Privacy-compliant design of Cookie Banners according to the GDPR

by **Gerald Spindler and Lydia Förster***

Abstract: Cookie banners appear on almost every website or application we access, but as often as they appear, as rarely do they comply with mandatory (data protection) laws. This is mainly due to the abundance of - partly diverging - regulations on national and international level. This article attempts to evaluate relevant legislative acts as well as European Guidelines, Recommendations and Decisions to determine what a privacy-compliant consent banner should contain.

Keywords: Cookie Banner; Dark Patterns; Cookies; Consent Banners; GDPR; Consent

Recommended citation: Gerald Spindler and Lydia Förster, Privacy-compliant design of Cookie Banners according to the GDPR, 14 (2023) JIPITEC 2 para 1.

A. Introduction

1 The General Data Protection Regulation has now been in force for 4 years. Its declared aim is to strengthen the fundamental right of the protection of personal data. One of the key elements in this context is the obligation of the data processor to obtain consent of the data subject. In this regard, users shall be given the opportunity to make a voluntary, specific and informed declaration of consent or refusal for each process that concerns their personal data. In the digital space, consent tools are typically used to request the consent of the data subject. When deploying and using these consent tools, it is also a basic principle that they must enable a granular, free and informed decision. However, this theoretical approach is at odds with current practice—a recent study conducted by the Federation of German Consumer Organisations (vzbv) concluded that one in ten consent tools (in form of a cookie banner) is illegal.[1] Consumer surveys in recent years have also repeatedly shown that consumers do not feel informed about what happens to their data and do not trust the processors.[2] However, this is not surprising, as 141-page cookie banners without reject-button are common practice.[3]

[*] Prof. Dr. Gerald Spindler is holder of the chair of Civil Law, Commercial and Economic Law, Comparative Law, Multimedia- and Telecommunication Law and head of the Institute for Business Law at the University of Göttingen, Germany and Lydia Förster is Ph.D. student at Prof. Spindler's chair at the University of Göttingen and research assistant at YPOG Law in Hamburg.

[1] A total of 949 websites were examined, in detail: Federation of German Consumer Organisations <www.vzbv.de/pressemitteilungen/jedes-zehnte-cookie-banner-ist-klar-rechtswidrig> accessed 11 December 2022.

[2] European Commission, 'Special Eurobarometer 431 Data Protection Report' (2015), p. 66 <https://slidelegend.com/eurobarometer-431-european-commission-europa-eu_59b42a331723dd6c7341efd0.html> accessed 11 December 2022; Bitkom, 'Datenschutz in der digitalen Welt' (2015), p.7 <www.bitkom.org/sites/default/files/file/import/Bitkom-Charts-PK-Datenschutz-22092015-final.pdf> accessed 11 December 2022.

[3] A Cookie Banner like this was for example used by the online news service *Focus online* (belonging to the media company *Burda Media)*, but was recently declared invalid by Regional Court Munich, since such an overlong banner, which does

2 One of the reasons for this disappointing result is that in addition to the GDPR, there are other area-specific regulations such as the ePrivacy Directive, and the Telecommunications Telemedia Data Protection Act (TTDPA). It is difficult to extract a clear guideline from this complex set of regulations, especially since none of the laws provides precise specifications regarding the concrete design of digital consent tools. Thus, the aim of this article is to determine which standards apply to obtaining consent in the digital space and to what extent. Furthermore, the specific design of a consent tool according to these standards will be assessed.

3 To this end, the functionality of cookies is first explained (B.) and a legal classification of cookies is made in order to determine which legal norms are applicable (C.). The focus will then shift to the question of whether consent is required under these standards and what requirements must be met for effective consent (D. and E.). Simultaneously, the relationship between the relevant provisions have to be evaluated to provide a precise legal assessment. Finally, this theoretical background is complemented by a chapter on the implementation of the specifications in practice (F.). The problems of consent tools will also be highlighted (G.). The study concludes with an overview of alternative consent methods (H.).

B. (Technical) Principles

4 The term cookies refers to small data files created by a web server or a script that can be placed on computers, smartphones, and other smart devices.[4] They usually store and transmit certain information about preferences like, e.g., user name, language, and (browsing) activities on visited websites to the provider of the cookie[5], who does not have to be identical to the operator of the website (*Third-party Cookie*).[6] The information the cookie stores vary, but it contains at least the name of the web server, from which it was created and a unique identifier (*Cookie-ID*), which enables the web server to recognize a user.[7]

I. Structure and functioning of HTTP Cookies

5 Cookies are simple text files consisting of a *Name* and a *Value*.[8] The cookie is either sent to the browser by the web server or created in the browser by a script (e.g. Javascript). The web server can then read the information directly from the server when the page is visited or transfer the information to the server via the website's script. Cookie information is stored locally on the particular device in the browser.[9] During a revisit to a particular website, the client browser searches for all cookies of this domain that match the web server and the directory path of the current request.[10]

II. Types of cookies

1. Technically necessary cookies

6 Technically necessary cookies are indispensable to be able to use a website and its basic functions. They serve, for example, to maintain the login over the duration of the visit to a website.[11]

2. Performance cookies

7 These types of cookies store information about how a website is used, for example, how long it takes for web pages to load, how the website performs with different browsers, or whether any errors have

not even contain an easily accessible reject button, ensures neither the voluntariness nor the informedness required for consent according to the TTDPA in conjunction with the GDPR, Regional Court Munich, Decision of 29 November 2022 – 33 O 14766/19, pp. 194 ff.

[4] Philipp Hacker, *Datenprivatrecht* (1st edn, Mohr Siebeck 2020) 27; Lisa Gradow, Ramona Greiner, *Quick Guide Consent Management* (Springer, 1st edn 2021) 5; detailed on the types and functioning of cookies: Stefan Ernst, 'Cookies nach der EuGH-Entscheidung "Verbraucherzentrale Bundesverband/Planet49"' [2020] WRP, 963.

[5] Gradow, Greiner (n 4) 6.

[6] Hacker (n 4) 27.

[7] Marian Arning, Tobias Born, 'Information als Wirtschaftsgut' in Nikolaus Forgó, Marcus Helfrich, Jochen Schneider (eds), *Betrieblicher Datenschutz* (3rd edn, C.H. Beck 2019, Part XI. chap. 2) para. 51.

[8] Stefan Hanloser, 'Geräte-Identifier im Spannungsfeld von DS-GVO, TMG und ePrivacy-VO' [2018] ZD 213 (214 f.).

[9] Hacker (n 4) 27.

[10] Céline Wenhold, *Nutzerprofilbildung durch Webtracking* (1st edn, Nomos 2018) 56 f.

[11] Ernst (n 4) 963.

occurred. The information is usually aggregated and used to improve the functioning of a website.[12]

3. Functional cookies

8 These types of cookies are primarily designed for the user's convenience, as they store information about their preferences, such as language settings and usernames or text size adjustments.[13]

4. Tracking/marketing cookies

9 Finally, tracking or marketing cookies collect information that help the provider (usually a third party) to place personalised advertising. They store, e.g., information about the frequency of access and the processed content. Advertising cookies enable behavioural information to be stored as part of the management of advertising by observing habits, which creates a profile of the user's preferences to be able to offer advertising customised to the interests of their profile.[14]

C. Legal classification of cookies

10 The first step in clarifying how the use of cookies can be legally compliant is to determine how they are classified legally, and which norms and regulations apply to them.

I. Personal data according to the GDPR

11 To fall within the scope of the application of the GDPR, the information stored by the cookies would have to be considered "personal data" within the meaning of Article 4 No. 1 GDPR. According to Art. 4 No. 1 GDPR, personal data is any information that relates to an identified or identifiable individual. "Identifiable" means any person who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. In determining whether a natural person is identifiable, Recital 26 GDPR states that the account shall be taken of all the means reasonably likely to be used by the controller or by any other person to identify the natural person. This means that the identifiability does not only apply to data that establishes a reference in itself, but also to data that must first be linked to further information (possibly with the help of third parties).[15] In determining whether the means are reasonably likely to be used to identify the natural person, any objective factors, such as the cost of identification and the time required, shall be taken into account, including the technology and technological developments available at the time of the processing, compared with Recital 26 GDPR. However, the extent to which also the (potential) knowledge and the (potential) means of third parties must be taken into account is disputed; more precisely, there is dissent as to whether every possibility of a reference to a person by a third party leads to identifiability (absolute approach[16]), or whether the focus lays mainly on the responsible person and their resources (relative approach[17]). The dispute already existed before the GDPR came into force and centered on the concept of determinability.[18] However, even with the enactment

[12] Ernst (n 4) 963.

[13] Ernst (n 4) 963.

[14] Ernst (n 4) 963.

[15] Stefan Ernst, 'Art. 4 DS-GVO' in Boris Paal, Daniel Pauly (eds), *Datenschutz-Grundverordnung* (C.H. Beck, 3rd edn 2021) para 12; Moritz Karg, 'Art. 4 Personenbezogenes Datum' in Spiros Simitis, Gerrit Hornung, Indra Spiecker gen. Döhmann (eds), *Datenschutzrecht* (Nomos, 1st edn 2019) para 46; Peter Gola, 'Art. 4' in Peter Gola (ed), *DS-GVO Kommentar* (2nd edn, C.H. Beck 2018) para 16; Achim Klabunde, 'Art. 4' in Eugen Ehmann, Martin Selmayr (eds), *DS-GVO Kommentar* (2nd edn, C.H. Beck 2018) para 17; Jürgen Kühling, Manuel Klar, 'Art. 4' in Jürgen Kühling, Benedikt Buchner (eds), *Datenschutz-Grundverordnung BDSG Kommentar* (3rd edn, C.H. Beck 2020) paras 20 ff.; Alexander Arning, Tobias Rothkegel, 'Art. 4 DSGVO' in Jürgen Taeger, Detlev Gabel (eds), *DSGVO – BDSG – TTDSG* (4th edn, R&V 2022) para 30.

[16] Benedikt Buchner, 'Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO' [2016] DuD 155 (156); Max Dregelies, 'Wohin laufen meine Daten?' [2017] VuR 256 (257); in this direction Klabunde (n 15) Art. 4 para 17 according to whom it is sufficient that any third party carries out the identification, but this must at least be generally probable; also in this direction: Stefan Herbst, 'Was sind personenbezogene Daten?' [2016] NVwZ 902 (906) who speaks of a *factual-absolute* personal reference.

[17] Klar, Kühling (n 15) DS-GVO Art. 4 para 26; Johanna Hofmann, Paul Johannes, 'DS-GVO: Anleitung zur autonomen Auslegung des Personenbezugs' [2017] ZD 221 (225 f.); Arning, Rothkegel (n 15) DS-GVO Art. 4 para 31; Jens Eckhardt, 'Anwendungsbereich des Datenschutzrechts – Geklärt durch den EuGH?' [2016] CR 786 (789).

[18] For a detailed explanation of the previous controversy on the interpretation of the concept of *determinability* with

of the GDPR, it could not be conclusively clarified; the spectrum ranges as already mentioned from a strictly absolute approach, according to which any way of linking leads to identifiability, including illegal ways, to a strongly relative approach, according to which it only depends on the person processing the data.[19] However, based on the GDPR and the recent case law of the CJEU, the following picture emerges:

12 Due to the fact that the text of the GDPR is ambiguous, its interpretation is ultimately not completely conclusive. Nevertheless, what can be stated is that the GDPR and the case law of the CJEU, especially when viewed together, tend towards a relative approach, albeit with some objective criteria.[20]

13 According to Recital 26 (3) GDPR, all means must be considered that are generally likely to be used by the controller or a third party to identify the natural person directly or indirectly. This is not a conclusive statement, as it does not specify when this probability exists and how wide the range of means considered is to be drawn. In any case, however, it is a rejection of the extremely relative theory, according to which only the responsible person's means are to be considered.[21] The wording of Recital 26 is explicitly broader in this respect. Thus, the resources of third parties must also be considered.

14 A further specification of the resources to be included was made by the CJEU in its *Breyer* ruling: According to this the effort, the actual availability, and also the legal permissibility of access to the knowledge or the relevant methods must be taken into account.[22] Prohibited methods were thus explicitly excluded by the CJEU.[23] However, the scope of application is also broadly drawn so that not only the knowledge and methods of the third party are relevant, but also whether the third party can establish a reference with the help of the participation of a fourth party.[24] Overall, this means that for the identifiability, the knowledge and resources of third parties must be taken into account when they are legally permitted and to a certain extent probable; purely fictitious possibilities must be disregarded.[25] In this regard, however, it should be critically noted that legal admissibility cannot be the primary criterion and illegal means cannot be excluded per se.[26] On the one hand, this results from the wording of Recital 26, which states that, in principle, all factors should first be included, insofar as their use is sufficiently probable. The fact that some methods are illegal does not make them generally unlikely. Instead of focusing on the abstract status of illegality or conformity with the law, the focus should rather be on whether the factual proximity and thus the possibility of using the data for identification is given.[27] According to the Article 29 Data Protection Working Party, a mere hypothetical possibility, in turn, is not enough to consider a person as identifiable.[28]

15 Thus, the term "all the means likely reasonably to be used" in Recital 26 include several factors such as the costs of conducting identification, the way the processing is structured, the advantage expected by the controller, "the intended purpose, the interests at stake for the individuals, as well as

further references see Matthias Bergt, 'Die Bestimmbarkeit als Grundproblem des Datenschutzrechts Überblick über den Theorienstreit und Lösungsvorschlag' [2015] ZD 365 and Stefan Brink, Jens Eckhardt, 'Wann ist ein Datum ein personenbezogenes Datum? Anwendungsbereich des Datenschutzrechts' [2015] ZD 205.

[19] In detail with further reference: Herbst (n 16) 903 ff.

[20] This finding is also reached by Klar, Kühling (n 15) DS-GVO Art. 4 para 26; Niko Härting, 'Datenschutz-Grundverordnung Anwendungsbereich, Verbotsprinzip, Einwilligung' [2016] ITRB 36 (36 f.); Florian Jotzo, *Der Schutz der personenbezogenen Daten* (Nomos, 2nd edn 2020) Part 2 Sachlich anwendbares Datenschutzrecht paras 97 f.; Wolfgang Ziebarth, 'Art. 4 DSGVO' in Gernot Sydow, Nikolaus Marsch (eds), *Europäische Datenschutzgrundverordnung* (3rd edn, Nomos 2022) para 37; In this direction: Peter Schantz, 'Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht' [2016] NJW 1841 (1843).

[21] Peter Meyerdierks, 'Sind IP-Adressen personenbezogene Daten?' [2009] MMR 8 (12) on the principle of determability.

[22] CJEU Case C-582/14 *Breyer/Germany* [2016] ECLI:EU:C:2016:779 paras 42 ff.

[23] CJEU Case C-582/14 *Breyer/Germany* [2016] ECLI:EU:C:2016:779 para 46.

[24] CJEU Case C-582/14 *Breyer/Germany* [2016] ECLI:EU:C:2016:779 para 43.

[25] Arning, Rothkegel (n 15) DS-GVO Art. 4 para 35; Ernst (n 15) DS-GVO Art. 4 paras 10 f.; Klar, Kühling (n 15) DS-GVO Art. 4 para 28; Klabunde (n 15) DS-GVO Art. 4 para 17.

[26] Affirmative: Herbst (n 16) 905; Karg (n 15) Art. 4 „Personenbezogenes Datum" para 64; disapproving: Peter Meyerdierks (n 21) 11 f. to the former legal situation on the interpretation of the concept of *determinability*.

[27] Georg Borges, 'DSGVO Art. 4' in Georg Borges, Marc Hiller (eds), *BeckOK IT-Recht* (7th edn, C.H. Beck 1.7.2021) para 20; Herbst (n 16) 905; Art. 29 Data Protection Working Party Opinion 4/2007 on the concept of personal data, WP 136, 01248/07/EN, 19.

[28] Art. 29 Data Protection Working Party (n 27) 15.

the risk of organisational dysfunctions (e.g. breaches of confidentiality duties) and technical failures".[29]

16 When applied to cookies, the result is as follows: Cookies themselves do not allow the identity of the user to be determined, as they do not contain any real names or similar directly identifying information.[30]

17 Beyond this, a distinction must be made: if the cookie merely stores user preferences or similar information in anonymous forms so that they can be retrieved when the website is closed and revisited, there will generally be no personal reference.[31] However, a different finding is reached if additional information is available. Both cookie information and the additional information must allow for identification when viewed together.[32] This applies in particular if a Cookie-ID is assigned, and the information is not stored anonymously. Usually, other digital traces (e.g. the IP address, log-in data) are left on visited websites, which, in combination with the unique Cookie ID, enables an identification.[33] This view seems to be shared by the CJEU, which determined that identifiability can be given if there is the possibility of merging cookies and the registration data entered on the website.[34] In addition, a personal reference may also exist if several cookies are combined to create a user profile, for example, to be able to show personalized advertising to the user.[35] This also results indirectly from Recital 30 and Article 4 No. 11 GDPR, which provide that profiling, including the creation of user profiles by combining and evaluating personal data, falls within the scope of the GDPR and explicitly mention cookies as a possible data basis for profiling.

18 Overall, no general statement can be made. A case-by-case examination is always necessary: cookies are personal data if they, together with other information or other cookies, enable a concrete reference to a person. This is particularly likely if the user is assigned a unique Cookie-ID. In addition, a reference to a person can also exist if the combination of cookies enables a unique user profile so that the reference to a specific person is given. If several parties are involved in the data collection and processing, identifiability is not precluded automatically. In this case, it must be examined whether the reference can be established by the responsible person and the third party with sufficient probability using the available means.

II. Storage of or access to information according to the ePrivacy Directive

19 Based on Article 5 (3) ePrivacy Directive 2002/58/EC[36], the regulations of the Directive are applicable when either information is stored on the user's terminal equipment or when stored information is accessed. This corresponds to the way cookies function: they store information in the browser and thus on the user's device to retrieve it directly or subsequently.[37] While this already opens the scope of application of the directive, it can be further stated that the Directive does not distinguish between personal and non-personal information.[38] Instead, all types of information are covered by Article 5 (3).[39] The relationship of both the ePrivacy Directive as well as any corresponding transposition legislation

[29] Art. 29 Data Protection Working Party (n 27) 15.

[30] Klar, Kühling (n 15) DS-GVO Art. 4 para 36; Peter Schmitz, in Thomas Hoeren, Ulrich Sieber, Bernd Holznagel (eds), *Handbuch Multimediarecht* (58th edn, C.H. Beck March 2022) Part. 16.2 para 76.

[31] Anno Haberer, 'Anforderungen an Cookie-Banner' [2020] MMR 810 (811).

[32] Borges (n 27) DS-GVO Art. 4 para 25; Klar, Kühling (n 15) DS-GVO Art. 4 No. 1 para 36.

[33] This is also indicated by recital 30 GDPR.

[34] CJEU Case C-673/17 *Planet49* [2019] ECLI:EU:C:2019:801 paras 45, 69.

[35] Ulrich Baumgartner, Guido Hansch, 'Onlinewerbung und Real-Time-Bidding' [2020] ZD 435 (436).

[36] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, 37 ff.

[37] Schmitz (n 30) Part. 16.2 para 76; Louisa Specht-Riemschneider, ‚Verbraucherdatenschutzrecht' in Louisa Specht, Reto Mantz (eds), Handbuch Europäisches und deutsches Datenschutzrecht (1st edn, C.H. Beck 2019) Sec. 9 Verbraucherdatenschutz para 63; Andreas Sesing, ‚Cookie-Banner – Hilfe, das Internet ist kaputt!' [2021] MMR 544.

[38] Specht-Riemschneider (n 37) Sec. 9 Verbraucherdatenschutz para 66; Wolf-Tassilo Böhm*, Valentino* Halim, 'Cookies zwischen ePrivacy und DS-GVO – was gilt?' [2020] MMR 651.

[39] Other opinion by the Danish Business authority which stated that the recording of MAC addresses of users' mobile devices is not subject to the requirements of providing information and obtaining consents from the users under the Danish Cookie Order, which implements Art. 5(3) of the ePrivacy Directive because no identification is possible; rightly critical of this opinion: Charlotte Tranberg, Storing Information on User's Devices [2015] EDPL 130 (136).

(Section 25 TTDPA) to other legal acts, in particular the GDPR, will also be of importance for the further course of the paper and has to be assessed in detail.[40]

III. Storage of or access to information according to the TTDPA

20 The Telecommunication-Telemedia-Data-Protection-Act (TTDPA) has come into force on 1 December 2021 and serves to adapt the TCA and the TMA to the GDPR, as well as to implement the ePrivacy Directive.[41] Primarily, the legal uncertainties caused by the coexistence of several laws should be eliminated.[42] According to Section 1 No. 2 TTDPA, the TTDPA focuses on the protection of data when using telecommunications services and telemedia. Pursuant to Section 2 (2) No. 1 TTDPA, a provider of telemedia is any natural or legal person, who provides their own telemedia services or those of a third party, participates in the provision of or provides access to the use of their own or third-party telemedia mediates. According to Section 1 (1) S. 1 TMA, telemedia are all electronic information and communication services, unless they are telecommunications services, telecommunications-based services, or broadcasting. The term telemedia services thus includes online offers of goods and services with the possibility of direct ordering, video on demand, internet search engines, but also "simple" homepages.[43] For the definition of the telecommunications provider, the TTDPA refers in Section 2 (1) TTDPA to the amended Telecommunications Act. In addition to so-called number-based interpersonal telecommunications services, the amended TCA now also covers number-independent interpersonal communications services according to Section 3 TCA. This means that "*over-the-top (OTT)*"[44] communication services, such as messengers like WhatsApp, also constitute telecommunications services.[45]

21 Section 25 TTDPA is particularly relevant for the use of cookies, and closely follows the wording of the ePrivacy Directive: the provision is applicable when information is stored on the user's terminal equipment or when such information is accessed. In this context, it is irrelevant whether this information is personal data or not. As explained above, this is precisely how cookies are designed to function.

IV. Excursus: processing of information according to the ePrivacy Draft Regulation

22 The ePrivacy Regulation was originally intended to come into force at the same time as the GDPR and to introduce specific regulations for the area of electronic communication that would specify and supplement the general regulations of the GDPR.[46] This makes it particularly relevant for the use of cookies, but the planned introduction failed—no agreement has been reached to this day. Trialogue negotiations with the Parliament and the Commission are ongoing.[47] Although an agreement is not to be expected soon, an overview of the legal requirements of the current draft of the ePrivacy Regulation for cookies should be provided: According to the current draft of the ePrivacy Draft Regulation, it applies to the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services and to information related to the terminal equipment of end-users, compared with Article 2 ePrivacy Draft Regulation. In contrast to the GDPR, the applicability does not depend on the content of the information; similar to the ePrivacy Directive the regulation is supposed to apply to non-personal data as well[48], so

[40] Cf. part D.3.

[41] Bundesregierung, 'Explanatory Memorandum to the government draft', BT-Drs. 19/27441, 1.

[42] Bundesregierung, 'Explanatory Memorandum to the government draft', BT-Drs. 19/27441, 1.

[43] Gesellschaft für Datenschutz und Datensicherheit e.V., 'GDD-Praxishilfe: Das neue TTDSG im Überblick' (June 2021) 3.

[44] Services that are offered via an Internet connection without the Internet service provider having providers themselves have any influence or control over the service would have. OTT services are therefore decoupled from the infrastructure providers.

[45] Thomas Wilmer, in Anne Riechert, Thomas Wilmer (eds), *TTDSG* (1st edn, Erich Schmidt Verlag 2022) § 2 para 6.

[46] Cf. European Commission, 'Explanatory memorandum for the proposal 2017/0003(COD)', Part. 1.1. Reasons for and objectives of the proposal.

[47] In detail on the legislative procedure until the recent Trilogue negotiations Pascal Schumacher, Lennart Sydow, Max von Schönfeld, 'Cookie Compliance, quo vadis?' [2021] MMR 603 (605).

[48] Critical in this regard: Nils Rauer, Diana Ettig, 'Rechtskonformer Einsatz von Cookies' [2018] ZD 255 (257) who criticize that this creates disincentives.

according to Article 8 (1) ePrivacy Draft Regulation, all information from terminal equipment of end users is placed under a processing ban.

D. Requirement for consent

23 First of all, it must be clarified whether and from which regulations a requirement for consent arises, which requirements are placed on the respective consent, and when which consent is required.

I. Requirement for consent according to the GDPR

24 Article 6 GDPR regulates the lawfulness of data processing. In addition to consent under Article 6 (1) lit. a GDPR, processing can also be based on other reasons, which are, however, largely excluded from this analysis. Accordingly, it must first be explained for which types of cookies consent is required under the GDPR and which cookies can generally be based on other legal grounds.

25 Besides consent, the necessity for the fulfillment of the contract according to Article 6 (1) lit. b GDPR or the legitimate interest according to Article 6 (1) lit. f GDPR come into consideration. Necessity is interpreted rather narrowly: a simple connection of the data processing to the contract is not sufficient.[49] Instead, it must be indispensable to achieve the purpose of the contract.[50] In the digital context, a rough guideline is: if the website or the app does not function properly without the cookie, there is a necessity for the placement of the cookie.[51] This will be the case in particular for technically necessary cookies, which is why these usually do not require consent.[52] For all other types of cookies, it must be examined whether there is a legitimate interest within the meaning of Article 6 (1) lit. f GDPR. In principle, economic interests are not excluded[53], which is likely to be particularly relevant for advertising cookies. Nevertheless, this interest must always be weighed against the interests, fundamental rights, and freedoms of the data subject.[54] No general statements can be made, as trends will only become apparent through future decisions in the course of the next few years. However, freedoms protected by fundamental rights, such as the right to informational self-determination, shall principally be weighted higher than interests protected by simple law, like e.g. pure profit maximization.

26 Overall, it can be concluded that only technically necessary cookies are usually exempted from the consent requirement; for all other types of cookies, a thorough examination must take place, which will probably often lead to consent being required, especially for advertising and tracking cookies.[55]

II. Requirement for consent according to the ePrivacy Directive

27 In accordance with Article 5 (3) ePrivacy Directive, consent is also required for the storage or assessment of information on terminal equipment. However, pursuant to Article 2 lit. f and Recital 17 ePrivacy Directive in combination with Article 94 (2) GDPR, consent is governed by the Data Protection Directive, which has been replaced by the GDPR. This means that the principles of Article 4 No. 11 and Article 7 GDPR also apply to consent under the ePrivacy Directive. Therefore, the requirements for consent according to Article 5 (3) ePrivacy Directive do not differ from the requirements according to Article 4 No. 11 and No. 7 GDPR. Thus, reference can be made to the explanations given above.

28 Similar to the GDPR, the ePrivacy Directive provides for an exception to the consent requirement in case of necessity. According to Article 5 (3) s. 2 ePrivacy Directive, storage or access is permitted if it is strictly necessary in order to provide the information service requested by the user. Again, the Article 29 Working Party advocated for a narrow interpretation of necessity, which would only exist if the functionality of the service could not be

[49] Marion Albers, Raoul-Darius Veit, 'Art. 6 DSGVO', in Heinrich Amadeus Wolff, Stefan Brink (eds), *BeckOK DatenschutzR* (41th edn, C.H. Beck 01.11.2021) DS-GVO Art. 6 para 44; Sebastian Schulz, 'Art. 6' in Peter Gola (ed), *DS-GVO Kommentar* (2nd edn, C.H. Beck 2018) para 38; Eike Michael Frenzel, 'Art. 6 DSGVO', in Boris Paal, Daniel Pauly (eds), *Datenschutz-Grundverordnung* (3rd edn, C.H. Beck 2021) para 14.

[50] Horst Heberlein, 'Art. 6 DS-GVO', in Eugen Ehmann, Martin Selmayr (eds), *DS-GVO Kommentar* (2nd edn, C.H. Beck 2018) para 13; Jürgen Taeger, 'Art. 6 DSGVO' in Jürgen Taeger, Detlev Gabel (eds), *DSGVO – BDSG – TTDSG* (4th edn, R&V 2022) para 49; Schulz (n 49) para 38; Albers, Veit (n 49) para 44.

[51] Also: Gradow, Greiner (n 4) 10 f.; Haberer (n 31) 810 (815).

[52] Sesing (n 37) 545; Haberer (n 31) 812.

[53] Conference of the Independent Data Protection Authorities of the Federal State and the *Länder* (DSK), 'Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien' (March 2019) 11.

[54] CJEU Case C-40/17 *Fashion ID/Verbraucherzentrale NRW* [2019] ECLI:EU:C:2019:629 para 95.

[55] DSK (n 53) 10.

guaranteed without the cookie.[56] The simplification or acceleration of certain processes by a cookie is not sufficient to affirm a necessity.[57] This will usually apply to technically necessary cookies. Article 29 Working Party mentions—among others as examples of the exception—*User input cookies*[58], which, for example, store which items have been placed in the shopping basket on a shopping site, or *authentication cookies*[59], which serve to recognize a person who has logged in once as being logged in again and to provide them with access to the specific content (e.g. in online banking). According to the group, the exceptions explicitly do not include tracking cookies of social plug-ins, third party advertising cookies, and first party analysis cookies.[60] This seems only consistent in view of the strict interpretation of necessity, as these do not have a positive influence on the functionality of the website, but rather serve the processors.[61]

III. Requirement for consent according to the TTDPA

29 Initially, it should be noted that the TTDPA also applies to entities that do not have their registered office in Germany. According to Section 1 (3) of the TTDPA, the scope of application extends to all companies or persons that have a German branch office, provide goods or services on the German market, or participate in the provision of services. This combination of the market location principle and the country-of-origin principle establishes a very broad scope of application. Consent is also required under Section 25 (1) TTDPA. However, reference is also made to the GDPR with regard to requirements of a lawful consent. This means that the handling of personal and non-personal data will be assessed according to the GDPR. The above statements on consent apply accordingly. With regard to exceptions, the provisions of the ePrivacy Directive are followed closely. According to Section 25 (2) No. 2 TTDPA consent is not required if the storage of information in the end user's terminal equipment or the access to information already stored in the end user's terminal equipment is absolutely necessary so that the provider of a telemedia service can provide a telemedia service expressly requested by the user. Based on the narrow interpretation of the term under the ePrivacy Directive as proposed by the Article 29 Working-Party[62], mainly technically necessary cookies are likely to be excluded. For all other types, a case-by-case assessment is required, especially advertising and tracking cookies will generally not be *necessary*.

30 However, the scope of application of the TTDPA alongside the GDPR still needs to be clarified. The TTDPA is independent of content and therefore also applies if there is no personal data within the meaning of the GDPR, and also if no processing within the meaning of Article 4 No. 2 GDPR has been carried out. The exclusive scope of application of the TTDPA is thus not very large, which leads to the question of which law applies when a process falls within the scope of application of both standards. Since Section 25 of the TTDPA is the long-demanded implementation of the Article 5 ePrivacy Directive, Article 95 GDPR could possibly intervene and lead to a sector-specific priority of the TTDPA. However, the standards would have to pursue the same objectives. This is not the case: the TTDPA, and in particular Section 25 of the TTDPA, aims to protect the equipment's integrity, which becomes clear in several places. As already explained, information is protected regardless of its personal reference, and the protected person can also be a legal entity. The GDPR, on the other hand, only aims to protect personal data and thus the right to informational self-determination of the individual, which is why the priority rule from Article 95 GDPR does not apply. The explanatory memorandum to the draft legislation also indicates that it was not intended that the GDPR would also be superseded via Article 95 GDPR with regard to the processing of personal data, as it states that the subsequent use of data (i.e., the use after accessing or storing non-personal information) will continue to be governed by general data protection law, in particular by the GDPR.[63]

31 In the area of telemedia services, however, the demarcation is hardly of any significance, since on the one hand the storage of non-personal information is usually the preliminary stage to the storage and processing of personal data, and on the other hand the requirements for consent are identical. Consent under the TTDPA and the GDPR can also be bundled and given by the same act. This avoids a situation where the user, after giving consent under the TTDPA, has to give practically

[56] Art. 29 Data Protection Working Party, Opinion 04/2012 on Cookie Consent Exemption, WP 194, 00879/12/EN, p. 4.

[57] Charlotte Tranberg, Storing Information on User's Devices [2015] EDPL 130, 133.

[58] Art. 29 Data Protection Working Party (n 56) 6.

[59] Art. 29 Data Protection Working Party (n 56) 6f.

[60] Art. 29 Data Protection Working Party (n 55) 9ff.

[61] Supporting this view *Ernst*, WRP 2020, 962 (967).

[62] Art. 29 Data Protection Working Party (n 56) 6ff.

[63] Explanatory Memorandum to the government draft, BT-Drs. 19/27441, p. 38.

identical consent under the GDPR a few seconds later. However, it must be clear to the users that they are consenting to multiple things by clicking a single button.[64]

IV. Excursus: consent according to the ePrivacy Draft Regulation

32 According to Article 8 (1) ePrivacy Draft Regulation, consent is also required for the use and storage of information on the user's terminal equipment, where reference is also made to the GDPR for the definition and prerequisite. According to Article 9 of the proposed ePrivacy Regulation, the definition of and the conditions for consent provided for in Article 4 (11) and Article 7 GDPR apply. In consequence, obtaining consent under both the GDPR and the proposed ePrivacy regulation follows the same rules.[65] Thus, the results found above are in principle similarly applicable.[66]

33 However, the revocation provision in Article 7 (3) GDPR is supplemented by an obligation to remind the end user of his right of revocation every six months, cf. Article 9 (3) ePrivacy Draft Regulation. In addition, the strict limitation of purpose is loosened in Article 9 (2) ePrivacy Draft Regulation to the effect that it should be possible to give general consent to the use of cookies through the settings of the Internet browser.

V. Excursus: consent according to the IAB Transparency and Consent Framework & other industry guidelines

34 In recent years, large industry associations such as *IAB Europe*[67] and other firms like *ISiCO*[68] have also published data protection guidelines[69] that can supposedly be used to design consent tools in compliance with the GDPR.[70] According to IAB Europe, the Transparency & Consent Framework (TCF) is intended to create a legally compliant standard "*by the industry for the industry*" that will provide a standardized solution for obtaining consent in accordance with the ePrivacy Directive and the GDPR.[71] With its system, IAB Europe wanted to satisfy two industry needs at once: first, it should be made easier to serve personalized advertising, and second, it is intended to simplify the process of obtaining advertising consent.

35 The IAB tool is in the advertising industry particularly popular for so-called "real time bidding"[72] to facilitate the management of user preferences for personalized advertising. When accessing websites connected to the tool and the associated platform developed by IAB Europe, users are asked to consent to the processing of their personal data for advertising purposes. The system generates a user ID, collects information on this ID and enables the cross-service storage of the respective user's settings for the services connected to the TCF (so-called *Consent String*). When the user accesses a connected service that offers personalizable advertising space, the Consent String provides information about whether and which advertising is displayed to the user by feeding all available information into the

[64] DSK, 'Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien' (December 2021) 9.

[65] European Data Protection Board, Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications, 25.05.2018, p. 2.

[66] Cf. Part D.1.

[67] The *Interactive Advertising Bureau Europe* is a global business organization in the online advertising industry with over 650 members, including global players such as *Google* and *Facebook.*

[68] The *Informationssicherheit und Datenschutz Compliance GmbH* is a consulting firm that supports the implementation of European and national data protection regulations and the implementation of IT security and compliance systems.

[69] *IAB Europe*, Transparency & Consent Framework v2.0 accessible via: https://iabeurope.eu/tcf-2-0/ (accessed 5th January 2023); *ISiCO*, Whitepaper: Cookie-Banner – Leitfaden zur sachgerechten Umsetzung accessible via: https://www.isico-datenschutz.de/blog/whitepaper-cookie-banner-dsgvo-konform/ (accessed 5th January 2023).

[70] Cf. https://iabeurope.eu/transparency-consent-framework/ (accessed 5th January 2023).

[71] Cf. https://iabeurope.eu/transparency-consent-framework/ (accessed 5th January 2023).

[72] "Real-time bidding refers to the use of an instantaneous automated online auction for the sale and purchase of online advertising space. Specifically, it means that when an individual accesses a website or application that contains an advertising space, behind the scenes through an automated online auction system and algorithms, technology companies representing thousands of advertisers can instantly (in real time) bid for that advertising space to display targeted advertising specifically tailored to that individual's profile." APD, Decision of 2 February 2022 – DOS-2019-01377, para 22.

real-time auction of advertising space that takes place automatically in the background.[73]

36 However, guidelines from organizations and interest groups have no legitimizing effect; compliance with these guidelines and the use of abovementioned tools do not automatically lead to conformity with the GDPR, even if this is suggested. This is also confirmed by the recent ruling of the Belgian Data Protection Authority *Autorité de Protection des donneés* (APD*)*, which declared the IAB Europe framework as incompatible with the GDPR.[74] In addition to numerous other violations, the consent mechanism is said to be invalid due to a lack of sufficient information (especially with regard to the aforementioned consent strings).[75] The standard for a legally compliant design of consent tools remains the GDPR, any industry guidelines, must be measured against it.

E. Conditions for effective consent under the GDPR

37 Although the use of cookies also falls within the scope of other laws, as just explained, there is always a reference to the GDPR, so that the GDPR always remains the central element for assessing the lawfulness of processing. Therefore, the requirements for an effective consent according to the GDPR will be further examined.

I. Form

38 Consent can be generally given without any formal requirements—any declaration of intent with explanatory value is necessary but also sufficient. According to Recital 32 GDPR it can be given in any form, including oral, written, and electronically transmitted declarations of consent. Even an implied declaration is principally possible—at least as long as it provides for a clear affirmative action.[76] However, according to Recital 32 GDPR mere silence does not have a sufficient explanatory value. In practical terms, this means that consent to the use of cookies is not given by continuing to browse on a website and disregarding the cookies banner. This does not constitute an unambiguously confirming act.[77] The same applies to the mere download of an app or other software: the download does not provide for a sufficient declaration of consent within the meaning of the GDPR.[78] Although the EU Commission and the European Parliament have not been able to enforce their demand that every consent must be explicit, the requirement of an "unambiguously indication" in Article 4 No. 11 and Recital 32 GDPR leads to a strong restriction of the generally possible implied consent[79], especially in the online area. Consent given through inactivity, e.g. by not unchecking pre-ticked consent fields, does not satisfy the requirement of a clearly confirming action.[80] This has now also been confirmed by the CJEU in its *Planet49* decision[81] and subsequently also by the Federal Supreme Court (BGH).[82] According to the courts, it is not sufficient for the consent requirement under the ePrivacy Directive (certainly not under the GDPR[83]) if the user

[73] Detailed explanation of the process and involved parties: APD, Decision of 2 February 2022 – DOS-2019-01377, paras 20 ff.

[74] APD, Decision of 2 February 2022 – DOS-2019-01377, paras 403 ff.

[75] However, IAB Europe defended itself against the decision at the Court of Appeal in Brussels. The Court suspended the proceedings in order to submit two preliminary questions to the CJEU: first, whether the TC strings constitute personal data and second, whether IAB Europe can actually be classified as a responsible party within the meaning of the GDPR, cf. Hof van beroep Brussels, Decision of 7 September 2022 –2022/AR/292.

[76] Bastian Stemmer, 'Art. 7 DS-GVO' in Heinrich Amadeus Wolff, Stefan Brink (eds), *BeckOK DatenschutzR* (41th edn, C.H. Beck 01.08.2022) para 84; But critical regarding the practicability of implied consent and also its compliance with data protection principles Benedikt Buchner, Jürgen Kühling, 'Art. 7', in Jürgen Kühling, Benedikt Buchner (eds), *Datenschutz-Grundverordnung BDSG Kommentar* (3rd edn, C.H. Beck 2020) Art. 7 para 27, Art 4 No. 11 para 58b; Critical of the practical suitability of the theoretically possible implied consent: Martin Franzen, 'Art. 4 DS-GVO' in Martin Franzen, Inken Gallner, Hartmut Oetker (eds), *Kommentar zum europäischen Arbeitsrecht* (4th edn, C.H. Beck 2022) para 20; Arning, Rothkegel (n 15) DSGVO Art. 4 para 283.

[77] Kühling, Buchner (n 76) Art. 7 para 27; Specht-Riemschneider (n 37) para 33; Paul Voigt, Axel Freiherr von dem Bussche, *DSGVO Praktikerhandbuch* (Springer 2018) 122.

[78] Philipp Albrecht, Florian Jotzo, *Das neue Datenschutzrecht der EU* (Nomos 2017) Part 3 para 39.; Kühling, Buchner (n 76) Art. 7 para 58c.

[79] Schulz (n 49) DS-GVO Art. 7 para 42; in this direction also Philipp Albrecht, Florian Jotzo, *Das neue Datenschutzrecht der EU* (Nomos 2017) Part 3 para 39; Klabunde (n 15) Art. 7 para 36, Art. 4 para 53.

[80] Cf. recital 32 sentence 3.

[81] CJEU Case C-673/17 *Planet49* [2019] ECLI:EU:C:2019:801.

[82] BGH MMR 2020, 609.

[83] CJEU Case C-673/17 *Planet49* [2019] ECLI:EU:C:2019:801 para

does not deselect pre-ticked consent tick boxes.[84] This puts a stop to the practice of legitimizing cookies through opt-out consents, which has been common for a long time and still occurs today.[85]

39 Although this does not impinge on any formal requirement, it is nevertheless advisable—especially for the digital area—to obtain the declaration of consent in a material form. Otherwise it is hardly ever possible to prove that consent has been obtained, as required by Article 7 (1) GDPR. A cookie banner proves to be an effective method in this respect. If consent is obtained using such means (i.e. in electronic form), Recital 32 states that care must be taken to ensure that the request is clear, concise, and not unnecessarily disruptive to the use of the service for which it is provided. These requirements are strongly linked to the requirement that consent must be given in an informed manner. The controller must ensure that the electronic consent tool is clear in terms of form, content, color, and other design, and does not mislead the user; it must be clear that consent to the processing of data is given by the electronic tool. In particular, the extent or purposes of the processing must be clearly and unambiguously explained, as will be shown below.

II. Timing and duration

40 Effective consent has to be given at the time of processing and must therefore be obtained in advance.[86] This is not explicitly regulated in the GDPR, but already follows from the protective purpose and the general prohibition of processing.[87] By giving consent, the data subject expresses that the processing may exceptionally be permissible within the limits of the consent given. Consequently, it must necessarily be obtained before the processing takes place.[88] Subsequent consent has no curative effect on unlawful data processing[89]; however, it can have an effect in the future and may lead to the data not having to be deleted and obtained again, as consent can be interpreted as a waiver of the right to deletion.[90]

41 In principle, consent does not have an expiration date.[91] However, the right to be forgotten from Article 17 (1) GDPR, according to which data must be deleted as soon as they are no longer required for the purposes for which they were collected, leads to a time limit.

III. Granularity and purpose limitation

42 According to Article 4 No. 11 and Article 6 (1) lit. a GDPR, consent must always be given for a specific case. This includes, for example, a specific data processing act as well as a concrete purpose.[92] This requirement follows from the fundamental right of protection of personal data in Article 8 CFR[93] and has now also been explicitly included in Article 5 lit. b GDPR as a general principle; the aim is to ensure that the data subject can monitor the scope of its declaration and that the controller has strict limits on the use of the personal data.[94] The purpose must

63; BGH MMR 2020, 609 para 34; Dirk Heckmann, Martin Scheurer, 'Datenschutzrecht' in Dirk Heckmann, Anne Paschke (eds), *jurisPK-Internetrecht* (7th edn, juris 2021) chapter 9 para 317.

[84] BGH MMR 2020, 609 para 47; CJEU Case C-673/17 *Planet49* [2019] ECLI:EU:C:2019:801 para 52, 59 ff.; *Heckmann, Scheuer* (n 83) chapter 9, para 739.

[85] Stemmer (n 76) DS-GVO Art. 7 para 86; Kühling, Buchner (n 76) Art. 7 para 58; Martin Eßer in Martin Eßer, Philipp Kramer, Kai von Lewinski (eds) 'Auernhammer DSGVO/ BDSG', (7th edn, Carl Heymanns 2020), Art. 4 para 101.

[86] Schulz (n 49) DS-GVO Art. 7 para 7; Stemmer (n 76) DS-GVO Art. 7 para 88; Kühling, Buchner (n 76) Art. 7 para 30.

[87] Kühling, Buchner (n 76) Art. 7 para 30; Schulz (n 49) DS-GVO Art. 7 para 7; Albert Ingold, 'Art. 7 Bedingungen für die Einwilligung' in Gernot Sydow, Nikolaus Marsch (eds), *Europäische Datenschutzgrundverordnung* (3rd edn, Nomos 2022 para 17.

[88] Ingold (n 87) Art. 7 para 17; Kühling, Buchner (n 76) Art. 7 para 30; Schulz (n 49) DS-GVO Art. 7 para 7.

[89] Schulz (n 49) DS-GVO Art. 7 para 7; Dirk Heckmann, Anne Paschke, 'Art. 7', in Eugen Ehmann, Martin Selmayr (eds), *DS-GVO Kommentar* (C.H. Beck, 2nd edn 2018) para 44.

[90] Heckmann, Paschke (n 89) para 44.

[91] Stemmer (n 76) DS-GVO Art. 7 para 88; Heckmann, Paschke (n 89) para 44; Kühling, Buchner (n 76) Art. 7 para 30.

[92] EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679 adopted on 4th of May 2020' (2020) 12 ff.; Stemmer (n 76) DS-GVO Art. 7 para. 77; Kühling, Buchner (n 76) Art. 7 para 61.

[93] Jan Henrik Klement, 'Art. 7 DS-GVO Bedingungen für die Einwilligung' in Spiros Simitis, Gerrit Hornung, Indra Spiecker gen. Döhmann (eds), *Datenschutzrecht* (1st edn, Nomos 2019) paras 18 f.; Kühling, Buchner (n 76) Art. 7 para 61.

[94] Stemmer (n 76) DS-GVO Art. 7 para 77; Heckmann, Paschke (n 89) Art. 7 para 63; Heinrich Amadeus Wolff, in Peter Schantz, Heinrich Amadeus Wolff (eds), *Das neue Datenschutzrecht* (1st edn, Nomos 2017) para 527; Winfried Veil, 'Einwilligung

be as precise as possible in order to protect the data subject from a gradual expansion or blurring of the purposes[95]; there should be no processing for purposes which the data subject did not expect and/or could not have expected at the time of the consent.[96] The granularity is closely linked to the criteria of voluntariness and informativeness. Recital 43 indicates that voluntariness is not given if the controller does not allow the data subject to give separate consent to different processing operations, although this would have been appropriate in the relevant case. If the processing fulfils several purposes, comprehensive information must be provided and separate consent must be obtained for each of these purposes, cf. Recital 32 GDPR. In practical terms, this means that a global or blank consent is generally not possible.[97] However, this does not preclude consent from being given for several purposes at the same time, provided that these purposes are specified and conclusively described; this already follows from the wording of Article 6 (1) lit a GDPR. However, the requirement for specificity reaches its limits where comprehensive specificity would unreasonably impair comprehensibility. In this case, the user would no longer have any actual knowledge due to the abundance of information and could therefore not make a genuine and informed decision.[98] Moreover, it should be noted that consent may also relate to several processing acts if they are subject to the same processing purpose. According to Recital 32, obtaining consent for each individual processing step is therefore not necessary and should be avoided due to the aforementioned lack of clarity.[99]

IV. Voluntariness

43 According to Article 4 No. 11 GDPR, consent requires a freely given indication of intent. The principle of voluntariness is one of the core elements of data protection law and can already be derived from Article 8 CFR.[100] However, there is no legal definition of the term voluntariness. Recital 42 at least specifies that the data subject should have a "genuine or free choice" and must therefore be able to refuse or withdraw consent without any detriment. In this regard, the EDPB defines the term "free" as a "real choice and control for data subjects".[101] This clarifies that consent may not be obtained by coercion and that there must be freedom of choice on the part of the person concerned. There is consensus insofar as that coercion is given when criminally relevant conduct is undertaken.[102] Otherwise, the formula requires further concretization, especially since not every interference with the will of the person concerned impairs their freedom of decision to such an extent that a lack of voluntariness must be assumed[103]; nor can every minor interference negate this freedom. Instead, it must have a certain relevance.[104]

44 Recital 43 of the GDPR explains in more detail that consent is not to be considered voluntary if there is a clear imbalance between the data subject and the controller, with public authorities being cited as an example of such an 'overbearing' counterpart.[105] However, such a relationship of subordination does not always lead to involuntariness but serves as an indicator.[106] In practice, there must always be

oder berechtigtes Interesse? – Datenverarbeitung zwischen Skylla und Charybdis' [2018] NJW 3337 (3340).

[95] EDPB (n 92) 16; Ernst (n 15) para 78; Marcus Helfrich, in Thomas Hoeren, Ulrich Sieber, Bernd Holznagel (eds), *Handbuch Multimediarecht* (58th edn, C.H. Beck March 2022) Part 16.1 para 58.

[96] Kühling, Buchner (n 76) Art. 7 para 61; Klement (n 93) Art. 7 para 69.

[97] Klement (n 93) Art. 7 paras 69 f.; Stemmer (n 76) DS-GVO Art. 7 para 79; Frenzel (n 49) Art. 7 para 8.

[98] Kühling, Buchner (n 76)Art. 7 para 65; Arning, Rothkegel (n 15) DS-GVO Art. 4 paras 273 f.; Stemmer (n 76) DS-GVO Art. 7 paras 77 f.

[99] Elke Sassenberg, 'Datenschutz in Schule und Schulverwaltung' in Louisa Specht, Reto Mantz (eds), Handbuch Europäisches und deutsches Datenschutzrecht (1st edn, C.H. Beck 2019) Sec.24 para 39.

[100] Heckmann, Paschke (n 89) Art. 7 para 48; Kühling, Buchner (n 76) Art. 7 para 41; Stemmer (n 76) DS-GVO Art. 7 para 42.

[101] EDPB (n 92) para 13.

[102] EDPB (n 92) para 24; Ingold (n 87) Art. 7 para 27; Martin Franzen, 'Art. 7 DS-GVO' in Martin Franzen, Inken Gallner, Hartmut Oetker (eds), *Kommentar zum europäischen Arbeitsrecht* (4th edn, C.H. Beck 2022) para 8; Stemmer (n 76)DS-GVO Art. 7 para 39; Heckmann, Paschke (n 89) Art. 7 para 53.

[103] Stemmer (n 76), DS-GVO Art. 7 para 40.

[104] EDPB (n 92) para 24; Schulz (n 49) DS-GVO Art. 7 para 29 even demands serious detriments; Lukas Ströbel, Tim Wybitul, 'Beschäftigtendatenschutz' in Louisa Specht, Reto Mantz (eds), Handbuch Europäisches und deutsches Datenschutzrecht (1st edn, C.H. Beck 2019) Sec. 10 para 61; Klement (n 93) Art. 7 para 48.

[105] EDPB (n 92) para 16; Kühling, Buchner (n 76) Art. 7 para 44; Stemmer (n 76) DS-GVO Art. 7 para 53.

[106] According to EDPB (n 92) para 21, an employment context provides for another use-case in this regard. The EDPB as-

a case-by-case assessment.[107] On the other hand, voluntariness can also be impaired in the case of less severe imbalances: for example, in the case of contracts between a trader and a consumer[108], or in the case of a monopolistic position of the responsible party.[109] However, the mere asymmetry of power alone is not sufficient; only when the affected party is also deprived of the possibility to determine whether and how the data processing takes place in the specific situation, the voluntariness of the declaration of consent is to be denied.[110] When assessing the case, especially the type and the availability of the service must be taken into account: in the area of necessities, a situation of coercion is more likely to be assumed than in the case of luxury goods.[111]

45 The requirements for voluntariness are furthermore determined by the *coupling prohibition* principle as laid down in Article 7 GDPR. A coupling exists if the conclusion of a contract or the provision of a service is made dependent on the consent of the data subject to a further collection or processing of its personal data that is not necessary for the processing of the transaction.[112] The prohibition is intended to protect the free and independent expression of the individual's will when giving consent and to prevent situations where a de facto compulsion to consent to the use of data arises.[113] However, the question regarding the scope of the coupling prohibition emerges. Considering the wording of the enacting terms of the GDPR, there would initially be many arguments against describing consent as a "return" for a gratuitous service as being given involuntarily.[114]

46 The scope of this coupling prohibition is therefore controversial. While Article 7(4) GDPR suggests through its wording that the coupling should only be strongly considered within an assessment of voluntariness, Recital 43 GDPR provides for a stricter approach. The Supreme Court of Austria had to deal with this question and concluded—unconvincingly—from the discrepancy between the wording of the provision and the recital that there is basically a presumption of involuntariness unless special circumstances speak in favour of voluntariness. In the view of the court, this was so obvious that there was no need to refer the matter to the CJEU.[115] The supervisory authorities also initially tended towards an absolute coupling prohibition.[116]

47 The literature, on the other hand, advocates for a relative coupling prohibition, i.e., that not every combination of consent and processing of data for an unrelated purpose leads to involuntariness, but instead a case-by-case assessment must always take place, whereby this circumstance of the coupling must particularly be taken into account.[117] A decision by the Higher Regional Court of Frankfurt follows this argumentative pattern, stating that coupling the granting of consent with an unrelated participation in a lottery does not lead to the consent given to be involuntary.[118] The relative approach is further supported by the fact that the principle of voluntariness prevailing in data protection law is a consequence of the principle of private autonomy—an absolute coupling prohibition, on the other hand, would lead to personal data being

sesses the consent given by an employee as being "problematic"; cf. also Art. 29 Data Protection Working Party, 'Opinion 02/2017 on data processing at work' WP 249, p. 23.

[107] EDPB (n 92) paras 17 f.; Ingold (n 87) Art. 7 para 28.

[108] Kühling, Buchner (n 76) Art. 7 para 44; Heckmann, Paschke (n 89) Art. 7 para 52; Isabell Conrad, Christina Treeger, '§ 34 Recht des Datenschutzes' in Astrid Auer-Reinsdorff, Isabell Conrad (eds), *Handbuch IT- und Datenschutzrecht* (3rd edn, C.H. Beck 2019) para 471; Different view Heinrich Amadeus Wolff, in Peter Schantz, Heinrich Amadeus Wolff (eds), *Das neue Datenschutzrecht* (1st edn, Nomos 2017) para 512.

[109] Buchner (n 16) 158; Kai-Uwe Plath, 'Art. 7 Bedingungen für die Einwilligung' in Kai-Uwe Plath (ed), *DSGVO/BDSG* (3rd edn, Verlag Otto Schmidt 2018) para 19; Heckmann, Paschke (n 89) Art. 7 para 52.

[110] Kühling, Buchner (n 76) Art. 7 para 44; Frenzel (n 49) Art. 7 para 18; Ingold (n 87) Art. 7 para 28.

[111] (n 87) Art. 7 para 27; In this direction probably Frenzel (n 49) Art. 7 para 18.

[112] EDPB (n 92) paras 14 f.; Heckmann, Paschke (n 89) Art. 7 para 94; Jan-Christoph Thode, ' in Uwe Schläger, Jan-Christoph Thode (eds), *Handbuch Datenschutz und IT-Sicherheit* (1st edn, Erich Schmidt Verlag 2018) chapter 2 para 88.

[113] EDPB (n 92) paras 26 f.; Heckmann, Paschke (n 89) Art. 7 para 94; Specht-Riemschneider (n 37) Sec. 9 para 27.

[114] CF. in this regard example 6a EDPB (n 92) paras 40.

[115] Austrian Highest Court (OGH), Decision of 31 August 2018 – 6 Ob 140/18h [2019] ZD 72 para 46.

[116] DSK, 'Kurzpapier No 20 - Einwilligung nach der DSGVO', 1; Benedikt Buchner, 'Die Einwilligung in Werbung' [2018] WRP 1283 (1286); Already distancing from such an absolute interpretation EDPB (n 92) para 35.

[117] Schulz (n 49) DS-GVO Art. 7 para 26; Taeger (n 50) DS-GVO Art. 7 para 90; Plath (n 109) Art. 7 para 19.

[118] Higher Regional Court Frankfurt a.M., Decision of 27 June 2019 – 6 U 6/19 [2019] ZD 507 para 12.

protected even against the expressly declared will of the data subject.[119] The sovereignty of the individual over its data, which is anchored in the Charter of Fundamental Rights, as well as the right to voluntarily disclose one's own personal data would be undermined in an intolerable manner.[120] Such an understanding would mean a disproportionate restriction of (informational) private autonomy and is consequently not in conformity with the Charter of Fundamental Rights.[121] Moreover, it is also the declared aim of the GDPR to strengthen both the personal rights of the individual and the digital single market.[122] However, an absolute coupling prohibition would represent a very strong impact on the freedom to choose an occupation and right to engage in work of data controllers (which is also protected in Article 15 CFR)[123] and, above all, would also make the "*data in return*" business model practically impossible. The fact that this cannot be the intention of the European legislator is also shown in the new Digital Content Directive.[124] In this regard, Article 3 (1) Digital Content Directive stipulates that data can also be used as a currency to "pay" for digital content. The scope of application of the directive would be reduced to zero if it were assumed that any link between data and contractual performance is excluded.[125] A connection between data and contractual performance is therefore not ruled out. However, this raises the very practice-relevant question of when data processing cannot be based on Article 6 (1) lit. b GDPR, meaning that consent of the data subject must be obtained. It should thus always be carefully examined whether the use of the data is unnecessary in the sense of this norm. Above all, consent should not be obtained "as a precaution", since, in case of a revocation or invalidity of the consent, other grounds for permission cannot be used.[126]

48 First of all, it should be noted that the scope of application of consent and the scope of application of the statutory authorization do not overlap. If the data is necessary for the performance of the contract, consent is not required.[127] This can be the case, for example, if the user wants to have goods delivered to their home address, then the usage and processing of the data is necessary to fulfil the contractual obligation.[128] The crucial point is therefore the interpretation of the term "necessity" within the meaning of Article 6 (1) lit b GDPR. The EDPB advocates for a narrow interpretation. Accordingly, necessity only exists if the success of the contract would be endangered if the data could not be used.

49 Some authors argue that in order to make the business model "service for data" possible, the inter-

[119] Heckmann, Paschke (n 89) Art. 7 para 95; Specht-Riemschneider (n 37) Sec. 9 para 28; Schulz (n 49) DS-GVO Art. 7 para 27; Plath (n 109) Art. 7 para 19; Heinrich Amadeus Wolff, in Peter Schantz, Heinrich Amadeus Wolff (eds), *Das neue Datenschutzrecht* (1st edn, Nomos 2017) para 515; Probably also Schmitz (n 30), part 16.2 para 280.

[120] Heckmann, Paschke (n 89) Art. 7 para 95; with regard to the Basic Law for the FRG Klement (n 93) Art. 7 para 59.

[121] Heckmann, Paschke (n 89) Art. 7 para 95; Veil (n 94) 3340; Specht-Riemschneider (n 37) Sec. 9 para 28; Björn Steinrötter, 'DSGVO Art. 7' in Georg Borges, Marc Hiller (eds), *BeckOK IT-Recht* (7th edn, C.H. Beck 1.7.2021) Art. 7 para 34.

[122] Cf. recital 2 sentence 2 GDPR.

[123] Schulz (n 49) DS-GVO Art. 7 para 27.

[124] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (Text with EEA relevance.), OJ L 136, 22.5.2019, 1 ff.

[125] Heckmann, Paschke (n 89) Art. 7 para 95.

[126] EDPB (n 92) paras 121 ff.; DSK (n 116) 3; Philip Uecker, 'Die Einwilligung im Datenschutzrecht und ihre Alternativen' [2019] ZD248 (249); Marie-Theres Tinnefeld, Isabell Conrad, 'Die selbstbestimmte Einwilligung im europäischen Recht' [2018] ZD391 (392); Malte Engeler, 'Das überschätzte Kopplungsverbot' [2018] ZD 55 (58); Admissible at most if there was information about the other legal basis: Kühling, Buchner (n 76) Art. 7 para 16 ff.; Peter Schantz, 'Art. 5 DS-GVO' in Heinrich Amadeus Wolff, Stefan brink (eds), *BeckOK DatenschutzR* (41th edn, C.H. Beck 01.08.2022) para 8; Heckmann, Paschke (n 89) Art. 7 para 20; Heberlein (n 50) Art. 6 para 7; Heckmann, Scheurer (n 83) chapter 9 para 354; different view Veil (94) 3342; Philip Hacker, 'Daten als Gegenleistung: Rechtsgeschäfte im Spannungsfeld von DS-GVO und allgemeinem Vertragsrecht' [2019] ZfPW 148 (160); Jonas Brinkmann, 'Sec. 307 Datenschutzklausel' in Beate Gsell, Wolfgang Krüger, Stephan Lorenz, Christoph Reymnn (eds), *beck-online.GROSSKOMMENTAR BGB* (7th edn., C.H. Beck 15.1.2022) paras 21 ff.; Philipp Kramer, ´Art. 6 DSGVO´ in Martin Eßer, Philipp Kramer, Kai von Lewinski (eds), *DSGVO BDSG*(7th edn, Carl Heymann 2020) para 23; Schulz (n 49) DS-GVO Art. 6 para 11; Frenzel (n 49) Art. 6 para 8, Art. 7 para 17a; Cf. also in this direction for the BDSG: BGH NJW 2008, 3055 para 43; Higher Regional Court (OLG) Frankfurt a.M. BeckRS 2005, 11716 para 29.

[127] EDPB (n 92) para 32.

[128] EDPB (n 92) para 24; 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' (Version 2.0, 8 October 2019) para 30; Frenzel (n 49) Art. 7 para 11.

pretation should be less restrictive.[129] In addition, according to the Digital Content Directive, such contracts should be possible, but these would generally fail due to the coupling prohibition if the necessity were to be interpreted in the sense of *indispensability*. However, considering the new European digital strategy, data should be able to be used as a valuable counterpart.[130] "*Data trading*" should be possible, but at the same time the undermining of the protective function of the GDPR must also be avoided; this can only be achieved by ensuring that only those business models whose essence is an "exchange for data" can be justified on the legal grounds of Article 6 (1) lit b GDPR. To prevent circumvention of a possible consent requirement, the definition of the content of the contract "data exchange" cannot be determined subjectively and unilaterally by the controller.[131] This can be ensured by reviewing the content of the general terms and conditions. However, the scope of application of the general terms and conditions is only opened if it is a secondary agreement and not the main performance obligation. For the delimitation, it depends primarily on what the parties have agreed. Above all, however, it depends on how the offer of the processor appears from the perspective of an objective recipient; if it is a typical performance-versus-data contract and this is made transparent, the transfer of the data can be the main purpose.

50 If, on the other hand, it is a different type of contract, the purpose of which is in particular the transmission of information or communication, and the processor attempts to expand this purpose in a non-transparent manner using an additional clause to include the provision of data, this may be subject to content review according to Section 307 (1) BGB. This will often lead to the clause being invalid because it contradicts the basic idea of the statutory regulations.[132] In addition, such agreements may also violate the transparency requirement or constitute a surprising clause within the meaning of Section 305c BGB.[133]

51 All in all, an absolute coupling prohibition should be rejected for the reasons just mentioned. The GDPR only imposes a relative prohibition of coupling; data exchange transactions, as provided for in the Digital Content Directive, are principally possible. However, the justification or the legal ground for justification always depends on the specific contractual performance. If the data exchange is the main purpose, then the necessity in the sense of Article 6 (1) lit b GDPR can be affirmed; however, this cannot be determined unilaterally by the potential processor, otherwise they would have the power to let the scope of consent lapse.[134] For the determination, it should be examined in each individual case, whether a bilateral contractual relationship exists between the processor and the data subject, whereby the decisive factor is if the data subject also receives a service or is granted benefits and does not only have to disclose its personal data without a real countervalue.[135]

52 Particularly in light of the Digital Content Directive, it seems very likely that new contract models will soon emerge in which the provision of data is offset by real value.[136] In all other cases, such agreements must be measured against Article 7 (4) GDPR and must also withstand a content review, which regularly leads to the invalidity of so-called "*take it or leave it*" offers with a unilateral definition of the purpose of the contract.[137] However, offers where the data subject is offered a real alternative to paying for the service with other monetary means instead of data may also be compatible with Article 7 (4) GDPR.[138] This is because there is freedom of choice between "payment" with the data by granting consent or the data-protecting alternative of rejecting the cookies and instead paying the equivalent

[129] Heckmann, Paschke (n 89) Art. 7 para 96; Schulz (n 49) DS-GVO Art. 7 para 30; The Bavarian data protection supervisory authority also advocated that such arrangements should not be permitted as a result of the coupling prohibition, but should be justified on the basis of article 6 (1) (b) of the GDPR if the situation is presented to the user in a clear and comprehensible manner and the user has a factual basis for his or her decision: Bavarian state office for data protection supervision (BayLDA), TB 2017/2018, p. 72.

[130] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'A European strategy for data' (COM/2020/66 final) 4 f.

[131] Kühling, Buchner (n 76) Art. 6 para 40a; Specht-Riemschneider (n 37) Sec. 9 para 49.

[132] BGH NJW 2013, 291 para 28; Brinkmann (n 126) para 17; Wolfgang Wurmnest, ´§ 307 Inhaltskontrolle´ in Franz Jürgen Säcker, Roland Rixecker, Hartmut Oetker (eds), Münchener Kommentar zum BGB (9th edn, C.H. Beck 2022) para 71.

[133] Taeger (n 50) DS-GVO Art. 7 para 44.

[134] Kühling, Buchner (n 76) Art. 7 para 51.

[135] Alexander Golland, ´Das Kopplungsverbot in der Datenschutz-Grundverordnung´ [2018] MMR, 130 (132).

[136] Kühling, Buchner (n 76) Art. 7 para 51 also assume this development.

[137] Also: Alexander Golland, ´Das Kopplungsverbot in der Datenschutz-Grundverordnung´ [2018] MMR 130

[138] EDPB (n 128) para 37.

value of the data with monetary means. In addition to these basic explanations, it should be noted that a disproportionately high price can again call the voluntary nature into question.[139]

V. Informed consent

53 Pursuant to Article 4 No. 11 GDPR, consent must be given in an informed manner to be effective. Once again, the aim is to ensure that the data subject can assess the impact of giving consent and that the data subject can clearly and unambiguously understand the circumstances of the data processing and the scope of their consent.[140] The GDPR itself does not exhaustively specify the minimum content that should be provided by the processor; a guiding framework, however, can be found in Articles 13 and 14 GDPR, which has been further specified by the EDPB to the effect that the following minimum information should be included: the identity of the controller, the purpose of each processing act, the type of data collected, the possibility of withdrawal, if applicable, information on the use of the data for automated decision-making according to Article 22 (2) lit. c GDPR and a notice on possible processing risks in the case of third country transfers pursuant to Article 49 GDPR.[141] In addition, the CJEU recently ruled that it is also necessary to provide information on whether third parties have access to the information and on the duration of cookies.[142] The latter seems particularly important regarding *persistent cookies*, which can—in contrast to *session cookies*—remain in place for years. It is important to emphasize that the provisions of Articles 13 and 14 GDPR are not conditions for the legal effectiveness of consent[143]; the enacting terms of the GDPR merely state that consent must be given in an informed manner (cf. Article 4 No 11). Articles 13 and 14 GDPR provide a framework for this, but the absence of certain information listed in these provisions does not result in the consent being legally ineffective.[144] This is supported not only by the fact that these standards are not in the enacting terms of the GDPR but also by the considerations in Recital 42, according to which informed consent is given if the data subject at least knows the identity of the controller and the purposes of the processing for which the personal data are intended.[145] However, the information specified by the EDPB and the CJEU should be provided in any case, because otherwise, it seems—especially regarding Recital 42—questionable whether the user can form a comprehensive understanding of the scope of his or her declaration.

54 Also, concerning the "how" of providing information, the GDPR does not make entirely clear statements. However, Recital 42 states that pre-formulated declarations (such as those in cookie banners) must be provided in an understandable and easily accessible form in clear and simple language, which is supplemented by Recital 32 with the requirement that, in addition to a clear and concise form, there should also be no unnecessary interruptions to the service. Consequently, the declaration of consent should be kept as short and precise as possible[146] and it must be written in a language that the data subject can understand, meaning that the common national language has to be chosen. Besides, the use of unnecessary technical vocabulary should also be avoided.[147] The complexity of the declaration by oversized, overlong banners or cookie banners and new information appearing in a variety of new tabs should be avoided.[148] Of course, the declaration as a

[139] With regard to the appropriate price, no general statements can be made; this depends on various circumstances such as the scope, type and exclusivity of the "lost" data, in detail to different criteria: Golland, (n 135) 130 (134 f.).

[140] Heckmann, Paschke (n 89) Art. 7 para 57; Kühling, Buchner (n 76) Art. 7 para 59; Arning, Rothkegel (n 15) DS-GVO Art. 4 para 277; Veil (n 94) 3339.

[141] EDPB (n 92) para 72; A slightly smaller circle is drawn by: Flemming Moos, Tobias Rothkegel, ´Anm. Zu EuGH, Setzen von Cookies erfordert aktive Einwilligung des Internetnutzers – Planet49´ [2019] MMR 732 (739) who usually consider it sufficient to provide information about the controller, the purposes of the processing and the revocability but not about the data types.

[142] Case C-673/17 *Planet49* [2019] ECLI:EU:C:2019:801 paras 75 f.

[143] EDPB (n 92) para 72; Philipp Albrecht, Florian Jotzo, *Das neue Datenschutzrecht der EU* (Nomos 2017) Part 3 para 41; Schulz (n 49) DS-GVO Art. 7 para 36; Arning, Rothkegel (n 15) DS-GVO Art. 4 para 278; Stemmer (n 76) para 99

[144] Schulz (n 49) DS-GVO Art. 7 para 36; Arning, Rothkegel (n 15) para 278; Philipp Albrecht, Florian Jotzo, *Das neue Datenschutzrecht der EU* (Nomos 2017)Part 3 para 41, Part 4 para 8; Kühling, Buchner (n 76) Art. 7 para 59.

[145] Also of this opinion: Moos, Rothkegel (n 141) 739.

[146] Heckmann, Paschke (n 89) Art. 7 para 42; Ingold (n 87) Art. 7 para 36.

[147] Kühling, Buchner (n 76) Art. 7 para 60; Ernst (n 15) Art. 4 para 83; Stemmer (n 76) DS-GVO Art. 7 para 66.

[148] Ernst (n 15) Art. 4 para 79 f.; Kühling, Buchner (n 76) Art. 7 para 60; Heinrich Amadeus Wolff, in Peter Schantz, Heinrich Amadeus Wolff (eds), *Das neue Datenschutzrecht* (1st edn, Nomos 2017) para 524.

whole must be legible[149]; it would not be sufficient to write the decisive information in minuscule font size.

55 The requirement to provide sufficient information is closely linked to the transparency requirement arising from Article 7 (2) GDPR: all decisive information should be disclosed to the data subject in a reasonable manner. To meet the need for completeness and transparency on the one hand and simplicity and conciseness on the other, a multilayer system seems appropriate.[150] On the first level, the minimum content described above should be presented in a concise form, and on another level, the remaining information pursuant to Articles 13 and 14 GDPR, as well as more detailed explanations, if necessary, should be provided.[151] If the decision is made to present more than the required minimum information on the first layer, the minimum content should be highlighted by size, shape, or colour to enable quick and complete comprehension of the most important information.[152] Neither the CJEU nor the German Federal Court have commented precisely on this, but at least in their view, a multilevel system does not seem to be inadmissible per se.[153] Furthermore, it should be noted that pursuant to recital 42 pre-formulated declarations of consent are subject to the control of general terms and conditions according to Directive 93/13/EEC. As a result, pre-formulated declarations of consent may be void, if, for instance, unfair clauses are used.

VI. Excursus: information obligations for consent-free cookies

56 Articles 13 and 14 GDPR set out extensive information obligations that the respective controller must fulfill when collecting personal data. From Article 13 GDPR (in case of direct collection) and Article 14 GDPR (in case of third party collection) respectively, arises an information obligation that the controller has to fulfill towards the data subject when collecting personal data.[154] The information obligation exists regardless of the legitimacy of the processing according to Articles 6 or 9 GDPR, even if the processing is carried out lawfully, the data subject has a right to know whether and which personal data are being collected, since only then the data subject's rights pursuant to Article 15ff. GDPR can be exercised adequately.[155] Furthermore, according to Recital 60 of the GDPR, the principle of fair and transparent processing requires that the data subject is always informed about the existence of the processing operation and its purpose. This means that, unless one of the exceptions listed in Articles 13 (4) and 14 (5) GDPR applies, the obligation exists and is abstract from other information obligations, in particular from the requirement of informed consent pursuant to Article 4 No. 11 GDPR. It is important to emphasize that the provisions of Articles 13 and 14 GDPR are not conditions for the legal effectiveness of consent; the enacting terms of the GDPR merely state that consent must be given in an informed manner (cf. Article 4 No 11 GDPR). Articles 13 and 14 GDPR provide a framework for this, but the absence of certain information listed in these provisions does not result in the consent being legally ineffective. Thus, a breach of the information requirements under Article 13f. GDPR can result in a fine under Article 83 (5) lit b GDPR, but does not affect the lawfulness of the processing; a lack of informed consent "only" results in the unlawfulness of the processing.

57 This means that if only consent-free cookies are set, solely the information requirements of Article 12ff. GDPR apply. The GDPR itself does not define the format or the specific way in which the information set out in Articles 13 and 14 GDPR must be provided. However, it follows from Article 12 (1) GDPR that

[149] Kühling, Buchner (n 76) Art. 7 para 60; also in this direction Heinrich Amadeus Wolff, in Peter Schantz, Heinrich Amadeus Wolff (eds), *Das neue Datenschutzrecht* (1st edn, Nomos 2017) para 524; Different opinion Stefan Ernst, ´Die Einwilligung nach der Datenschutzgrundverordnung´ [2017] ZD 110 (113).

[150] EDPB (n 92) para 69; Kühling, Buchner (n 76) Art. 7 para 59; Schulz (n 49) DS-GVO Art. 7 para 47; Stemmer (n 76)Art. 7 para 57; Klement (n 93) Art. 7 para 74.

[151] Also in this direction: Schulz (n 49) DS-GVO Art. 7 para 47.

[152] EDPB (n 92) para 71; Heckmann, Paschke (n 89) Art. 7 para 42; Also to distinguish from other declarations Schmitz (n 30) para 275.

[153] This rather unsatisfactory result for the practice is also reached by: Böhm, Halim (n 38) 655; different view Maren Pollmann, Dennis-Kenji Kipker, ´Informierte Einwilligung in der Online Welt´ [2016] DuD 378 (379).

[154] Alexandra Mester, 'Art. 13, 14 DS-GVO' in Jürgen Taeger, Detlev Gabel (eds), *DSGVO – BDSG – TTDSG* (R&V, 4th edn 2022) Art. 13 para 4, Art. 14 para 5; Matthias Bäcker, 'Art. 13, 14', in Jürgen Kühling, Benedikt Buchner (eds), *Datenschutz-Grundverordnung BDSG Kommentar* (3rd edn, C.H. Beck 2020) Art. 13 para 12; Art. 14 para 9.

[155] Rainer Knyrim, 'Art. 13'13 f.', in Eugen Ehmann, Martin Selmayr (eds), *Datenschutz-Grundverordnung Kommentar* (2nd edn, C.H. Beck 2018) Art. 13 para 1, Art. 14 para 1; Mester (n 154) Art. 13 para 1, Art. 14 para 2.

the controller has to take appropriate measures to provide the information to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. According to Article 12 (7) GDPR the information may be provided in combination with standardized icons to give in an easily visible, intelligible, and clearly legible manner a meaningful overview of the intended processing. Although Article 12 ff GDPR do not prescribe a specific form, the Article 29 Working Party is of the opinion that the controller has to take into account all the circumstances of the data collection and processing when deciding on the appropriate manner and form of provision.[156] Furthermore:

> *"In particular, appropriate measures will need to be assessed in light of the product/service user experience. This means taking account of the device used (if applicable), the nature of the user interfaces/ interactions with the data controller (the user "journey") and the limitations that those factors entail."*[157]

58 Nevertheless, the data controllers are not completely free as to the choice of medium; in particular in the online context, a "*media discontinuity*"[158] would generally be inadmissible.[159] The required information should be available on the website of the data controller.[160] Since no concrete specifications are made, the design as a separate part of a website on which the information can be viewed in bundled form—i.e., the "*classic*" data privacy statement—is possible.[161] However, the controller must actively inform the data subjects and ensure that they can receive the information in a timely manner; this follows from the wording of Articles 13 (1) and 14 (1) GDPR, according to which the relevant information must be "*provided*".[162] It is not sufficient for the data controllers to make certain information available for retrieval only, for example in a general privacy statement on their website.[163] The user of the website should therefore be referred to the necessary information directly when visiting the website; this can be done, for example, by placing an HTML element with a forwarding link.[164]

59 Although the timing of the presentation of information is not explicitly defined in Article 12 ff GDPR, the wording "at the time of data collection" in Article 12 (1) GDPR does not indicate whether the information must be shown during or before the data collection. It follows, at least from the purpose of the information obligations, that they must be fulfilled immediately before the start of data collection.[165] In the case of third-party collection in the sense of Article 14 GDPR, the responsible party must provide the information within a reasonable period of time after receipt of the data, but no later than one month, Article 14 (3) GDPR.

60 Since the information should be clear and understandable for the reader, the Article 29 Data Protection Working Party also proposes other forms of design than the classic data privacy statement in order to prevent information fatigue. These include, on the one hand, a layered approach and, on the other hand, *push* or *pull* notices. The Article 29 Working Party states that:

> *"In the digital context, in light of the volume of information which is required to be provided to the data subject, a layered approach may be followed by data controllers where they opt to use a combination of methods to ensure transparency. WP29 recommends in particular that layered privacy statements/notices should be used to link to the various categories of information which must be provided to the data subject, rather than displaying all such information in a single notice on the screen, in order to avoid information fatigue. Layered privacy statements/notices can help resolve the tension between completeness and understanding, notably by allowing users to navigate directly to the section of the statement/notice that they wish to read. It should be noted that layered privacy statements/notices are not merely nested pages that require several clicks to get to the relevant information. The design and layout of the first layer of the privacy statement/notice should be such that the data subject has a clear overview of the information available to them on the processing of their personal data and where/how they can find that detailed information within the layers of the privacy statement/notice."*[166]

[156] Article 29 Working Party, 'Guidelines on transparency under Regulation 2016/679 last revised and adopted on 11th of April 2018', para 24.

[157] Article 29 Working Party (n 156) para 24.

[158] when the information is not provided in the form that is also used for data collection (e.g. electronically).

[159] Mester (n 154) Art. 13 para 36.

[160] Article 29 Working Party (n 156) para 17, 40.

[161] Article 29 Working Party (n 156) para 24; Oliver Daum, ´Pflichtangaben auf Webseiten´ [2020] MMR 643 (645); critical in this regard Joerg Heidrich, Michael Koch, ´Die Nutzer im Netz zwischen Einfluss und Ohnmacht´ [2020] MMR 581 who see this as "*information overkill*".

[162] Article 29 Working Party (n 156) para 33; Mester (n 154) Art. 13 para 36.

[163] Bäcker (n 155) Art. 14 para 41; Bernd Lorenz, ´Datenschutzrechtliche Informationspflichten´ [2019] VuR 213 (220).

[164] Article 29 Working Party (n 156) para 33.

[165] Bäcker (n 155) Art. 13 para 56; detailed Article 29 Working Party (n 156) para 26.

[166] Article 29 Working Party (n 156) para 35.

61 The Article 29 Working Party also presents a proposal on what information should be displayed and at what level:

> *"As regards the content of the first modality used by a controller to inform data subjects in a layered approach (in other words the primary way in which the controller first engages with a data subject), or the content of the first layer of a layered privacy statement/notice, WP29 recommends that the first layer/modality should include the details of the purposes of processing, the identity of controller and a description of the data subject's rights. (Furthermore this information should be directly brought to the attention of a data subject at the time of collection of the personal data e.g. displayed as a data subject fills in an online form.) The importance of providing this information upfront arises in particular from Recital 39.34 While controllers must be able to demonstrate accountability as to what further information they decide to prioritise, WP29's position is that, in line with the fairness principle, in addition to the information detailed above in this paragraph, the first layer/modality should also contain information on the processing which has the most impact on the data subject and processing which could surprise them. Therefore, the data subject should be able to understand from information contained in the first layer/modality what the consequences of the processing in question will be for the data subject (see also above at paragraph 10)."*[167]

62 Instead of the multi-level approach, the Article 29 Working Party believes that the form of push or pull notices can also be useful. Push notices involve the provision of information "just-in-time"[168], while pull notices command access to information via tools such as a privacy dashboard.[169] None of these procedures are legally required, but to fulfil the information obligation from Article 13 or 14 GDPR, providers must always check whether the form they have chosen creates the necessary transparency, or whether it is more likely that a large part of the information will go unnoticed.[170]

63 Overall, the GDPR leaves a great degree of discretion to the controller with regard to the presentation of the information. However, this does not mean that it is sufficient to make all the information available for retrieval in an unstructured manner. It is the responsibility of the controller to take appropriate measures to ensure that the information is presented in a concise, transparent, intelligible, and easily accessible form. The controller must therefore always examine carefully whether the concretely chosen form of information provision does not contradict this objective.[171]

VII. Revocability

64 Article 7 (3) GDPR stipulates that consent is freely revocable. The controller must inform the data subject about this possibility and also has to ensure that the data subject can withdraw consent at any time. Withdrawal of consent must be as simple as its original granting. In particular, according to Article 7 (3) S. 4 GDPR the withdrawal of consent can be carried out in the same way as consent was given.

65 The GDPR does not impose any material, formal, or temporal requirements for revocation, in particular, no special form must be followed[172] and the controller must inform the data subject of this. The requirement that the revocation must be as simple as the consent leads to a reciprocal right of revocation. This means that if consent can be given electronically via a cookie banner by mouse click or keystroke, this must also apply to revocation.[173] Thus, consent given via a cookie banner cannot be made dependent on a revocation email or a call to a service centre, for example.[174] This would constitute an unreasonable effort and is not in line with the simplicity requirement.

66 However, it may be rather difficult to set up the appropriate revocation environment if the data subject has not created a user account so that the revocation option can be integrated into the user interface.[175] One possibility would be to set up a pop-up window when the user wants to close the website or app and scrolls with the mouse on the X-button, asking whether the consent should be

[167] Article 29 Working Party (n 156) para 36.

[168] Article 29 Working Party (n 156) para 39, a just in time notice is described by the Article 29 Working Group as [a] *notice [which] is used to provide specific 'privacy information' in an ad hoc manner, as and when it is most relevant for the data subject to read.*

[169] Article 29 Working Party (n 156) para 39.

[170] Article 29 Working Party (n 156) para 34.

[171] For the question of which information must be provided in accordance with Art. 13 and 14 GDPR, see the overview: Article 29 Working Party (n 156) 35 ff.

[172] Heckmann, Paschke (n 89) Art. 7 para 91; Stemmer (n 76) DS-GVO Art. 7 para 95; Kramer (n 126) Art. 7 para 39.

[173] EDPB (n 92) para 114Kramer (n 126) Art. 7 para 40; Uwe Schläger, ´Einwilligung´ in Schläger/ Jan Christoph Thode (ed), Handbuch Datenschutz und IT-Sicherheit (1st edn, Erich Schmidt 2018) para 90.

[174] LfDI BaWü, 'FAQ Cookies und Tracking durch Betreiber von Webseiten und Hersteller von Smartphone-Apps' (Version 2.0 März 2022) 27.

[175] Also remarked by Heckmann, Paschke (n 89) Art. 7 para 91.

revoked and set the corresponding tick boxes there, which the user can simply click on.[176]

F. Design of a Cookie Banner

67 There are several regulations that have to be followed, yet, there is still a spectrum of design options. It should be noted, however, that the design to be chosen on the spectrum should not only be legal but also adequately designed from the perspective of behavioural science. This is because designs that have been proven to lead to users being confused, fatigued, or even deceived and therefore lead to suboptimal behaviour[177] can also call into question the active and informed consent and/or voluntariness of consent from a legal perspective. Manipulative design methods should be refrained from; the choice ends where misbehaviour is deliberately challenged.

I. Placement, Visibility and Accessibility

68 To give the user a sufficient choice to start with, the banner must be presented in a suitable place, at a suitable time, and in a suitable colour.

69 For this purpose, the cookies banner should appear directly when the website or application is opened and not at a later time.[178] This procedure is necessary, on the one hand, to enable actual consent prior to processing. On the other hand, however, it also avoids that the user first contractually commits themselves on the website and then only being shown the consent at the end of an order process.

70 A design in which no cookie banner appears when the website is visited, but only when the user calls up a specific product should be avoided. In this case, the user's propensity to buy is exploited. Behavioural science studies have shown that shoppers are more likely to give their consent when they are already far along in the shopping process, to avoid having to search for alternative products.[179] To enable users to make a truly voluntary decision, they should be given the opportunity to do so before any interaction on the website.

71 In addition, the cookie banner should be placed in a way that it is clearly visible when the page is called up; this can best be achieved with a separate pop-up element, making the cookie banner stand out from the rest of the website. The banner should have colour highlighting at the bottom or top of the website. The consent element should not merge with the page and disappear when scrolling. The user should be given the opportunity to engage with the relevant data protection provisions; this is impaired if the corresponding banner has already disappeared after a single scroll.

72 Furthermore, a colour scheme should be chosen that does not unnecessarily complicate the absorption of information, therefore colours that are comfortable for the eyes should be used.

II. Mandatory information

73 In order to enable the user to give informed consent under the GDPR, the following information must already be included at the first level of the cookie banner:

- the identity of the controller,
- the purpose of each processing act,
- the type of data collected,
- the duration of the data usage
- the possibility of withdrawal,
- if applicable, information on the use of the data for automated decision-making pursuant to Article 22 (2) lit c GDPR, and
- a notice on possible processing risks in the case of third-country transfers pursuant to Article 49 GDPR.

74 To ensure that consumers actually read and process the information completely, a short text with short and easy-to-understand sentences should be chosen. With increasing complexity, which is reinforced by the use of legal language or very technical terms, for example, the level of understanding decreases.[180]

[176] Heckmann, Paschke (n 89) Art. 7 para 91 and Georg Schröder, *Datenschutzrecht für die Praxis* (4th edn, dfv 2021) 154 suggests setting a checkbox on the data protection declaration next to the place where consent was given.

[177] Detailed on this: CNIL, 'IP Report No 6: Shaping Choices in the Digital World' (2019) 27 <https://linc.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf> accessed 10 December 2022.

[178] Also DSK (n 53) 9.

[179] Sara Elisa Kettner, Christian Thorun, Max *Vetter*, 'Wege zur besseren Informiertheit: Verhaltenswissenschaftliche Ergebnisse zur Wirksamkeit des One-Pager-Ansatzes und weiterer Lösungsansätze im Datenschutz' (Con Policy, 28.02.2018) <https://www.conpolicy.de/data/user_upload/Studien/Bericht_ConPolicy_2018_02_Wege_zur_besseren_Informiertheit.pdf > accessed 10 December 2022.

[180] In detail with further reference: Conpolicy, 'Abschlussbericht: Innovatives Datenschutz-Einwilligungsmanagement' (2020)

Despite the required conciseness, it must immediately be apparent to the user what they are consenting to, overview-like summaries such as "this site uses cookies to enhance your browsing experience" or "advertising analysis and marketing purposes" are not sufficient[181] because it is not clear which data should be processed for which purpose, so the data subject is not sufficiently informed.[182] Each purpose must be explained individually and specifically, if third-party services are integrated, these must be named individually, and the purposes of any partners must also be clearly and unambiguously listed. It is not sufficient to refer to the websites and/or privacy policies of the third parties for details of third-party cookies.[183] In order to achieve a sufficient degree of information, but also not overwhelm the user with information, a mixture of fixed text modules and drop-down elements or sidebar elements should be chosen. The 'fixed' text should explain what the consent is being requested for and how cookies work, as well as how and for what purposes they are used. If third-party providers are involved, they should also be listed directly. Above all, designs that induce the user to give consent as a result of a flood of information and that have pre-clicked purposes and third-party providers—requiring significant effort to deselect—are to be avoided.[184] In these cases, the required level of information is usually already lacking, as the information is prepared in an inappropriately complex manner, and active consent is also absent, as everything has already been pre-clicked. Transparent information should be available before consent is given, i.e., it must be possible to give granular consent already at the first level of the cookie banner and to obtain information about purposes and third-party providers and duration without detours. In particular, the frequently encountered "One-Click-Away" designs, in which only "accept all" "reject all" or "settings" can be selected at the first level and further information—especially on the purposes of processing—is only provided via the Settings selection, are not transparent because not all the necessary information is directly available.[185] However, it is possible to use an "accept all" and "reject all" button if further information and individual options for selecting and deselecting third-party providers are available at the same level.

75 Neither the legal requirements nor the courts and data protection authorities make strict statements on the question of whether all information should already be 'unfolded' on the first level. However, since clarity also plays a major role in the reception of information, the presentation of information about purposes, providers, and duration of use should be logically bundled in a drop-down menu or sidebar on the first level. This should be designed intuitively. The fold-out or expanding menu items should be easily recognizable as such; greying out or similar designs should be avoided, otherwise there is a lack of transparency since the information cannot be found.[186] There shouldn't be an excessive number of levels on which the user has the opportunity to make a decision only at the very last level, since the attention and receptiveness decreases with each level.[187] The user should not be overwhelmed with the necessary information, but it should also not be hidden.

76 According to Recital 32 of the GDPR, clear and simple language should be used for the information (this already applies to the headline of the banner). Which also means that the relevant information must be provided in the official language of the

part 2.1.2.2.1; The EDPB is therefore also against the use of such language: EDPB (n 92) para 67.

[181] Also with this opinion: Landesbeauftragter für Datenschutz und Informationsfreiheit (LfDI) BaWü, FAQ Cookies und Tracking durch Betreiber von Webseiten und Hersteller von Smartphone-Apps, Version 2.0 März 2022 p. 19; LfDI Niedersachsen, 'Handreichung: Datenschutzkonforme Einwilligungen auf Webseiten – Anforderungen an Consent Layer' (November 2020) 3; this design was recently classified as Dark Pattern (Left in the Dark Pattern – type: ambiguous wording or information) by the EDPB cf. EDPB, 'Guidelines 3/2022 on Dark Patterns in social media platform interfaces: How to recognize and avoid them' (Version 1.0, 14 March 2022) para 67 f., detailed on more types of Dark patterns and on the term in general see below part F.6.

[182] EDPB (n 181) para 68.

[183] This design is classified as Dark Pattern by the EDPB (Hindering Pattern – type: Dead End), cf. EDPB (n 181) para 78 f.; already in 2014: Damien Clifford 'EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour' [2014] JIPITEC 194 (199), but on the Data Protection Directive which was applicable until 2018.

[184] EDPB (n 181) para 118 f. (Overloading Pattern- type: too many options).

[185] The danish data protection authority also recently ruled in this way: Datatilysnet, Vejledning: Behandling af personoplysninger om hjemmesidebesøgende, 02.2022 <https://www.datatilsynet.dk/media/7784/vejledning-om-behandling-af-personoplysninger-om-hjemmesidebesoegende.pdf> accessed 10 December 2022.

[186] This design is classified as Dark Pattern by the EDPB (Stirring Pattern – type: Hidden in Plain Sight), cf. EDPB (n 181) para 47 ff.

[187] This design is classified as Dark Pattern by the EDPB (Overloading Pattern – type: Privacy Maze), cf. EDPB (n 181) para 47.

country concerned.[188] Despite the simple and clear language, the wording should not be so trivializing that the user is not even aware of what they are agreeing to or that they are giving legally effective consent at all. Formulations such as "A quick cookie and then onwards" should therefore be avoided for the consent button. The consent button should be labelled in a way that reflects its nature, and it should be clear what is meant by the button. A simple "okay, thank you" or "got it" will often not be sufficient, as it won't be clear whether the *okay* should only mean acknowledgement or active consent.

77 The information relevant to consent should be clearly separated from other information, so it should for example not be "buried" in the privacy policy. In addition, the Consent Banner should not be filled with contextless information that distracts from the actual consent process, e.g., cookie recipes or further links to cookies or cookie recipes, as this distracts the users from the actually relevant information and they will be more likely to click an "okay" button as they are not aware that they consent to data processing.[189]

78 To continue, other types of framing, in which the consent is set in a certain framework, can call the informed consent into question. Behavioural science studies have shown that consumers trust the judgment of "experts", so if a button is labelled "proceed with expert settings" or "proceed with recommended settings" instead of 'agree' or 'accept all', the consent rate can be increased[190]; however, these consents are not informed consents in the sense of the GDPR, as no information is provided about which operations and processing purposes are being consented to. Such labelling is therefore not sufficient according to the GDPR.

III. Active participation and defaults

79 As stated above, Recital 43 GDPR provides that consent is only deemed to have been given voluntarily if the data subject has a genuine or free choice and is therefore also able to refuse consent. Cookie banners where there is no choice at all, but only information about the use of cookies, are therefore generally inadmissible.[191]

80 The situation is similar if no rejection option is presented at the first level, but only via a "Learn more" link.[192] A mere notice about the processing, without decision options, is only sufficient if only consent-free cookies are set.

81 With the *Planet49* decision of the CJEU[193] and the subsequent BGH ruling[194], opt-out designs where consent is for all purposes pre-selected, and the user must opt-out are generally impermissible.[195] This was recently confirmed by the EDPB, as the *default effect* is exploited by such a design, which nudges users to keep a pre-selected option, they are unlikely to change this even if given the possibility.[196] The same applies if only some purposes are preselected since in this case there is no active consent on the part of the user. Only the necessary cookies may be permanently preselected as no consent is required for these.

82 The reverse design, on the other hand, in which all cookies and purposes are initially deselected complies with the requirement of voluntariness since the user must become active to consent to the processing. However, the consent process must not be unduly prolonged by requiring the user to review an interminable list of individual cookies and to select or deselect each one individually, without being given the opportunity to provide consent or rejection for all of them at once.[197]

[188] LfDI BaWü (n 174) 24; if the information is presented only in another language, this constitutes a dark pattern according the EDPB (Left in the dark Pattern – type: language discontinuity), EDPB (n 181) para 69.

[189] This design is classified as Dark Pattern by the EDPB (Skipping Pattern – type: Look over there), cf. EDPB (n 181) para 99 f.

[190] Detailed on the *Expert frame* with further references: Conpolicy (n 180) part 2.1.2.2.2.

[191] This is also the position of the DSK: DSK (n 53) 10.

[192] This has also been confirmed by the CJEU: CJEU Case C-61/19 *Orange Romania* [2020] ECLI:EU:C:2020:901 para 52; and by national courts: Regional Court Cologne GRUR-Prax 2021, 385.

[193] CJEU Case C-673/17 *Planet49* [2019] ECLI:EU:C:2019:801.

[194] BGH m. Anm. Gierschmann, ´Verwendung personenbezogener Daten - Cookie Einwilligung II´ [2020] MMR 609.

[195] in detail on the preceding decisions Agnieszka Jabtonowska and Adrianna Michatowicz, 'Planet49: Pre-Ticked Checkboxes Are Not Sufficient to Convey User's Consent to the Storage of Cookies' [2020] EDPL 137.

[196] This design was also classified as Dark Pattern (Skipping Pattern – type: deceiptive snugness), EDPB (n 181) para 127.

[197] EDPB (n 181) para 118 f. (Overloading Pattern - type: too many options).

IV. Revocability

83 According to Article 7 (3) GDPR, the revocation must be possible at any time and just as easy to implement as the consent. Thus, it would not be permissible to hide the revocation option somewhere in the privacy policy making it difficult to find. On the other hand, it will probably not be necessary to keep the cookies banner open all the time to allow immediate revocation, this will probably be more of a bother. Instead, the revocation option should be placed in an easy-to-find location, and in particular, it should be designed reciprocally to consent; if this was possible via a click-in-the-cookie banner, the revocation must also be possible via a click.

84 It is also important to ensure that the revocation option remains available and easy to find throughout the entire use of the website or app. According to the *Cookie Banner Task Force* by the EDPB a suitable solution is to implement a shortcut that enables the revocation by simply clicking on it (“small hovering and permanently visible icon”).[198] A notice in the cookie banner that a revocation option can be found in the privacy policy or is possible via an email does regularly not meet the requirements of Article 7 (4) GDPR.[199]

V. Cookie-Walls

85 Cookie walls that block access to the site until the user chooses one of the options are not per se permitted under the GDPR. However, designs in which the user can only consent or can choose between general consent and general rejection, are not in line with the principle of voluntariness, as there is no genuine choice here.[200] In addition, the necessary granularity does not exist in the previously mentioned scenarios.

86 These types of cookie walls must be distinguished from the so-called “PUR model”, which is very often found in the journalistic context. In this model, users can choose whether they want to access journalistic content without tracking, in which case they must pay a fee to use the service, or whether they consent to data processing and tracking, in which case they can use the site without paying further monetary compensation.[201] This raises the question if the consent is given voluntarily. Several data protection authorities of the Member States and the EDPB have expressed their views on this issue, and most of them have come to the same conclusion: cookie walls with an adequate alternative offer do not per se exclude the voluntary nature of consent.[202] However, this is only the case if the alternative offer is provided by the same party; pleading that (news) offers are available from other providers does not lead to a genuine and

[198] EDPB (Cookie Banner Task Force), Report of the work undertaken by the Cookie Banner Taskforce, 17.1.2023, para 32.

[199] EDPB (n 181) para 58 ff. (Hindering Pattern – type: Dead End) and para 45 (Hindering Pattern – type: longer than necessary).

[200] Further details: Bundesverband Digitale Wirtschaft (BVDW), ‘White Paper zum Wege-Modell / PUR-Modell / Cookie-Wall’ (18.10.2021) 2, available at: <https://www.bvdw.org/fileadmin/bvdw/upload/dokumente/20211012_BVDW_Mehrwegemodell_PUR_Modell.pdf> accessed 11 December 2022.

[201] in detail on issues of contract law, in particular on how a revocation of consent affects the contract: Dominik Nikol, Johannes Rost, ´Pur-Modelle unter dem neuen Digitale-Inhalte-Gesetz´ [2022] NJW 975.

[202] EDPB (n 92) para 37 f.; DSK (Germany), decision of 22.3.2023 ‘Bewertung von Pur-Abo-Modellen auf Websites’, available at: <https://www.datenschutzkonferenz-online.de/media/pm/DSK_Beschluss_Bewertung_von_Pur-Abo-Modellen_auf_Websites.pdf> accessed 1.4.2023; Austrian Data Protection Authority, decision of 25.5.2018, available at: <https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181130_DSB_D122_931_0003_DSB_2018_00/DSBT_20181130_DSB_D122_931_0003_DSB_2018_00.pdf> accessed 11 December 2022; p. 6; Spanish Data Protection Authority, Guide to the use of cookies, point 3.2.10, July 2022, available at:https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf <https://www.aepd.es/es/documento/guia-cookies.pdf> accessed 11 December 2022; Italian Data Protection Authorities, Guidelines on the use of cookies and other tracking tools, point 6.1 available at: <https://www.garanteprivacy.it/documents/10160/0/Consultazione+sul”e+”Linee+guida+s’ll’utilizzo+di+cookie+e+di+altri+strumenti+di+tracciamen“o “+-+Allegato+1+-+Linee+guida.pdf/72eab081-e4c4-4500-77c3-8b6957f8cd12?version=2.0> accessed 11 December 2022; more reluctant, after the general ban on cookie walls was suspended by the Conseil d’etat (Decision of 6.19.2020 available at: <https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2020-06-19/434684)> accessed 11 December 2022 now the *CNIL*, Délibération n° 2020-091 v. 17.9.2020, available at: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038783337> accessed 11 December 2022; Questions-réponses sur les lignes directrices modificatives et ecommendationion « cookies et autres traceurs » de la CNIL, question 27, available at: <https://www.cnil.fr/fr/questions-reponses-lignes-directrices-modificatives-et-recommandation-cookies-traceurs> accessed 11 December 2022; states that cookie walls are only in certain cases contrary to the voluntariness requirement; other opinion is taken by the Dutch Data Protection Authorities, who undifferentiatedly consider cookie walls to be inadmissible, available at: <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/cookies> accessed 11 December 2022.

free choice.[203] Furthermore, the alternative offer must have a reasonable price[204], which depends on the circumstances of the individual case. The limit is usually reached where the price is so high that users are deterred from using the offer, as there is no real choice.[205] The view of the permissibility of the PUR model is also supported by the current draft of the ePrivacy Regulation[206]:

> *In contrast to access to website content provided against monetary payment, where access is provided without direct monetary payment and is made dependent on the consent of the end-user to the storage and reading of cookies for additional purposes, requiring such consent would normally not be considered as depriving the end-user of a genuine choice if the end-user is able to choose between services, on the basis of clear, precise and user-friendly information about the purposes of cookies and similar techniques, between an offer that includes consenting to the use of cookies for additional purposes on the one hand, and an equivalent offer by the same provider that does not involve consenting to data use for additional purposes, on the other hand. Conversely, in some cases, making access to website content dependent on consent to the use of such cookies may be considered, in the presence of a clear imbalance between the end-user and the service provider as depriving the end-user of a genuine choice. (Emphasis added by the author)*

87 Whether this view will prevail remains to be seen[207], since the result will be a digital two-class society despite the formal "freedom" and fair design of the model, since privacy will only be granted to those who can "afford" it. In particular, if this model is no longer used only in journalistic areas, but also by other digital services, it seems questionable whether its permissibility is in line with the values of the GDPR. The protection of personal data should not be made dependent on the solvency of the individual.

VI. Nudging and Dark Patterns

88 Nudging and Dark Pattens describe special methods of influencing behaviour. Dark pattern is a collective term for digital decision environments that are designed to induce users to take actions that could potentially be contrary to their presumed interest, or that they probably would not have taken without being influenced.[208] The EDPB has recently defined Dark Patterns as:

> *[...] interfaces and user experiences [....] that lead users into making unintended, unwilling and potentially harmful decisions in regards of their personal data. Dark patterns aim to influence users' behaviours and can hinder their ability "to effectively protect their personal data and make conscious choices", for example by making them unable "to give an informed and freely given consent".*[209]

89 The distinction between Nudging and Dark Patterns is not always easy to make. Nudging is intended to make it "easier" for the person concerned to make decisions. No option for action is prohibited or excluded from the outset, but the decision is steered in a certain direction through special design.[210] Nudging is generally intended to help the person concerned, whereas Dark Patterns are usually intended to mislead the person into making detrimental decisions. However, the actual interest of the person concerned can vary, so that nudging is not per se useful or in line with interests.

[203] EDPB (n 92) para 38; Spanish Data Protection Authorities, Guidance on the use of cookies, July 2020, point 3.2.10, available at: < https://www.aepd.es/es/documento/guia-cookies.pdf > accessed 11 December 2022; Italian Data Protection Authorities, Guidelines on the use of cookies and other tracking tools, point 6.1 available at: <https://www.garanteprivacy.it/documents/10160/0/Consultazione+sul"e+"Linee+guida+s'll'utilizzo+di+cookie+e+di+altri+strumenti+di+tracciamento "+-+Allegato+1+-+Linee+guida.pdf/72eab081-e4c4-4500-77c3-8b6957f8cd12?version=2.0> accessed 11 December 2022; Austrian Data Protection Authority, decision of 25.5.2018, available at: <https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181130_DSB_D122_931_0003_DSB_2018_00/DSBT_20181130_DSB_D122_931_0003_DSB_2018_00.pdf>, p. 6 accessed 11 December 2022.

[204] DSK (n 202) 1.

[205] Nikol, Rost (n 201) 976.

[206] Cf. recital 20aaaa ePrivacy Regulation Draft, available at: <https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf> accessed 11 December 2022.

[207] The CNIL also appears to be very sceptical in this regard, making its comments on these designs on"y " conditional on the legality of this practies" CNIL, Deliberation No. 2020-091, 17.9.2020, para 19 available at: <https://www.cnil.fr/sites/default/files/atoms/files/lignes_directrices_de_la_cnil_sur_les_cookies_et_autres_traceurs.pdf> accessed 11 December 2022

[208] Carolin Loy, Ulrich Baumgartner, ´Consent-Banner und Nudging´ [2021] ZD 404 (404); Mario Martini, Christian Drews, Paul Seeliger, Quirin Weinzierl, ´Dark Patterns´ [2021] ZfDR 47 (49).

[209] EDPB (n 181) para 3.

[210] Loy, Baumgartner (n 208) 404.

90 Neither the ePrivacy Directive, the GDPR, nor the TTDPA explicitly address these phenomena. Thus, there are no binding legal provisions for a permissible design. Hence, it is always necessary to consider each case based on the guidelines outlined above regarding voluntariness and informed consent as well as the new Dark Patterns Guidelines by the EDPB and the findings by the Cookie Banner Task Force[211] (although the specifications are explicitly not conclusive[212]). In addition, recourse can also be made to the recommendations of some Data Protection Authorities, which have recently made initial recommendations on nudging.[213]

91 The behaviour of a user of a website or an app can be influenced by colour design and the size and placement of the choices. Not every colour highlighting leads to the exclusion of voluntariness. On the contrary, the colour highlighting of the options can even be useful for the person concerned and can prevent a long search. Nevertheless, those designs are to be omitted in which the consent to the processing is highlighted in colour, while the rejection option is greyed out or barely visible[214], as this seriously calls into question the voluntary nature of the consenting process. This could lead the person concerned to the erroneous assumption that there is only the possibility of consenting, leaving them with the wrong assumption not having a real choice.

92 To avoid confusion, especially on the first level, not only the consent button should be highlighted in colour, especially not in a colour that the (regular computer) user associates with something positive. In *Windows,* in particular, the buttons that can be clicked or are to be clicked are highlighted in blue, for example, in installations. If now on the first level the “accept all” button is highlighted blue, one tends to click this button from routine, our learned behaviour is activated and the probability that the click was preceded actually by a comprehensive information admission sinks.

93 It follows from Recital 32 GDPR that the required information in the case of pre-formulated declarations of consent (as in the case of cookie banners) must be presented in a clear and comprehensible manner. Accordingly, if a cookie banner uses a slider, to select or deselect individual cookies, whose colour design is counterintuitive—for example, if consent leaves the slider in red and rejection leaves the slider in green—there is regularly no informed choice.[215] Green is generally associated with consent, so linking it to the rejection of data processing is misleading. The same applies to the position of the slider. In the digital context, the position of the slider on the right means that an option is turned on, and the position on the left means that the option is turned off. If this is reversed in the cookie banner, especially in combination with misleading colour codes, it is for the average user no longer easy to understand what their action will result in, so that the required information is regularly lacking. If a special colour code is used on the first level (e.g., green is consent and red is rejection), this should be maintained on all levels of the consent banner and not suddenly be swapped. The same applies to the positioning of the buttons, processors should take care that all information, inclusive of control buttons, are displayed consistently.[216] Otherwise, users may become unclear about what their actions mean and lack the necessary information. To definitely exclude nudging in the wrong direction or even misleading, either no button should have a particular colour or both should have the same colour.[217]

94 The uncertainty caused by renewed requests for rejection with the indication that consent is urgently needed or that the existence of the website or the service would be impaired without consent can also seriously call into question the voluntary nature of consent, especially since the GDPR stipulates that rejection should be as simple as consent. A neutral notice before consent in the information text that and for what purpose it is useful will not be objectionable. But the aggravation of the refusal and/or the repeated request[218] paired with an emotional ap-

[211] EDPB (Cookie Banner Task Force), Report of the work undertaken by the Cookie Banner Taskforce, 17.1.2023.

[212] EDPB (n 181) Annex: List of Dark Patterns Categories and Types, p. 60; EDPB (Cookie Banner Task Force) (n 211) Disclaimer, 1.

[213] LfDI Niedersachsen (n 181) 7 ff.

[214] EDPB (Cookie Banner Task Force) (n 211) para 18.

[215] EDPB (n 181) para 95 (Left in the Dark Pattern – type: conflicting information); LfDI BaWü (n 174) 26.

[216] Otherwise this can be classified as a Dark Pattern EDPB (n 181) para 66 (Fickle Pattern – type: Lacking Hierarchy); Loy, Baumgartner (n 208) 407 who classify this design as misdirection pattern; LfDI BaWü (n 174) 26.

[217] This view is also supported by the French data protection authority CNIL, Délibération n° 2020-092 du 17 septembre 2020 portant adoption d’une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux «cookies et autres traceurs», p. 10 No. 34; <https://www.cnil.fr/sites/default/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf> accessed 11 December 2022; also agreeing LfDI BaWü, FAQ Cookies und Tracking durch Betreiber von Webseiten und Hersteller von Smartphone-Apps, Version 2.0 März 2022 p. 21.

[218] In this direction also LfDI Niedersachsen (n 181) 7; EDPB

peal[219] or the indication that the website will only be usable to a very limited extent violates the principle of voluntariness. Consent given for such external considerations is not voluntary.

G. Practical problems with current consent mechanisms

95 The General Data Protection Regulation aims at protecting personal data. One of the cornerstones is consent, which is intended to ensure that processing only takes place if the informed data subject has agreed to it.

96 However, the objectives of the GDPR are currently only moderately achieved due to several reasons. As already explained, the legal situation is extremely complex. Several laws apply to the same processes. This problem has been addressed with the introduction of the TTDPA, among other things, but even with the introduction of the TTDPA, there is only a punctual improvement. It has become clear that the requirements of the GDPR generally also apply to consent for the storage of and access to information in end devices, but open questions in this regard have not been clarified. In particular, it remains questionable which cookies are covered by the exceptions. There are also no requirements for the design of the consent procedure. All in all, there is still uncertainty about which cookies require consent and which cookies are covered by the legal permissions in the GDPR or TTDPA. In addition, there are inconsistent provisions of the data protection authorities of the individual member states.[220] The result is that the data controllers generally ask for consent. In practice, this means that on every website visited and for every application used, data processing must be consented to or rejected in advance, regardless of whether obtaining consent was legally required in the specific case. This leads to a certain consent fatigue: the affected parties simply no longer want to deal with the content of the banner, even if it is prepared in compliance with the GDPR. This leads to the clicking without reading phenomenon, which has also been observed concerning data protection declarations. The EDPB also pointed this out:

> *This may result in a certain degree of click fatigue: when encountered too many times, the actual warning effect of consent mechanisms is diminishing.*[221]

This fatigue makes misleading designs even more effective; informed consent is practically rare.

97 This was also critically considered in the legislative process for the TTDPA, but the proposed Section 24 (3) which specifically aimed at cookie banners was not included in the final act:

> *(3) In the cases referred to in paragraph 1, the consent [...] shall be designed in such a way that the user can declare his consent or opt-out by using buttons legibly labeled with nothing other than the words "consent" and "opt-out." The buttons must be presented on the same level in a graphically equivalent manner. The obligation to provide information in accordance with paragraph 1 and the permissibility of using a further button that enables the user to give itemized and individual consent to the use of individual storage or access as defined in sentence 1 on a graphically separately designed level shall remain unaffected by this.*[222]

98 Given these problems, modern consent solutions have been proposed, which will be outlined in the following.

H. Innovative consent management

I. Browser and Software solution

99 The GDPR itself does not lay down any specific requirements for the design of consent, neither with regard to banner designs nor with regard to other possibilities. However, it also addresses technology. According to Article 25 GDPR, data protection-friendly default settings and data protection requirements are to be technically guaranteed. In this context, so-called Do-Not-Track (DNT) mechanisms are being discussed.[223] These mechanisms intend to enable users to make settings in their browsers that allow or deny the collection of data by tracking

(181) para 110 (Overloading Pattern – type: continuous prompting).

[219] EDPB (n 181) para 163 (Stirring Pattern – type: Emotional Steering).

[220] Until recently, it was still the case in France that for certain cookies 'informed browsing' should be sufficient to meet the requirements for consent, Art. 2 Délibération n° 2013-378 du 5 décembre 2013 portant adoption d'une recommandation relative aux Cookies et aux autres traceurs visés par l'article 32-II de la loi du 6 janvier 1978, whereas the German authorities consider this to be insufficient EDPB (n 92) paras 79, 86.

[221] EDPB (n 92) para 87.

[222] Statement of the Bundesrat and counterstatement of the Federal Government, ´Entwurf eines Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien' (BT-Drs. 19/28396, 2021) 3 f.

[223] Cf. Specht-Riemschneider (n 37) Sec. 9 para 39.

tools of certain online services. This could restore at least a minimum of informational self-determination, which is currently impaired due to the previously addressed problems of consent fatigue and information overload. The German Federal Council has advocated for a DNT provision in the preparation of the TTDPA, which was not implemented by the legislator.[224] This result is accurate, even if it does not lead to an improvement of the cookie banner problems in the short term. A national DNT provision would be in conflict with the GDPR in terms of content and competence; the GDPR establishes the requirement of granularity, a single consent for any processing of personal data would currently not be data protection compliant. The Article 29 Working Party also expressed its opposition to the GDPR compliance of such a browser solution:

> *However, as general browser settings are not intended to apply to the application of a tracking technology in one individual case, they are unsuitable for providing consent under Article 7 and recital 32 of the GDPR (as the consent is not informed and specific enough).*[225]

100 Moreover, very precise specifications for the implementation of DNT would have to be introduced for browser providers in order to prevent misuse by them.[226] However, the national legislator has no regulatory competence for the design of consent mechanisms in the area of the GDPR.

101 The reduction of cookie banners would, by the current law, not be possible through a DNT function. However, the current draft of the ePrivacy Regulation contains in Article 9 (2) the provision that consent can also be given via suitable technical settings of software that enables access to the Internet, insofar as this is technically possible and feasible. Article 10 of the draft expands this by adding the provision that software placed on the market that permits electronic communication must also provide settings to prevent the storage or processing of information on the user's terminal equipment. In addition, the software must inform the user about the setting options directly during installation and require a decision by the user regarding the cookie setting. In the case of software that has already been installed, these requirements must be met at the latest during the next update. Thus, in future law, DNT settings in software or browsers could actually eliminate the need for individual consent on every website and every application.

102 However, the proposed rules have not been received without criticism. The Article 29 Working Party criticized, among other things, the fact that there are no rules on how to deal with outdated browsers or software that can no longer be updated.[227] In addition, they pointed out that, based on the current regulations, the software doesn't need to be set by default to prevent the storage or processing of information.[228] The Article 29 Working Party also calls for the establishment of uniform DNT standards to ensure that consent given in this manner is always voluntarily informed and granular.[229] Practical concerns were also expressed, partly doubting the technical feasibility of the project.[230] Whether and in what form DNT will be possible under the ePrivacy regulation is still uncertain, as the negotiations have not yet been concluded. For the moment, it, therefore, remains that DNT settings do not currently meet the requirements for effective consent.

II. Button solution

103 It has been suggested that, to ensure that the data subjects are actually informed and to make them aware of the consequences of their actions, the buttons should be specially labelled.[231] This is not a completely new approach to consent, but an increased warning function is to be achieved through appropriate labelling. For cookie walls, in particular, it is proposed to label the button with "*Pay with my data now*" or "*Agree to my surfing behaviour being tracked now*" in order to encourage the user to take a closer look at the consent to data processing.[232] The German Federal Council also proposed a comparable

[224] Statement of the Bundesrat and counterstatement of the Federal Government (n 222) 4.

[225] Art. 29 Data Protection Working Party, 'Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)' (WP 247, 17/EN) para 24.

[226] In detail on the danger of misuse: *Golland*, Statement on the TTDSG draft, pp. 13f. <https://www.bundestag.de/resource/blob/836010/498ffdbeff45200bdc011b13acc38b31/19-9-1054_Stellungnahme_SV_Dr_Golland_PwC_Legal_oeA_TTDSG_21-04-2021-data.pdf> accessed 13 October 2022.

[227] Art. 29 Data Protection Working Party (n 225) para 49.

[228] Art. 29 Data Protection Working Party (n 225) para 19.

[229] Art. 29 Data Protection Working Party (n 225) paras 24, 48.

[230] The Commission nationale informatique & libertés (CNIL) does not consider the current state of technology to be so advanced that effective consent can be given via corresponding settings in the browser: recommendation *CNIL* „cookies and other trackers", paras 71 – 73.

[231] Andreas Sesing, `Cookie-Banner-Hilfe, das Internet ist kaputt' [2021] MMR 544 (547).

[232] Sesing (n 231) 547.

provision in its opinion on the draft TTDPA, which however was not included in the final Act.[233]

104 This minor modification will not be sufficient to address the problems outlined above; a more comprehensive solution for consent management is needed. Since the labelling of the buttons cannot compensate for an otherwise cumbersome or difficult-to-understand consent banner. Nevertheless, the uniform and warning labelling of the button could be added as a complementary step. However, in this respect, the national legislator should refrain from imposing fixed labelling requirements, as otherwise the spectrum enabled by the GDPR would be unlawfully restricted, which would lead to the corresponding national requirements being unlawful under EU law.[234]

III. PIMS

105 Another approach, which has been under discussion for some years, could be to provide data subjects with more centralized information and consent tools (so-called Personal Information Management Systems (PIMS)), which would allow them to manage consent in a particularly user-friendly way. The user should be able to make all the desired and required privacy settings via a central dashboard, which must be accepted by the respective service providers. To link the respective settings to the data usage requests, a service is intermediated: a data fiduciary. This trustee takes over the administration without earning any money from the use of the data. The advantage of this approach is that the number of consents could be significantly reduced, and simple acceptance and rejection is made possible. The user also always has an overview and persistent cookies, which remain even after the website has been closed, are not lost sight of. Furthermore, it is always possible to revoke them.

106 A distinction must be made to PIMS that are designed for data sharing intermediation[235] (to simplify the intended exchange of data between the data subject and the controller) and PIMS designed to ensure a secure and simple exchange of data in the B2B area. In this case, the management system primarily serves to promote data trade; Article 10ff. Data Governance Act (DGA)[236] is aimed at these systems. Among other things Article 12 DGA stipulates that:

107 The provision of data-sharing services referred to in Article 10 shall be subject to the following conditions:

> (a) the data intermediation services provider shall not use the data for which it provides data intermediation services for purposes other than to put them at the disposal of data users and shall provide data intermediation services through a separate legal person;
>
> (b) the commercial terms, including pricing, for the provision of data intermediation services to a data holder or data user shall not be dependent upon whether the data holder or data user uses other services provided by the same data intermediation services provider or by a related entity, and if so to what degree the data holder or data user uses such other services;
>
> (c) the data collected with respect to any activity of a natural or legal person for the purpose of the provision of the data intermediation service, including the date, time and geolocation data, duration of activity and connections to other natural or legal persons established by the person who uses the data intermediation service, shall be used only for the development of that data intermediation service, which may entail the use of data for the detection of fraud or cybersecurity, and shall be made available to the data holders upon request;
>
> (d) the data intermediation services provider shall facilitate the exchange of the data in the format in which it receives it from a data subject or a data holder, shall convert the data into specific formats only to enhance interoperability within and across sectors or if requested by the data user or where mandated by Union law or to ensure harmonisation with international or European data standards and shall offer an opt-out possibility regarding those conversions to data subjects or data holders, unless the conversion is mandated by Union law;
>
> (e) data intermediation services may include offering additional specific tools and services to data holders or data subjects for the specific purpose of facilitating the exchange of data, such as temporary storage, curation, conversion, anonymisation and pseudonymisation, such tools being used only at the explicit request or approval of the data holder or data subject and third-party tools offered in that context not being used for other purposes;

[233] Statement of the Bundesrat and counterstatement of the Federal Government (n 222) 4.

[234] Based on this reasoning, the corresponding provision in the TTDPA proposed by the Federal Council was rejected by the Federal Government Statement of the Bundesrat and counterstatement of the Federal Government (n 222) 4.

[235] Detailed information on all types of PIMS: *Blankertz et al.*, Datentreuhandmodelle – Themenpapier, April 2020, pp. 3 ff. <https://pure.mpg.de/rest/items/item_3222478_2/component/file_3222479/content> accessed 11 December 2022.

[236] Regulation of the European Parliament and of the Council of 30 May 2022 on European data governance 2022/868 (Data Governance Act) (EU) 2022/868, OJ L 151, 1.

108 It is evident that the regulations are specifically intended to govern data trading via a central system and not primarily to simplify consent. PIMS, which are only intended to serve as a "consent assistant", have not yet been subject to any concrete legal regulation at European level.

109 A provision in this regard has now been introduced on the national level by the TTDPA. Section 26 (1) TTDPA cumulatively requires that consent management services have user-friendly and competitive procedures and applications for obtaining and managing consent, have no economic self-interest in consent and managed data, do not process information about consent decisions for other purposes and, finally, present a security concept that demonstrates compliance with data protection and data security requirements. If these requirements are met, these services can be recognized by a body that is yet to be determined. The actual rules have not yet been established by Section 26 (1) TTDPA, since Section 26 (2) TTDPA stipulates that the German Federal Government shall regulate the content of Section 26 (1) No. 1 - 4 TTDPA by statutory order. So far, however, it is not yet foreseeable when such an ordinance will come into force.[237] According to the German Federal Government, an expert opinion has already been requested.[238] This opinion was completed in December 2021.[239] The finalization of the ordinance based on this expert opinion is planned for the end of 2022. Then it is to be submitted to the European Commission for notification. If the proposal will be accepted, the regulation could be promulgated. However, the provisions can be blocked by the Commission for 12–18 months if a harmonization in the same area is (to be) carried out by the EU. Such harmonizing provisions may lie in the DGA, which also contains provisions for data-sharing services as shown above, so a temporary blocking of the regulations by the Federal Government is indeed possible.[240]

110 Apart from the lack of a concretizing regulation, there are several other problems. The prototype of a PIMS that serves as a consent assistant could function as follows: the trustee manages the data of the data subject, i.e. they grant or deny consent on behalf of the data subjects according to their specific preferences (these can be defined in the trust agreement). Although such systems are included in the TTDPA the legally compliant design of a PIMS is problematic, even if civil law questions of data trust[241] are ignored. Actions by and with those systems must always be measured against the GDPR. If PIMS are to function as a kind of consent assistant, several data protection questions arise.

1. Data protection issues

111 Initially, it should be noted that there are several (processing) acts that need to be distinguished from one another, and each needs to be evaluated and, if necessary, justified separately according to the GDPR standards. The evaluation depends on the exact design of the PIMS, but for simplicity, the following explanations are based on the prototype of the consent assistant described above[242]:

112 The information sent by the user to the data trustee will usually be stored or at least temporarily stored; this (temporary) storage already constitutes the first relevant processing act under Article 4 GDPR. The same applies to the forwarding or making available of the relevant information to or for the third party so that the latter can adjust the use of its cookies accordingly. Besides consent according to Article 6 (1) lit. a GDPR, the fulfilment of a contract pursuant to Article 6 (1) lit. b GDPR could be considered as a justification for these processing operations since the

[237] The *Bitcom* has completely advocated against the introduction of national PIMS provisions because of the pending Data Governance Act; in their view, only a uniform European regulation makes sense: *Bitcom*, Statement on the TTDSG draft, pp. 13f.: <https://www.bmwi.de/Redaktion/DE/Downloads/Stellungnahmen/Stellungnahmen-TTDSG/bitkom.pdf?__blob=publicationFile&v=4> accessed 11 December 2022:, p. 3; Other view: Rolf Schwartmann/Kristin Benedikt/ Yvette Reif, ´Entwurf zum TTDSG: Für einen zeitgemäßen Online-Datenschutz´ [2021] MMR 99 (101) who think that Germany should take on its role as a driving force.

[238] *Bender*, Federal ministry of economics and energy, speech at the conference: Das TTDSG und neue Wege zur Einwilligungsverwaltung, 3.11.2021 <https://stiftungdatenschutz.org/veranstaltungen/unsere-veranstaltungen-detailansicht/ttdsg-einwilligungsverwaltung-234#lg=1&slide=12> accessed 11 December 2022.

[239] Oliver *Stiemerling/ Steffen Weiß/ Christiane Wendehorst*, Forschungsgutachten zum Einwilligungsmanagement, 16.12.2021, available via: <https://www.ecambria-experts.de/it-sachverstaendiger/wp-content/uploads/2022/01/211216-Gutachten_fuer_Bundesministerium_fuer_Wirtschaft_und_Energie_p-os37621.pdf> accessed 11 December 2022.

[240] Also of this opinion: Alexander Golland, Anne Riechert, in Anne Riechert, Thomas Wilmer (eds), *TTDSG* (Erich Schmidt Verlag, 1st edn 2022) § 26 para 3.

[241] Detailed on this: Louisa *Specht-Riemenschneider, Aline Blankertz, Pascal Sierek, Ruben Schneider, Jakop Knapp, Theresa Henne*, `*Die Datentreuhand* -Beil. 25 (33ff).

[242] for further scenarios and the legal implications, see Jens Nebel, Einwilligungsverwaltungsdienste nach dem TTDSG´ [2022] CR 18 (19 ff.).

performance of these actions will regularly be governed by the trust agreement. However, this justification does not apply to sensitive data within the meaning of Article 9 GDPR. The evaluation and the storage of the data by the responsible website operator and controller must of course also be justified. Depending on the future legal regulation on PIMS—to be discussed below—these processing acts could be permitted by Article 6 (1) lit. c GDPR.

113 Another central question for these types of management systems is whether consent by a third party is possible at all. Representation concerning consent is generally rejected by a certain number of authors.[243] This is partly based on the fact that consent is not a declaration of intent, but a reason of justification.[244] Some authors focus on the existence of the representation rules regarding data subjects' rights in Article 80 GDPR and conclude *e contrario* that no representation is possible with regard to other acts such as consent.[245] Neither the ECJ nor international or national data protection authorities have explicitly commented on the issue, although the EDPS' opinion 9/2016 on Personal Information Management Systems[246] strongly suggests that representation is principally possible, since otherwise the user-friendly system the EDPS described[247] would hardly be feasible. Without the possibility of representation, the fiduciary would only be a mostly useless third party who does not contribute to an improvement of consent management. A significant part of the literature favours, however, the possibility of representation with regard to consent.[248] On the one hand, this is because representation is not fundamentally unknown in EU law, even if it has not been explicitly anchored in the GDPR, and on the other hand, because the GDPR primarily serves to protect the right of informational self-determination, and the decision to use a representative is ultimately also an expression of this right.[249] However, to ensure a high level of data protection, it is necessary to apply the same requirements to the proxy as to the consent itself.[250] Depending on the specific design and configuration of the system, the trustee may also be merely a messenger, which should legally be even more possible according to the view advocated here.

114 A crucial factor for the success of PIMS will be whether a legal obligation for data controllers to take account of the forwarded decisions (consent/no consent) is introduced. If the controllers are not obliged to take into account the decisions made by the data subjects within the PIMS, they can continue using their own consent tools, which aggravates the actual problem[251] as data subjects will then regularly have to make multiple decisions for the same process. This will significantly reduce trust in PIMS and hinder their success.

115 A further problem is that, in principle, users would have to decide for each individual processing operation, i.e., for each individual website, whether they want to consent or refuse to data processing—even if they use a PIMS—to ensure that there is no violation of the principle of granularity and certainty. However, this would just result in moving the aforementioned problems to a different setting. The user would no longer have to consent to the websites rather than in their PIMS, and the number of consents would not be reduced so that consent fatigue would also quickly develop in this scenario. It is argued that the principle of certainty should be interpreted according to the situation and that the spe-

[243] Stefan Ernst, 'Die Einwilligung nach der Datenschutzgrundverordnung´ [2017] ZD 110 (111); Helferich, 'Einführung und Grundbegriffe des Datenschutzes' (56th ed. May 2021), Part. 16.1 para 51; Taeger (n 50) Art. 7 para 10; Schulz (n 49) DS-GVO Art. 7 para 8 f.

[244] Ulrich Freiherr von Ulmenstrein, `Datensouveränität durch repräsentative Rechtswahrnehmung´ [2020] DuD 528 (534) Schulz (n 49) DS-GVO Art. 7 para 8, who, however, classifies consent as a "real act".

[245] Michael Funke, 'Die Vereinbarkeit von Data Trusts mit der Datenschutzgrundverordnung (DSGVO)' (Algorithm Watch, December 2020) 15, <https://algorithmwatch.org/de/wp-content/uploads/2020/11/Die-Vereinbarkeit-von-Data-Trusts-mit-der-DSGVO-Michael-Funke-AlgorithmWatch-2020-1.pdf> accessed 13 October 2022 who leaves the question unanswered.

[246] EDPS, 'Opinion 9/2016 on Personal Information Management Systems' (20.10.2016) 8 <https://edps.europa.eu/sites/default/files/publication/16-10-20_pims_opinion_en.pdf> accessed 13 October 2022.

[247] EDPS, ´Opinion on Personal Information Management Systems´ (n 246) 8.

[248] Birgit Hoffmann, ´Einwilligung der betroffenen Person als Legitimationsgrundlage eines datenverarbeitenden Vorgangs im Sozialrecht nach dem Inkrafttreten der DSGVO` [2017] NZS 807 (808); Thomas Janicki, `Die Einwilligungsfähigkeit zwischen Digitalisierung und demographischem Wandel´ [2019] DSRITB 313 (323); Ingold (n 87) Art. 7 para 19; Specht-Riemenschneider, Blankertz, Sierek, Schneider, Knapp, Henne (n 241) 25 (41).

[249] Jürgen Kühling, ´Der datenschutzrechtliche Rahmen für Datentreuhänder´ [2021] ZfDR 1 (8); Funke (n 245) 15.

[250] So correctly: Specht-Riemenschneider, Blankertz, Sierek, Schneider, Knapp, Henne (n 241) 41; Jürgen Kühling, ´Der datenschutzrechtliche Rahmen für Datentreuhänder´ [2021] ZfDR 1 (8).

[251] This is also expected by: *Golland*, NJW 2021, 2238 (2241).

cific circumstances of the situation may lead to a broad interpretation.[252] The background and purpose of the use of PIMS are precisely to give and manage a *typified* consent that is merely *generic*—this must be considered so that the requirement for certainty should already be fulfilled if only objective foreseeability regarding the processing operations is given.[253] However, this is not officially or judicially confirmed, and to avoid legal uncertainty there is a need for legislative action with regard to the possibility of "broad consent".[254] This has already been discussed for medical research[255] and seems very beneficial for PIMS. In its opinion on PIMS, the EDPS already encouraged that the conditions under which this type of broad consent shall be permitted should be examined.[256] The user should be able to give or refuse consent for specific purposes in a bundled way. Of course, there should still be the possibility to decide granularly if this is desired. In the case of broad consent, it must always be ensured that the data subjects are aware that they are practically giving multiple consents and that they are accurately informed about the purposes for which they are giving this multiple consent; comprehensive information for the user is essential. Since the "relaxation" of the strict granularity in Recital 33 explicitly refers only to scientific research and also the opening clause in Article 9 (2) lit. j GDPR has only a very narrow scope of application, a regulatory act with regard to PIMS is mandatory. There has to be a balance between the necessity of informing and educating the user and keeping the system simple and practicable.

2. Technical implementation

116 In addition to the legislative issues, designing a user-friendly, legally compliant, and efficient system is also a technical challenge. So far, there are only a few providers that have already presented widely developed (test) systems, such as *NetID* or *NOYB*. The functioning of NOYBs system "Advanced Data Protection Control" (ADPC) is an extension of the simple DNT-browser setting: web pages can send their privacy requests in a machine-readable way, and ADPC allows the response to be transmitted using special header signals or via Java Script. Similar to a "camera release"-request, users can release their data via a uniform pop-up in the browser. Furthermore, intelligent settings should also be possible, allowing users to choose to receive only certain requests—a function similar to a spam filter.[257] In contrast, NetID's system does not focus on browser signals, but on log-in solutions: users have to register once and can manage their consents and other privacy settings in the NetID portal. When data subjects visit a website, they can use the NetID log-in and the privacy settings are applied directly to the website without the user having to make any additional decisions.[258]

3. Certification procedure

117 It is of utmost importance that the reliability of the data trustees is ensured. Article 26 (1) TTDPA already provides for a certification procedure. In order to assure a high level of data protection, it is essential to ensure that only reliable independent companies receive such certification and not obvious stakeholders. The *Data Ethics Commission* has also warned that if PIMS are designed incorrectly, there is a risk that instead of enabling genuine self-determination, affected persons will be led down a path of unconscious or careless external determination and that the operators of the PIMS can exploit their full decision-making power in a way that is not in line with the users' interests.[259] A strict certification procedure must be in place to ensure that this kind of abuse will not occur. For instance, criticism was voiced against NetID questioning its data-protecting intent, as it was founded by *Mediengruppe RTL Deutschland*, *ProSiebenSat.1* and

[252] Nebel (n 242) 21.

[253] Nebel (n 242) 21.

[254] Specht-Riemenschneider, Blankertz, Sierek, Schneider, Knapp, Henne (n 241) 41.

[255] On this matter: Stefanie Hänold, `Die Zulässigkeit eines„broad consent" in der medizinischen Forschung - a never ending story?` [2020] ZD-Aktuell 06954; Thanos Rammos, `Die datenschutzrechtliche Zulässigkeit von Broad Consent für Forschungszwecke nach der DSGVO´ [2017] DSRITB 359;; Carina Dorneck/Ulrich M Gasser/Jens Kersten/Josef Franz Lindner/Kim Philip Linoh/Katja Nebe/ Henning Rosenau/Birgit Schmidt am Busch,´Contextual Consent` [2019] MedR 431.

[256] EDPS, ´Opinion on Personal Information Management Systems´ (n 246) 8.

[257] Cf. <https://noyb.eu/de/neues-browser-signal-koennte-cookie-banner-ueberfluessig-machen> (accessed on 15th November 2021) accessed 11 December 2022.

[258] Cf. <https://image.netid.de/cd/netid/netid_spot_30.mp4> and <https://image.netid.de/cd/netid/netid_spot2_30.mp4> accessed 11 December 2022.

[259] Gutachten der Datenethikkommission, 23.10.2019, Sec. 4.3.2 <https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=98CEBC17A4DF3180E-939F10819AC4129.2_cid295?__blob=publicationFile&v=6> accessed 11 December 2022.

United Internet.[260] According to some critics, the fact that such media and Internet giants do not primarily have the interests of the data subjects in mind becomes particularly evident as NetID uses dark patterns.[261] These are intended to ensure that as much data as possible can be collected.[262] Such circumstances should be taken into account in the certification process; on the other hand, not only strict consumer protection organizations should be certified, since PIMS should not be designed to reject all queries in general. They should be auxiliary tools that allow the users to exercise their decision-making authority and do not deprive them of this authority in one direction or the other.

118 Overall, PIMS have great potential to minimize the above-mentioned problems[263], but their success depends on the legislative requirements for their design and in particular, on whether they are technically feasible.

I. Conclusion

119 In conclusion, it can be stated that despite sector-specific regulations, the requirements of the GDPR are central and form the benchmark for the analysis of consent tools, primarily because the ePrivacy Directive, the TTDPA, and the draft of the ePrivacy Regulation refer to its regulatory regime. This means that for the storage and access or other processing of personal and non-personal data, it is generally necessary to obtain a clear, informed, voluntary, and granular consent.

120 Even if no explicit specifications are made for the design, it follows from these requirements that the cookie banner must be clearly visible and contain all the necessary information in clear and simple language; care must be taken to ensure that this information is arranged in a reasonable manner and, if necessary, can be accessed via easy-to-find dropdown menus or sidebars. The data subject must be given the opportunity to give his or her consent or refusal granularly for each processing purpose, the listing of the purposes, and, if applicable, third-party providers must also be done in a transparent manner, and a simple, if possible bundled, selection and deselection option must be provided. The information should already be available on the first level and not be hidden behind links or in the data protection declaration. In addition, the labelling and design of the buttons must be as neutral and comprehensible as possible, and misleading colour choices or designations must be avoided. Other forms of negative nudging or dark patterns must also be averted, even if the applicable standards do not advocate any explicit prohibitions in this regard, a design that is intended to cause behavioural anomalies for the user regularly violates the principle of voluntariness and the transparency respectively information obligation.

121 Even cookie banners that meet these requirements and are therefore formally legally compliant cannot completely prevent practical problems such as consent fatigue. It is therefore important to examine new forms of consent management that allow users to manage their consent centrally in order to avoid constant consent queries. However, these PIMS must also enable a voluntary, informed and, in principle, granular decision; it remains to be seen to what extent this will be implemented by the expected ePrivacy Regulation. Until then, it remains that users must be able to give their consent on websites they visit or apps they use according to the picture drawn here.

[260] Florian Meier,´Datenkrake im Schafspelz: netID´ (2019) flomei-online <https://www.flomei.de/blog/2019/12/15/datenkrake-im-schafspelz-netid/> accessed 11 December 2022.

[261] In detail: Torsten *Kleinz*, ´NetID: LogIn-Allianz startet mit 60 Partnerseiten´ (2018) heise-online <https://www.heise.de/newsticker/meldung/NetID-LogIn-Allianz-startet-mit-60-Partnerseiten-4216340.html> accessed 11 December 2022.

[262] Meier (n 260).

[263] Cf. Part H.3.