigorous conditions of lawful grounds and the mandatory data subject's rights is generally very costly and unfriendly to authorized merchandising and likely to make it unsustainable.

Against the backdrop that Art. 6 (1) (b) GDPR is not appliable in merchandising scenarios as data processing is the main performance of these contracts, the anytime revocable consent according to Art. 6 (1) (a) in combination with Art. 7 (3) GDPR renders merchandising contracts not binding anymore. Reflected in the *landlady* case, merchandising contracts as licensing agreements regarding personal data are in general at risk of being disregarded under the GDPR. In practice, long-term cooperation between the data subject and the controller, as well as the first controller and the second one (sub-licensee), would be hardly feasible because controllers would lack a reliable legal status to invest. Efforts are made to mediate the conflict between the principle of *pacta sunt servanda* and the anytime revocable consent under the GDPR. However, they all suffer from several flaws, including strict and overly narrow prerequisites, compromising the GDPR's high-level data protection, and ignoring the EDPB and EDPS's objections to commercialization of personal data.

Moreover, the rigorous conditions for validity are likely to render consent voluntarily given by data subjects invalid and consequently, the data processing. It deviates from the genuine will of the individual. *Vice versa*, Controllers in authorized merchandising cases are facing insurmountable obstacles. Besides the free revocable consent that would discourage them from making a significant and sustained investment in merchandising, it is almost impossible for agencies to prove that the consent given by young models is genuine and voluntary provided on the strong structural inequity. The *company-advertising* case is a prime example of how the strong protection offered by the GDPR could make ordinary merchandising very costly. Since the controller failed to notify the revocability of consent according to Art. 7 (3) GDPR, consent given by the data subject was invalid as his control over personal data was compromised in a significant way.

Apart from compliance requirements for the legality, the GDPR requires data controllers to establish mechanisms for responding to the rights of data subjects including the right to information and its associated rights, the right to rectification, the right to erasure ("right to be forgotten"), and the right to data portability. Although they are applicable and non-negotiable in merchandising contracts, there are significant questions about their suitability and effectiveness in relation to the expectations of the data subject who chooses the publicity voluntarily.

As a result, while the cost for compliance is transferred to controllers, the uneven protection for data subjects is not necessarily ideal for them. It is conceivable that data controllers would rely on their *de facto* capacity and power to weaken the negative impact of revocable consent. In other words, the more the data subject relies on the services the controller provides, the more difficult it is to withdraw consent and the more *de facto* similar to a contractual relationship.