Analyzing Zoom's Customer License Grant clause

Benjamin Lim (mail@limbenjamin.com)

Zoom is a videoconferencing platform that allows its users to have video calls with each other. Other features include the ability to record video calls and have auto-generated live transcription of the call. In July 2023, Zoom modified their Terms of Service (ToS) to include a "Customer license grant" clause which sought to

> grant Zoom a perpetual, worldwide, non-exclusive, royalty-free, sublicensable, and transferable licence and all other right required or necessary to redistribute, publish, import, access, use, store, transmit, review, disclose, preserve, extract, modify, reproduce, share, use, display, copy, distribute, translate, transcribe, create derivative works, and process Customer Content and to perform all acts with respect to the Customer Content: [. . .] (ii) for the purpose of product and service development, marketing, analytics, quality assurance, machine learning, artificial intelligence, training, testing, improvement of the Services, Software, or Zoom's other products, services, and software, or any combination thereof [1].

As stated in the ToS, the term "Customer Content" includes "content, files, documents, or other materials" uploaded by the customer [2]. This includes the video stream itself which would constitute personal data since an individual can be identified from the video. Due to public discontent, Zoom eventually backtracked and removed the controversial clause. In this essay, I will explore whether this clause complies with Article 6(1)(a) and Article 6(1)(b) of European Union's General Data Protection Regulation (GDPR).

---

1 Zoom, 'Zoom Terms of Service — Zoom' (*Zoom*, 27 July 2023) <https://web.archive.org/web/20230806121701/https://explore.zoom.us/en/terms/> accessed 11 November 2023, clause 10.4

2 Zoom (n 1), clause 10.1

Data Privacy as a fundamental human right

The GDPR can be traced back to its genesis in the 1948 UN Universal Declaration of Human Rights (UDHR), of which article 12 protects the right to privacy of *inter alia* an individual, his home and his correspondence [3]. With the advancement of technology, more facets of an individual's life and his or her communication takes place digitally. *A fortiori*, it is inevitable that the right to protection must extend to personal data. One of the earlier efforts was the Data Protection Directive (DPD) [4], which is *lex specialis* regulation addressing personal data protection. A major change occurred in 2009 when the Charter of Fundamental Rights (CFR) of the European Union (EU) came into force. The right of an individual to the protection of his or her personal data is now enshrined as a fundamental human right [5].

Consent as a last resort

Article 6(1) of the GDPR lays down 6 conditions under which data processing can be considered lawful. Article 6(1)(a) is the clause of last resort if all the other 5 conditions cannot be fulfilled [6]. It specifies that consent must be obtained from the data subject. Logically, if the data processor had the mandate to process the data lawfully under any other condition, there is no reason to take an extra step of obtaining consent. Consent is unnecessary and meaningless since the data processor can still process data lawfully even if the data subject refused to consent. Thus, Article 6(1)(a) must be the clause of last resort that is invoked only if processing cannot be justified under the other conditions. When analyzing Zoom's clause later in the essay, we have to take into context that we would not be looking at Article 6(1)(a) if processing was lawful under other conditions. Hence, any breach of Article 6(1)(a) would translate to unlawful processing and indicate a breach of the fundamental human right to privacy.

---

3 Universal Declaration of Human Right UDHR, (adopted 10 December 1948 UNGA Res 217 A(III)) (UDHR), art. 12

4 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 [1995] OJ L281/31

5 Charter of Fundamental Rights of the European Union [2000] OJ C364/1, art. 8

6 Damien Welfare, *Cornerstone on Information Law* (Bloomsbury Professional 2019), pp. 56

GDPR v Data Protection Directive

The GDPR has only been in force for the last 5 years and case law on the GDPR is scant. Later in the essay, I would be bringing up case law from the DPD. Thus, at this juncture, it is also important to establish how Article 6(1)(a) of the GDPR compares to Article 2(h) of the DPD. Article 2(h) of the DPD defines consent using the terms "freely given specific and informed indication", while Article 4(11) of the GDPR defines consent using the terms "freely given, specific, informed and unambiguous indication". It is immediately clear that that the GDPR imposes an additional requirement of unambiguity on top of what the DPD requires. This is supported in the Article 29 Data Protection Working Party (A29 WP)'s guidelines 05/2020 on consent, which states that guidance provided in Opinion 15/2011 pertaining to the DPD remains valid and that the key requirements for consent carry over to the GDPR [7]. This analysis is also supported in Bundesverband v Planet49, where the court stated that "Article 6(1)(a) of the GDPR [...] appears even more stringent than that of Article 2(h) of Directive 95/46" [8]. A corollary to that statement would be that any practice that violates Article 2(h) of the DPD would also definitely violate the stricter Article 6(1)(a) of the GDPR. Hence, it should be alright to cite DPD cases to support my arguments as long as it pertains to the unlawfulness of certain practices.

Consent must be a choice

Article 6(1)(a) of the GDPR requires that data subjects' consent to the processing of the subject's personal data for purposes which are clearly specified [9]. These few words encapsulate much meaning. For consent to be valid, the data subject must have been given a choice to provide or decline consent. After all, if the data subject was not presented with a choice, has he or she truly consented or was he or she forced to consent. This position is supported by A29 WP's guidelines on consent, where it is stated that consent must be "freely given", if the data subject feels "compelled" or if there are "negative consequences"

---

7 Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679* (2017) <https://ec.europa.eu/newsroom/article29/items/623051>, para. 4

8 Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände v Planet49 GmbH* ECLI:EU:C:2019:801, para. 61

9 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) [2016] OJ L119/1, art. 6(1)(a)

associated with non-consent, then the consent will not be valid [10]. Kosta points out that consent has to be an "autonomous act [...] free from external manipulation" [11]. This position is supported by case law as well. In Meta v Bundeskartellamt, the court noted that consent is not valid if the data subject "has no genuine or free choice" or if refusal comes with "detriments" [12].

When analyzing Zoom's ToS, we observed that modification of ToS comes under the "General Changes" clause [13], where it is stated that "If you continue to use the service [...], then you agree to the revised terms and conditions". It is rather clear that the data subject is left with no choice but to consent in order to continue using the service. Withholding consent would lead to the negative consequence of losing access to the service. Hence such a modification would likely not comply with the GDPR's lawful processing requirements. At this point, critics may argue that the data subject has a choice. They can either choose to use Zoom or choose a competitor if they do not agree with Zoom's data protection policies.

The A29 WP has guidelines for such a scenario as well, justifying that the freedom to choose in such a scenario is contingent on market forces and would implicitly create an obligation for Zoom to monitor developments in the video conferencing market to ensure that data subjects continue to have an alternative [14]. There is also the subjective issue on how to determine if a competitor's service is considered equivalent. The principle of *lex parsimoniae* suggests invalidating the argument with implicit obligations, assumptions, subjectiveness and favoring the straightforward outcome of requiring the company to provide such an alternative themselves. *A fortiori*, since these implicit obligations are not written into the GDPR, any mechanism to enforce them would be *ultra vires* of the GDPR. Hence, the argument cannot be valid. Nonetheless, this argument sets the stage for our next point on companies which dominate the market and create power imbalances.

---

10 Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679* (n 7), para. 3

11 Eleni Kosta, *Consent in European Data Protection Law: Nijhoff Studies in European Union Law* (BRILL 2013), sect. 4.5.1

12 Case C-252/21 *Meta Platforms Inc v Bundeskartellamt* ECLI:EU:C:2023:537, para. 143

13 Zoom (n 1), clause 15.1

14 Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679* (n 7), para. 38

Imbalance of Power

The COVID-19 pandemic brought about a change in working habits. As more individuals started to work remotely, videoconferencing platforms like Zoom witnessed unprecedented growth of up to 2900% in a year [15]. Zoom was reported to have 57% market share of the entire global videoconferencing market in 2023 [16]. This puts Zoom in a position of immense power and there might be a risk that individuals who consented did so because they did not have viable alternatives to turn to. The problem is further compounded by the fact that Zoom does not support cross-platform video calls. All participants in the call have to use Zoom which introduces further imbalance of power when the participant with most power chooses to use Zoom over an alternative. The courts in Madrid and Zurich are among some who have adopted the use of Zoom to conduct video hearings [17]. For Spain in particular, criminal trials with penalties of less than five years of imprisonment can be conducted remotely without consent from the defendant [18]. Defendants in those trials are literally forced to consent to Zoom's ToS to avoid possible further criminal charges for non-appearance before the court.

A29 WP guidelines uses employment as an example of a situation where imbalance of powers exists [19]. Carey also speaks of the "perceived inequality of bargaining power between employees and employers" leading to the problematic nature of the consent [20]. The COVID-19 pandemic has also led to interviews from many companies being conducted over Zoom. Job seekers have no choice but to consent to Zoom's ToS to get a chance at a job. The examples covered illustrate that many users of Zoom may not have freely consented to the ToS, hence consent may not have been lawfully obtained.

To remedy the situation, Zoom could probably work on cross-platform integration with

---

15 Mansoor Iqbal, 'Zoom Revenue and Usage Statistics (2023)' (*Business of Apps*, 18 July 2023) <https://www.businessofapps.com/data/zoom-statistics/> accessed 20 November 2023

16 Lionel Sujay Vailshery, '15 Zoom Users & Revenue Statistics (2023)' (*Statista*, 10 October 2023) <https://www.statista.com/statistics/1331323/videoconferencing-market-share/> accessed 25 November 2023

17 Annie Sanders, 'Video-Hearings in Europe Before, During and After the COVID-19 Pandemic' [2021] 12(2) Internation Journal For Court Administration 3 <https://iacajournal.org/articles/10.36745/ijca.379>, pp. 13

18 Sanders (n 17), pp. 11

19 Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679* (n 7), para. 21

20 Peter Carey, *Data protection: A Practical Guide to UK and EU Law* (Oxford University Press 2015), pp. 67

other videoconferencing software and limit the processing of data to only users using Zoom's own software. Given that Zoom already supports dialing-in and receiving audio over a phone call, it should be possible to extend that functionality to video as well. Participants of video calls using other software would have their videos streamed to Zoom users and their data would subsequently have to be deleted after the conclusion of the call. This would be allowed as it is "necessary for the performance of a contract" to facilitate the communication between two users.

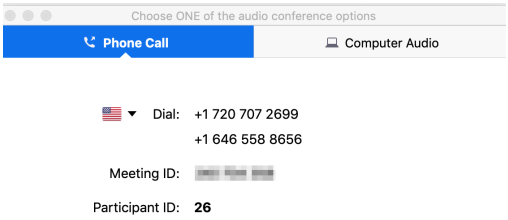

Figure 1: Dialing-in allows participants an alternative to using Zoom software. [21]

Ex Ante Consent

Consent has to be obtained prior to performing data processing. Logically, this has to be so because we would not know if the user would eventually give his or her consent. If consent is eventually withheld, then the *ex post* processing would have been unlawful. This position is supported by Fashion ID v Verbraucherzentrale NRW where the court is of the opinion that it would not be "efficient and timely protection of data subjects' rights" if consent was given after "collection and transmission has already taken place" [22]. This has also been the *de facto* process predating GDPR. The Lindop report stated that Code of Practices in the banking sector mandated employee consent before records are sent to third parties and several survey respondents preferred consent to be obtained at the point of information collection [23].

---

[21] Zoom Developers Forum (https://devforum.zoom.us/t/how-to-retrieve-dial-in-numbers-of-a-meeting/3504) accessed 25 November 2023

[22] Case C-40/17 *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV* ECLI:EU:C:2018:1039, para. 132

[23] Norman Lindop, *Report of the Committee on data protection* (Cmnd 7341, Her Majesty's Stationery Office, London 1978) (Lindop Report), pp. 44

Zoom's COO gave the comment quoted below in response to widespread concerns on the change in ToS.

> Zoom participants receive an in-meeting notice or a Chat Compose pop-up when these features are enabled through our UI [24].

It appears that an "in-meeting notice" is displayed after the participants have joined the meeting. As Zoom has backtracked on their intention to process customer data as outlined in the "Customer license grant" clause, it would not be possible for us to know what the "in-meeting notice" entails. Based on the nomenclature alone, I would assume it is a notice that is displayed during the meeting. This would not comply with Article 6(1) of the GDPR as *ex ante* consent needs to be sought before processing the data. Ideally, this should occur in a "pre-meeting" dialog where data subjects are given a choice to decline. Once participants join the meeting, their voice and video data would be transmitted to other participants and processed by Zoom. At this juncture, it would be too late to seek consent.

Secondly, it is also possible that Zoom's COO meant that an "in-meeting notice" will be displayed when the features are enabled mid-call. In such a scenario, it will be impossible to notify the participants "pre-meeting" because the features were not enabled at that point in time. However, Zoom is also not in the clear. Taking the assumption that the notice merely allows acknowledgment, this is once again not compliant. According to the A29 WP guidelines, controllers need to re-obtain consent for any change in purposes for data processing [25]. Zoom will need to have an "in-meeting dialog" that allows the participant to accept or decline the changes to how their data will be used, and not merely inform the participant of the change.

Informed Consent

According to A29 WP guidelines, controllers have to use plain language and cannot hide behind "long privacy policies" that are "full of legal jargon" [26]. Separately, A29 WP also state

---

[24] ACA Group, 'Zoom's New Terms of Service Create Data Privacy Concerns' (*ACA Global*, 9 August 2023) <https://www.acaglobal.com/insights/zooms-new-terms-service-create-data-privacy-concerns> accessed 25 November 2023

[25] Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679* (n 7), para. 90

[26] Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679* (n 7), para. 67

that “Blanket acceptance of general terms and conditions” cannot constitute lawful consent [27]. The rationale behind the guidelines is that the data subject has to fully understand what he or she is consenting to. Overly long policies that are difficult to understand put the data subject in a difficult position and may entice him to agree without full understanding. Calo has observed similar phenomenon, even going as far to say that “graphic warnings” like those required on cigarette packages, may be required to fully appraise data subjects of the implications of their consent [28].

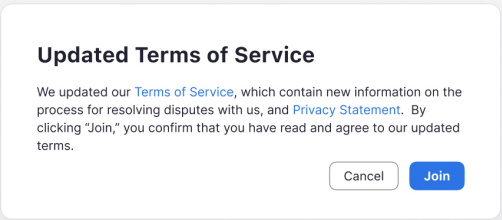

Figure 2: Zoom ToS Update dialog. [29]

Zoom’s ToS update dialog violates both guidelines described above. Firstly, a link to the entire contents of ToS is provided to the data subject. There is no attempt to provide a summarized version in plain language. Secondly, clicking the “Join” button would entail “blanket acceptance” of the entire ToS which is also proscribed. In Bundesverband v Planet49, the court found that consent must be specific, and the data controller cannot “infer” the data subject’s intention [30]. Zoom chose to use the word “Join” instead of “Agree”. This is troubling as it could be argued that Zoom is “inferring” that the data subject has read and consented to the ToS, when the data subject merely joined and did not specifically agree or accept anything. This form of design is known as “Dark Patterns”. The European Data Protection Board (EDPB)’s guidance on dark patterns specifically calls out such a practice, stating that “Look over there” patterns could result in “consent [which] might not be properly informed” [31]. Zoom’s choice of colors for the buttons raises concerns as well.

---

27 Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679* (n 7), para. 81

28 MR Calo, ‘Against Notice Skepticism in Privacy (and Elsewhere)’ [2012] 87 Notre Dame Law Review 1027 <https://scholarship.law.nd.edu/ndlr/vol87/iss3/3/>, pp. 1069-70

29 Zoom Support (https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0057985) accessed 25 November 2023

30 *Bundesverband v Planet49* (n 8), para. 58

31 European Data Protection Board, *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them* (2022) <https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf>, para. 100

The outcome that Zoom is hoping to obtain is displayed in a more appealing blue while the alternative is displayed in a neutral white. This resembles the “Emotional Steering” pattern, where appealing visuals are used in favorable options to influence the user’s emotions and subsequently their behaviour [32]. EDPB’s position is that “Emotional Steering” has implications on informed consent [33]. Zoom could probably do more to condense the changes before presenting it to the user for specific acceptance by using words like “Agree” in a neutral color.

Withdrawal of Consent

An additional condition for consent to be considered valid is the ability for data subjects to withdraw consent in a manner that is equivalent in ease as providing consent [34]. The rationale for allowing withdrawal of consent is due to the voluntary nature of consent. If a data subject is no longer comfortable with the consent but is unable to withdraw his or her consent, then he or she is forced to continue consenting. The GDPR has also mandated that withdrawal needs to be as easy as providing consent. In Orange România SA v ANSPDCP, the court noted that consent “was called into question” since Orange România SA imposed additional burdens on customers who declined to consent, requiring these customers to declare the non-consent in writing [35]. Similarly, a data subject’s consent may be forced simply because he or she is unable to overcome all the hurdles needed to withdraw or reject consent. Kosta builds on this point, arguing that the right to withdraw consent is “derive[d] from the right to informational self-determination” and cannot be waived [36].

Looking at the “Customer License Grant”, Zoom has requested for a “perpetual” license to customer content and a “perpetual, irrevocable” license to service generated data or aggregated anonymous data [37]. It can reasonably be deduced that the license to customer content is not irrevocable, and thus withdrawal of consent is possible. Unfortunately, Zoom

---

32 European Data Protection Board, *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them* (n 31), para. 39

33 European Data Protection Board, *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them* (n 31), sect. 4.3.1

34 Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679* (n 7), para. 85

35 Case Case C-61/19 *Orange Romania SA v Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)* ECLI:EU:C:2019:801, para. 50

36 Kosta (n 11), sect. 4.10.1

37 Zoom (n 1), clause 10.4

did not provide any steps to withdraw consent. Hence, data subjects will have to take substantial effort to contact Zoom to enquire on the withdrawal process if it exists. Since provision of consent is a simple button click and withdrawal requires considerably more effort, the consent obtained from the data subject is likely to be considered invalid.

Granularity of Consent requested

For consent to be lawful, data subjects must be allowed to separately consent to different data processing operations [38]. In addition, if consent is not required for the performance of the contract, it cannot mandate consent as a condition for fulfilment of the contract [39] [40]. The reasoning behind the legislation is to avoid "bundling" of multiple processing operations, some of which are required and others which are optional, in turn forcing the data subject to decide on either "all or nothing". Data subjects must be able to choose which optional data processing operations they would consent to and there should not be any disincentives from withholding their consent for certain operations.

Zoom has clearly "bundled" multiple operations, namely "redistribute, publish, import, access, use, store, transmit, review, disclose, preserve, extract, modify, reproduce, share, use, display, copy, distribute, translate, transcribe, create derivative works" into a single request for consent. Zoom has also bundled multiple purposes, namely "product and service development, marketing, analytics, quality assurance, machine learning, artificial intelligence, training, testing, improvement of the Services, Software, or Zoom's other products, services, and software" into that same request. This is clearly in violation of the requirement for requests to be granular in nature. According to Mantelero, "bundling" is common especially for Big Data processing which "extracts hidden or unpredictable inferences and correlations" from the data [41] as it is difficult to define the purpose when it is exploratory in nature.

Such "bundling" also raises concerns with transparency and may affect whether consent is considered to be informed. According to A29 WP guidelines, the "purpose for each of

---

38 reg 2016/679 (n 9), recital 43

39 reg 2016/679 (n 9), recital 43

40 Welfare (n 6), pp. 57

41 Alessandro Mantelero, 'The Future of Consumer Data Protection in the E.U. Re-Thinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics' [2014] 30 Computer Law & Security Review 643 <https://www.sciencedirect.com/science/article/pii/S026736491400154X>, pp. 652

the processing operations for which consent is sought" must be clearly mentioned [42]. In this case, we are unsure if the request to redistribute *inter alia* falls under which specific purpose. Zoom should split up the operations as well as purposes individually and allow users to consent to each processing operation as per their wishes. Mantelero proposes a different model where a Data Protection Impact Assessment (DPIA) is performed, and adequate measures taken to minimize possible impact of processing instead of specifying the purpose *ex ante* [43]. If such a model is adopted by regulators, it may alleviate the difficulties faced by companies seeking consent for big data processing.

It is important at this point to note that the purposes specified above are all optional and have no bearing on the fulfilment of the contract, which is the provision of videoconferencing services. Zoom does not need to request consent for processing if it is necessary for the provision of their core service. We will explore this in more detail in the next paragraph.

Lawful processing via necessity for performance of contract

Article 6(1)(b) of the GDPR states that processing is lawful if it leads into a contract or is necessary for the fulfilment of the contract [44]. Processing done under this clause does not require consent from the data subject. The rationale behind this clause is to allow the "freedom to conduct business" when it is in the mutual interest of both parties [45]. This is supported in Breyer v Bundesrepublik where the court commented that a data controller can process data without the data subject's consent only if it is "necessary to facilitate and charge for the specific use of those services by that user" [46]. In Meta v Bundeskartellamt, the court also reiterates the position, stating that the controller "must therefore be able to demonstrate how the main subject matter of the contract cannot be achieved if the processing in question does not occur" [47]. The Information Commissioner's Office (ICO)

---

42 Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679* (n 7), para. 64ii

43 Mantelero (n 41), pp. 656-657

44 reg 2016/679 (n 9), art. 6(1)(b)

45 European Data Protection Board, *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* (2019) <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf>, para. 2

46 Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* ECLI:EU:C:2016:779, para. 64

47 *Meta v Bundeskartellamt* (n 12), para. 98

requires processing to be "targeted and proportionate" to be considered necessary [48].

As stated earlier, none of the purposes specified by Zoom in their "Customer license grant" can be considered necessary for the performance of a contract. Even without further "product and service development" or "quality assurance" or "improvement of services", Zoom's existing video call service is still usable. "Marketing" , "analytics" as well as "artificial intelligence" and "machine learning" do not even directly affect the service. Improvement of services as well as marketing has been specifically called out as too vague in A29 WP's opinion on purpose limitation [49]. *A fortiori*, since such operations are done "solely on the initiative of the data controller", they are deemed to be outside the scope of Article 6(1)(b) [50]. Hence, Zoom cannot claim that processing is lawful under Article 6(1)(b) of the GDPR.

As an exercise, let us use the list of "bundled" operations above and attempt to justify how it can be used for the provision of its core videoconferencing service. We could probably argue that the ability to access, transmit and display personal data is necessary for Zoom to fulfill their contractual obligation. Zoom will have to access video from the webcam, transmit it across the web and display that video on the other participants' screen. For participants that wish to make use of Zoom's meeting recording function, Zoom would likely be able to justify storing the recording and publishing it on a private web link for the participant to share with others who wish to watch the recording. For participants that wish to use the automatic captioning feature, transcribing and translating will probably be a reasonable ask.

Processing which leads into a contract is also valid cause under Article 6(1)(b) of the GDPR. If a data subjects requests Zoom to import data from a file and extract certain fields to create a Zoom account, such processing can be considered lawful, since it is "proportionate", involving the storage of only the relevant fields and is necessary for the creation of a Zoom account, which is the act of contract formation.

That said, it would be extremely challenging for Zoom to justify how the remaining operations, namely redistribute, review, disclose, preserve, modify, reproduce and creation

---

48 Information Commissioner's Office, 'A guide to lawful basis' (*Information Commissioner's Office*, 7 October 2022) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/> accessed 3 December 2023

49 Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation* (2013) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>, para. 16, para. 48

50 Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation* (n 49), para. 47

of derivative works are necessary to lead into a contract, fulfill the contract or facilitate the service required by the user.

Conclusion

In this essay, we have explored the importance of having a choice, considered imbalances in power, timeliness of consent, whether consent was sufficiently informed, the ability to withdraw consent and finally granularity of consent. These are all important factors to ensure lawfulness of consent obtained under Article 6(1)(a) of the GDPR. We looked at how Zoom's modified ToS fared under each factor and highlighted areas where Zoom fell short. We then looked at Article 6(1)(b) of the GDPR and concluded that some of the operations might be permitted if the processing was necessary for the performance of the contract. However, all the purposes stated by Zoom in the modified ToS could not be considered necessary. Thus, it is highly unlikely that Zoom's processing of data under the modified ToS could be considered lawful under both Article 6(1)(a) or (b).

With the increasing number of novel uses of data, it is ever more important for consumers to understand their fundamental rights to data privacy so as to safeguard their personal data from exploitation.

Bibliography

Books

Carey P, *Data protection: A Practical Guide to UK and EU Law* (Oxford University Press 2015).

Kosta E, *Consent in European Data Protection Law: Nijhoff Studies in European Union Law* (BRILL 2013).

Welfare D, *Cornerstone on Information Law* (Bloomsbury Professional 2019).

Treaties

Universal Declaration of Human Right UDHR, (adopted 10 December 1948 UNGA Res 217 A(III)).

Legislation

Charter of Fundamental Rights of the European Union [2000] OJ C364/1.

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 [1995] OJ L281/31.

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) [2016] OJ L119/1.

Cases

Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände v Planet49 GmbH* ECLI:EU:C:2019:801.

Case C-40/17 *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV* ECLI:EU:C:2018:1039.

Case C-252/21 *Meta Platforms Inc v Bundeskartellamt* ECLI:EU:C:2023:537.

Case Case C-61/19 *Orange Romania SA v Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)* ECLI:EU:C:2019:801.

Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* ECLI:EU:C:2016:779.

Articles

Calo MR, 'Against Notice Skepticism in Privacy (and Elsewhere)' [2012] 87 Notre Dame Law Review 1027 <https://scholarship.law.nd.edu/ndlr/vol87/iss3/3/>.

Mantelero A, 'The Future of Consumer Data Protection in the E.U. Re-Thinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics' [2014] 30 Computer Law & Security Review 643 <https://www.sciencedirect.com/science/article/pii/S026736491400154X>.

Sanders A, 'Video-Hearings in Europe Before, During and After the COVID-19 Pandemic' [2021] 12(2) Internation Journal For Court Administration 3 <https://iacajournal.org/articles/10.36745/ijca.379>.

Reports

Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation* (2013) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>.

— *Guidelines on consent under Regulation 2016/679* (2017) <https://ec.europa.eu/newsroom/article29/items/623051>.

European Data Protection Board, *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* (2019) <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf>.

— *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them* (2022) <https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf>.

Lindop N, *Report of the Committee on data protection* (Cmnd 7341, Her Majesty's Stationery Office, London 1978).

Secondary Sources

ACA Group, 'Zoom's New Terms of Service Create Data Privacy Concerns' (*ACA Global*, 9 August 2023) <https://www.acaglobal.com/insights/zooms-new-terms-service-create-data-privacy-concerns> accessed 25 November 2023.

Information Commissioner's Office, 'A guide to lawful basis' (*Information Commissioner's Office*, 7 October 2022) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/> accessed 3 December 2023.

Iqbal M, 'Zoom Revenue and Usage Statistics (2023)' (*Business of Apps*, 18 July 2023) <https://www.businessofapps.com/data/zoom-statistics/> accessed 20 November 2023.

Vailshery LS, '15 Zoom Users & Revenue Statistics (2023)' (*Statista*, 10 October 2023) <https://www.statista.com/statistics/1331323/videoconferencing-market-share/> accessed 25 November 2023.

Zoom, 'Zoom Terms of Service — Zoom' (*Zoom*, 27 July 2023) <https://web.archive.org/web/20230806121701/https://explore.zoom.us/en/terms/> accessed 11 November 2023.