

Wiedemann, Klaus

Article — Published Version

The ECJ's Decision in "Planet49" (Case C-673/17): A Cookie Monster or Much Ado About Nothing?

IIC - International Review of Intellectual Property and Competition Law

Provided in Cooperation with:

Springer Nature

Suggested Citation: Wiedemann, Klaus (2020) : The ECJ's Decision in "Planet49" (Case C-673/17): A Cookie Monster or Much Ado About Nothing?, IIC - International Review of Intellectual Property and Competition Law, ISSN 2195-0237, Springer, Berlin, Heidelberg, Vol. 51, Iss. 4, pp. 543-553, <https://doi.org/10.1007/s40319-020-00927-w>

This Version is available at:

<https://hdl.handle.net/10419/288623>

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.



<https://creativecommons.org/licenses/by/4.0/>



The ECJ's Decision in “*Planet49*” (Case C-673/17): A Cookie Monster or Much Ado About Nothing?

Klaus Wiedemann

Published online: 23 March 2020
© The Author(s) 2020

Abstract In “*Planet49*”, the ECJ ruled that a pre-selected checkbox on a website (which the user must actively deselect to refuse consent) does not constitute valid consent under data protection law. In this context, the Court also provided guidance on the extent of the existing informational duties. It furthermore found that it does not make a difference with respect to Art. 5(3) ePrivacy Directive whether or not information that is stored or accessed on the terminal device of a user constitutes personal data. The majority of these findings is not surprising and in accordance with the values underlying today's data protection and privacy regulations. Unfortunately, the ECJ failed to address the role Art. 7(2) GDPR plays for online declarations referring to both consent *and* other matters. It thus missed a valuable opportunity to provide further clarity on how consent can be given in a way that is compliant with data protection regulations and user-friendly at the same time. Unfortunately, the Court was not asked to show a way out of the dogmatic Gordian knot arising from the German Telemedia Act, parts of which are still in clear contradiction to Art. 5(3) ePrivacy Directive.

Keywords Data protection law · Online privacy · Consent · Cookies · GDPR · ePrivacy Directive

1 Facts of the Case

1.1 Introduction

In late 2019, the European Court of Justice (ECJ) issued a judgment in Case C-673/17 (*Planet49*) upon a request for a preliminary ruling (Art. 267 Treaty on the

K. Wiedemann (✉)
Junior Research Fellow, Max Planck Institute for Innovation and Competition, Munich, Germany
e-mail: klaus.wiedemann@ip.mpg.de

Functioning of the European Union) by the German Federal Supreme Court.¹ The questions stemming from the underlying proceedings between the Federal Union of Consumer Organisations and Associations (Federation of Consumer Organisations) and Planet49 GmbH, an online gaming company, refer to the granting of consent to data processing in online environments and corresponding side issues. Fortunately, due to procedural issues the ruling refers not only to the (repealed) Data Protection Directive² (DPD), but also to the General Data Protection Regulation³ (GDPR).⁴ The focus of the decision is on the interplay of either regime with the so-called ePrivacy Directive.⁵ In the following, the analysis will mainly examine the interplay of the ePrivacy Directive and the GDPR.

1.2 Matter in Dispute

The matter in dispute was an online promotional lottery organised by Planet49 GmbH.⁶ To participate, users had to provide their name and address. They were confronted with a webpage containing three items relevant for the legal analysis: two bodies of explanatory text (each accompanied by a checkbox) and a button which roughly read “Click here to participate free of charge”. The first checkbox was *not* pre-selected. The attached text basically allowed third parties to contact users by post, telephone, e-mail, etc. for advertising purposes. The second checkbox contained a *pre-selected* tick. Its accompanying text read: “I agree to the web analytics service Remintrex being used for me. This has the consequence that [Planet49] sets cookies, which enables Planet49 to evaluate my surfing and use behaviour on websites of advertising partners and thus enables advertising by

¹ Case C-673/17, *Planet49*, 1 October 2019, ECLI:EU:C:2019:801. For the headnotes to this decision see this issue of IIC at <https://doi.org/10.1007/s40319-020-00926-x>.

² Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31, 23 November 1995.

³ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1, 4 May 2016.

⁴ Cf. Case C-673/17, *Planet49*, 1 October 2019, ECLI:EU:C:2019:801, paras. 38–43: The GDPR became applicable during the national proceedings. Thus, it will most likely be applied in the main proceedings. This is why the ECJ passed judgment on either regime.

⁵ 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 201/37, 31 July 2002, amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337/11, 18 December 2009. Until today, legislators have failed to introduce the so-called ePrivacy Regulation, which was supposed to replace the ePrivacy Directive (cf. the original proposal, European Commission (2017)). After a variety of different drafts were not endorsed by the EU Member States, the ePrivacy Regulation’s future currently remains unclear.

⁶ Case C-673/17, *Planet49*, 1 October 2019, ECLI:EU:C:2019:801, paras. 25–31.

Remintrex that is based on my interests. (...)” Thus, the pre-selected second checkbox allowed extensive cookie-based tracking of users for advertising purposes. Before clicking the button, users had to actively tick the first checkbox, while it was *not* mandatory to leave the second checkbox ticked. Users were free to untick the box and, in doing so, deny consent to the placing of cookies (and subsequent tracking).⁷

1.3 Questions Referred to the Court

Three questions were submitted to the ECJ, all of which only refer to the second, pre-selected checkbox.⁸ Firstly, is valid consent given within the meaning of Arts. 5(3) and 2(f) ePrivacy Directive, read in conjunction with Art. 2(h) DPD or, now, Art. 6(1)(a) GDPR, if the storage of information, or access to information already stored in the user's terminal equipment, is permitted by way of a pre-selected checkbox which the user must deselect to refuse his or her consent? Secondly, what information does the service provider have to give, according to Art. 5(3) ePrivacy Directive, within the scope of the provision of clear and comprehensive information to the user – and does this include the duration of the operation of the cookies and whether third parties are given access to the cookies? Thirdly, when information is stored or accessed in accordance with Art. 5(3) ePrivacy Directive, does it make a difference whether or not this information constitutes personal data under data protection law?

2 Decision of the Court

2.1 Consent by Means of a Pre-Selected Checkbox?

It is not surprising that the ECJ ruled in response to the first question that a pre-selected checkbox which the user must deselect to refuse his or her consent does not constitute valid consent for the data processing envisaged by Planet49.

2.1.1 Reasoning of the Court

The ECJ's primary line of argumentation is that *active behaviour* on the part of the user is necessary for valid consent.⁹ Thus, a pre-selected checkbox does not suffice. This is convincing and holds true under the DPD and the GDPR. In terms of methodology, the ECJ's interpretation of the relevant statutes is of a literal and a historical nature.

The starting point of this assessment is the wording of the first sentence of Art. 5(3) ePrivacy Directive:

⁷ *Ibid.*, para. 28.

⁸ The request consisted of two main questions, whereby the first was divided into three sub-questions. For the sake of structure, they will be analysed here in a different order and partially combined.

⁹ Case C-673/17, *Planet49*, 1 October 2019, ECLI:EU:C:2019:801, paras. 49–62.

Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with [the DPD], inter alia, about the purposes of the processing.

Article 2(f) ePrivacy Directive links the ePrivacy Directive to the DPD. The term “consent” under the ePrivacy Directive refers to the definition contained in Art. 2(h) DPD. Pursuant to Art. 94(2) GDPR, this link now refers to the GDPR’s definition of consent in Art. 4(11) GDPR.

Firstly, the ECJ refers, by means of a literal interpretation, to the wording of Art. 5(3) ePrivacy Directive. This provision does not directly state *how* consent should be granted, but still implies that the act of granting consent is an active one (“given his or her consent”).¹⁰ This is supported by Recital 17, which lists “ticking a box when visiting an Internet website”, an active behaviour, by way of example in the context of the granting of consent. This finding is complemented by Art. 2(h) DPD, where consent is defined as a “freely given specific and informed indication” of the data subject’s wishes. Use of the term “indication” indeed implies active behaviour. Also, consent must be given “unambiguously”.¹¹ This is only possible when the user takes action (as opposed to remaining passive). Under the GDPR, the legal situation is defined in an even clearer manner. According to Art. 4(11) GDPR, consent means “any (...) indication of the data subject’s wishes (...) by a statement or by a clear affirmative action (...)”. The term “clear affirmative action” strongly suggests active behaviour on the part of the user. *In casu*, Recital 32 GDPR provides a killer argument, declaring that “[s]ilence, pre-ticked boxes or inactivity should not (...) constitute consent.” This interpretation¹² of Art. 4(11) GDPR barely leaves any doubt that the pre-selected checkbox did not constitute valid consent.

This line of reasoning is supported by means of a historical interpretation. The initial 2002 ePrivacy Directive demanded in its Art. 5(3) that the user “is provided with clear and comprehensive information in accordance with [the DPD] (...) and is offered the right to refuse such processing”. This opt-out approach was replaced in 2009, whereas now the user must have “given his or her consent”. This deliberate change of wording shows that consent now must result from an (active) opt-in, as opposed to the opt-out solution in place before.¹³

2.1.2 Between-the-Line-Implications on Art. 7(2) GDPR

In the following, it will be argued that the ECJ’s decision on Art. 5(3) ePrivacy Directive is convincing, even though the Court failed to explicitly address one question worthy of note (regarding the interpretation of Art. 7(2) GDPR), which is decisive for the matter

¹⁰ Case C-673/17, *Planet49*, 1 October 2019, ECLI:EU:C:2019:801, para. 49.

¹¹ Art. 7(a) DPD.

¹² Recitals are not supposed to have an autonomous legal effect, but rather serve as a tool to interpret the corresponding provisions in the binding part of the respective legal act; Baratta (2014), pp. 302–303.

¹³ Case C-673/17, *Planet49*, 1 October 2019, ECLI:EU:C:2019:801, para. 56.

in dispute and for future cases. Still, based on what has *not* been said, *Planet49* can be of value for the interpretation of Art. 7(2) GDPR and for further defining the conditions for the granting of valid consent in online environments.

The ECJ has been criticised¹⁴ for not discussing and solving the present case under Art. 7(2) GDPR, which reads:

If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

The underlying idea of this argument is as follows: Art. 7(2) GDPR takes for granted that consent can be given as part of a "written declaration which also concerns other matters".¹⁵ The most common scenario would probably be a demand for consent contained in terms and conditions, whereas the latter also refers to other subject matter (such as delivery time and costs, warranty issues, etc.). In the case at hand, one might argue that the button and the two checkboxes combined represent such a declaration. Consequently, the behaviour on the part of the user might, arguably, be considered active. She has to actively click the button in order to participate in the lottery, which could be considered an indication of agreeing with the text next to the second checkbox. This might be enough to assume an "affirmative action" under Art. 4(11) GDPR.

Blame can be laid on the ECJ for not openly mentioning, let alone discussing, Art. 7(2) GDPR, as this line of argumentation is rather obvious and might also be invoked by other data controllers in similar situations. Yet, the way the Court argues implies that it was aware of this statute, but simply found that the overall conditions for valid consent were not given. This finding is correct, for different reasons, and – even though every case calls for individual assessment – provides valuable general implications for the assessment of the validity of consent.

Firstly, the underlying rationale of Art. 7(2) GDPR is to *protect* data subjects by making sure, through formal requirements, that the request for consent is made in a visually transparent and intellectually understandable manner.¹⁶ Put differently, the statute does not aim at lowering the threshold for the giving of valid consent, but at raising and specifying the level of protection instead. This is in line with the ECJ's argument that "the fact that a user selects the button to participate in the promotional lottery organised by that company cannot (...) be sufficient for it to be concluded that the user validly gave his or her consent to the storage of cookies."¹⁷ The Court argues that the consent given in the case at hand was not "specific" enough according to Art. 4(11) GDPR.¹⁸ With a view to the design of the website

¹⁴ Hanloser (2019), pp. 560–561.

¹⁵ The term "written declaration" includes statements given by electronic means (Recital 32 GDPR).

¹⁶ Cf. Klement in Simitis et al. (2019), Art. 7, para. 75.

¹⁷ Case C-673/17, *Planet49*, 1 October 2019, ECLI:EU:C:2019:801, para. 59.

¹⁸ Case C-673/17, *Planet49*, 1 October 2019, ECLI:EU:C:2019:801, para. 58. Alternatively, one might argue (as does Klement, *supra* note 16, para. 77) that Art. 7(2) GDPR specifies the requirement that consent be "informed" and "unambiguous" (Art. 4(11) GDPR).

presented to the users, this is convincing. A “declaration which also concerns other matters” should not serve as a means of circumventing the safeguards that lawmakers wanted to put in place. At the same time, the Court’s arguing underlines that Art. 7(2) GDPR draws a fine, delicate line between valid and invalid consent. The ECJ fortunately did not follow the Advocate General (AG), who argued that “participation in the online lottery and the giving of consent (...) cannot form part of the same act.”¹⁹ This approach would render Art. 7(2) GDPR (de facto) void and create unnecessary obstacles to the granting of consent.²⁰ Thus, had the text on the button, for instance, made clear reference to the data protection implications given, clicking it would have included specific, valid consent.²¹

Secondly, the ECJ’s reasoning confirms that for a meaningful assessment, it is imperative to consider *all* provisions relevant, in particular Arts. 4(11), 6(1)(a) and 7 GDPR. These statutes must be read in conjunction and with a view to the corresponding Recitals when assessing the validity of consent in a given case.²² The user’s viewpoint is to be taken, without unduly dividing what is presented to him in an artificial manner. In the present case, this means that the complete œuvre of items shown to users by Planet49 must be assessed in its entirety and with the abovementioned statutes’ *telos* in mind. It is obvious that a user clicking the button would like to participate in the lottery. Yet, it is convincing when the ECJ implicitly argues that this act of clicking is neither an “unambiguous indication” of his or her wishes nor a “clear affirmative action” with a view to the extensive online tracking envisaged by Planet49. Clicking the button has nothing to do per se with the granting of consent to the processing of personal data. Users just want to participate in the lottery. Thus, assuming a “specific” indication of a wish to consent to the processing of their personal data seems too far-fetched.²³ This is also underlined by the basic rationale of Recital 32, that “[s]ilence, pre-ticked boxes or inactivity should not (...) constitute consent.” Accordingly, one should not argue that all kinds of active behaviour suffice per se. Rather, a holistic assessment of the individual circumstances must find that the way in which consent is granted reflects the GDPR’s spirit in that it must be given actively. One might argue²⁴ that the second checkbox actually increases the user’s freedom. She is able to deny consent but still participate in the lottery, which could imply “freely given” consent (Art. 4(11) GDPR). But judging from the disputed website’s layout, a free, deliberate choice can be doubted. The requirement to actively tick the first checkbox suggests, from a user’s point of view, that the second checkbox must be left ticked as well. Put differently, a user must get the impression that if it is necessary to tick the first box,

¹⁹ Case C-673/17, *Planet49*, 21 March 2019, ECLI:EU:C:2019:246, para. 89.

²⁰ Cf. Moos and Rothkegel (2019), p. 738.

²¹ *Ibid.*

²² Cf. Buchner and Petri in Kühling and Buchner (2018), Art. 6, para. 18.

²³ Case C-673/17, *Planet49*, 1 October 2019, ECLI:EU:C:2019:801, para. 58. In this regard, Art. 4(11) GDPR is complemented by the principle of purpose limitation (Art. 5(1)(b) GDPR). In the context of consent, this principle must be read in conjunction with Art. 6(1)(a) GDPR and demands a certain level of specificity of the consent granted (Buchner and Kühling in Kühling and Buchner (2018), Art. 7, para. 61).

²⁴ Hanloser (2019), p. 561.

she will not be able to proceed without leaving the second box checked all the more.²⁵

2.2 Informational Duties

In response to the second question, the ECJ ruled that Art. 5(3) ePrivacy Directive must be interpreted “as meaning that the information that the service provider must give to a website user includes the duration of the operation of cookies and whether or not third parties may have access to those cookies.”²⁶ This is (mostly) true under the DPD and the GDPR.

Article 5(3) ePrivacy Directive demands that the user be “provided with clear and comprehensive information, in accordance with [the DPD]”. Article 10 DPD lists the information to be provided in a non-exhaustive (“at least”) manner. With a view to the extensive amount of profiling made possible by tracking,²⁷ the ECJ’s interpretation that the duration of the operation of cookies must be provided is convincing. Under the GDPR, this discussion is obsolete, as the information has to be provided anyway.²⁸ In addition, under Arts. 10(c) DPD and 13(1)(e) GDPR, the recipients or categories of recipients of the data must be provided.

Two points are noteworthy.²⁹ Firstly, as regards third-party data sharing, it is not clear whether, according to the ECJ, the service provider would also be obliged to inform users about the fact that data are *not* shared with third parties (“whether or not third parties may have access”³⁰). Under the GDPR, it would be rather difficult to argue for an obligation this far-reaching.³¹ Article 13(1)(e) GDPR states that “the controller shall (...) provide the data subject with all of the following information: (...) the recipients or categories of recipients of the personal data, *if any*”.³² This wording implies that an informational duty only exists when there *are* third-party recipients in the first place. With a view to the present case, this discussion is an academic one, as setting cookies in the context of an advertising network is barely possible without third-party data sharing. But for other data controllers,³³ it makes a difference whether they *always* have to inform if third-party recipients exist. Secondly, the ECJ did not discuss whether consent is only “informed” (Art. 4(11) GDPR) when the data controller has complied with the informational duties arising from Arts. 13–14 GDPR. One might argue that a user is only capable of giving truly

²⁵ AG Szpunar argues, based on the premise that users were not informed that the second checkbox can be unticked, that no “informed” (Art. 4(11) GDPR) consent was given (Case C-673/17, *Planet49*, 21 March 2019, ECLI:EU:C:2019:246, paras. 91–92).

²⁶ Case C-673/17, *Planet49*, 1 October 2019, ECLI:EU:C:2019:801, para. 71.

²⁷ *Ibid.*, para. 78.

²⁸ Art. 13(2)(a) GDPR.

²⁹ See Hanloser (2019), p. 562.

³⁰ Case C-673/17, *Planet49*, 1 October 2019, ECLI:EU:C:2019:801, para. 81.

³¹ Art. 10(c) DPD is drafted more openly: “at least the following information”, “any further information such as”.

³² Emphasis added.

³³ Art. 4(7) GDPR.

informed consent when she has received all the information pursuant to these statutes. Yet, the answer to this question is quite foreseeable, as Recital 42 implies differently: “For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended.” The small amount of information to be provided “at least” suggests that informed consent can be given even if the data controller does not comply with all her informational duties.³⁴

2.3 “Information” under Art. 5(3) ePrivacy Directive

The ECJ found that in the context of Art. 5(3) ePrivacy Directive, it makes no difference whether the information stored or accessed constitutes personal data under the DPD or GDPR.³⁵ This is correct. The ePrivacy Directive chose not to use the term “personal data” in its Art. 5(3), but in many other instances, and its Recital 24 makes clear that the private sphere of users can be threatened through “spyware, web bugs, hidden identifiers and other similar devices” that do not necessarily qualify as personal data.³⁶

The term information is broader than personal data. This means that protection under the ePrivacy Directive is given at an earlier point in time than under the DPD and the GDPR. Information flows are (partially) regulated, no matter if they represent personal data or not. In online contexts, once enough information stored on the terminal equipment of a user is collected and combined, its legal qualification might “tip” and it might be qualified as personal data under data protection legislation.³⁷ This in turn means that all the GDPR safeguards and obligations apply.³⁸ The “pivot point” is reached, as a rule of thumb, with identifiability of the natural person.³⁹ The legal qualification of information might change during the course of time for different reasons.⁴⁰ This renders data protection compliance

³⁴ The same outcome is reached by Art. 29 Working Party (2018), p. 15 and by Buchner and Kühling in Kühling and Buchner (2018), Art. 7, para. 59.

³⁵ Case C-673/17, *Planet49*, 1 October 2019, ECLI:EU:C:2019:801, para. 71.

³⁶ The term personal data is defined in Arts. 2(a) DPD and 4(1) GDPR.

³⁷ It has been proven in various contexts that sometimes very few pieces of information suffice to establish a link to the identity of a natural person. Cf. Sweeney (2000), p. 1 who found that “combinations of few characteristics often combine in populations to uniquely or nearly uniquely identify some individuals. (...) It was found that 87% (216 million of 248 million) of the population in the United States had reported characteristics that likely made them unique based only on [their 5-digit ZIP code, gender and date of birth].”

³⁸ The GDPR is only applicable when personal data are processed: Art. 2(1) GDPR. The processing of mere information does not suffice. On the distinction between the terms privacy and data protection, cf. Kokott and Sobotta (2013) *passim*.

³⁹ Cf. Art. 4(1) GDPR: Personal data might be given no matter if the person they relate to is identified or identifiable, whereby the latter “is one who can be identified, directly or indirectly (...)”. Also see Recital 30 GDPR: The association of natural persons with online identifiers “may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.”

⁴⁰ For instance, see Recital 26 GDPR: “To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments” (emphasis added).

cumbersome, as could be witnessed in the notorious *Breyer* decision.⁴¹ The responsibility to assess if personal data are given (or not yet given) lies with the data controller.

In sum, Art. 5(3) ePrivacy Directive can be seen as part of a two-step protection regime: privacy implications stemming from the processing of information are partially tackled (only) under the ePrivacy Directive, while data protection implications stemming from the processing of personal data fall, in addition, under the GDPR.

3 Further Thoughts

It is unfortunate that the ECJ was not asked to decide whether the German Telemedia Act, Sec. 15(3) is compatible with Art. 5(3) ePrivacy Directive. This national statute “authorises a service provider to establish user profiles through pseudonyms for purposes of advertising, market analysis, or configuration of electronic media, provided that the user does not object and the service provider has informed the user of his or her right of refusal (...).”⁴² This opt-out solution (“does not object”) is in clear-cut contradiction to the opt-in requirement contained in Art. 5(3) ePrivacy Directive (“has given his or her consent”).⁴³

In its request for a preliminary ruling, the German Federal Supreme Court indicated that an interpretation of Sec. 15(3) Telemedia Act in line with the ePrivacy Directive would be possible.⁴⁴ This approach is questionable, as this interpretation would run entirely counter to the wording of the national statute. Also, a direct application of Art. 5(3) ePrivacy Directive is not possible, as Directives cannot create obligations for individuals.⁴⁵ With a view to the primacy of EU law, the lesser dogmatic evil would probably be not to apply Sec. 15(3) Telemedia Act at all. This has also been suggested by the *Datenschutzkonferenz*, which is a joint body of the data protection authorities of the German federal and state governments.⁴⁶ Consequently, this would mean that in Germany, the cases which are supposed to fall under Sec. 15(3) Telemedia Act would fall instead under the GDPR. This leads to various dogmatic questions, e.g. whether a data controller (who would like to establish user profiles) could rely not only on consent,⁴⁷ but alternatively on its legitimate interests as legal basis: Art.

⁴¹ Case C-582/14, *Breyer*, 19 October 2016, ECLI:EU:C:2016:779. The case dealt, *inter alia*, with the question under which circumstances dynamic IP addresses are personal data. The ECJ gave a great deal of attention to the aspect of identifiability (*cf.* paras. 31–49).

⁴² Opinion of AG Szpunar, Case C-673/17, *Planet49*, 21 March 2019, ECLI:EU:C:2019:246, para. 21.

⁴³ Sec. 15(3) Telemedia Act was not amended in line with the 2009 amendment of Art. 5(3) ePrivacy Directive and, thus, still reflects the initial version of the ePrivacy Directive.

⁴⁴ Case No. I ZR 7/16, *Planet49*, 5 October 2017, ECLI:DE:BGH:2017:051017BIZR7.16.0, para. 13.

⁴⁵ This has been settled case law of the ECJ since Case C-152/84, *Marshall*, 26 February 1986, ECLI:EU:C:1986:84, para. 48; *cf.* for instance Case C-201/02, *Wells*, 7 January 2004, ECLI:EU:C:2004:12, para. 56.

⁴⁶ *Datenschutzkonferenz* (2019), p. 6.

⁴⁷ Art. 6(1)(a) GDPR.

6(1)(f) GDPR.⁴⁸ An apparently incoherent picture would become manifest. The scope of application of Art. 5(3) ePrivacy Directive is broad, referring to information, whereas the GDPR only covers personal data processing. Yet, the former legal regime strictly demands consent, whereas the latter is more flexible by also providing a legal basis (legitimate interests) that can be applied without user consent. This shows that the ePrivacy Directive is not only part of the two-step protection regime pictured above, but also *lex specialis* to the GDPR. Thus, Art. 6(1)(f) GDPR should not be accepted as the legal basis for the placing of cookies, as this runs counter to the rationale of the ePrivacy Directive's opt-in solution. This is in line with the reasoning of the ECJ (in a different context) that "the interpretation of a provision of EU law requires that account be taken not only of its wording and the objectives it pursues, but also of its legislative context and the provisions of EU law as a whole".⁴⁹ Hence, in the context discussed here, Art. 6(1)(f) GDPR should be interpreted in line with Art. 5(3) ePrivacy Directive to the effect that legitimate interests are regularly *not* given.⁵⁰ Apart from that, a protection gap resulting from Germany's legislative inaction still exists, taken that the GDPR only covers the processing of personal data, whereas Art. 5(3) ePrivacy Directive covers all sorts of information.⁵¹

These questions might become obsolete as a revision of the Telemedia Act is now under consideration. Delivery of the judgment of the German Federal Supreme Court has been scheduled for 28 May 2020. It remains to be seen whether the Court will be able to undo the Gordian knot pictured above.

Acknowledgments Open access funding provided by Projekt DEAL.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

Article 29 Working Party (2018) Guidelines on Consent under Regulation 2016/679 (last revised and adopted on 10 April 2018), 17/EN, WP259 rev.01. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051. Accessed 25 Feb 2020

⁴⁸ According to Recital 47 GDPR, the processing of personal data for direct marketing purposes may fall under this clause. Also, in Case C-131/12, *Google Spain*, 13 May 2014, ECLI:EU:C:2014:317, para. 81 the ECJ took for granted that economic interests are legitimate interests (referring to Art. 7(f) DPD, which is the predecessor to Art. 6(1)(f)).

⁴⁹ Case C-673/17, *Planet49*, 1 October 2019, ECLI:EU:C:2019:801, para. 48.

⁵⁰ Also cf. Moos and Rothkegel (2019), p. 740.

⁵¹ *Ibid.*

- Baratta R (2014) Complexity of EU law in the domestic implementing process. *Theory Pract Legis* 2(3):293–308
- Datenschutzkonferenz (2019) Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien. https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf. Accessed 25 Feb 2020
- European Commission (2017) Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10 January 2017, COM(2017) 10 final. <https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications>. Accessed 25 Feb 2020
- Hanloser S (2019) Anmerkung [Case Note on Planet49]. *ZD* 9(12):560–562
- Kokott J, Sobotta C (2013) The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *Int Data Priv Law* 3(4):222–228
- Kühling J, Buchner B (eds) (2018) *Datenschutz-Grundverordnung/BDSG—Kommentar*, 2nd edn. C.H. Beck, Munich
- Moos F, Rothkegel T (2019) Anmerkung [Case Note on Planet49] *MMR* 22(11):736–740
- Simitis S et al (eds) (2019) *Datenschutzrecht—DSGVO mit BDSG*, 1st edn. Nomos, Baden-Baden
- Sweeney L (2000) Simple demographics often identify people uniquely. Carnegie Mellon University, Data Privacy Working Paper 3. <https://dataprivacylab.org/projects/identifiability/paper1.pdf>. Accessed 25 Feb 2020

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.