Datatilsynet

BRYAN CAVE LEIGHTON PAISNER LLP
One Boulder Plaza, 1801 13th Street, Suite 300, Boulder
CO 80302-5387

Your reference	Our reference	Date
	20/02136-5	24.01.2021

Advance notification of an administrative fine

1. Background

On 24 February 2020, the Norwegian Data Protection Authority ("NO DPA", "we") ordered Grindr LLC ("Grindr") to provide information regarding the sharing of personal data of its users with third party advertisers. We received your reply on behalf of Grindr on 22 May 2020.

The information you provided has not mitigated our concerns regarding the lawfulness of Grindr's personal data sharing with advertising partners.

We are therefore notifying you of our intent to make the decision outlined below.

The purpose of an advance notification is to allow for contradiction. In other words, this a draft decision. Before making a final decision, we will take into account your comments, which you must submit within the time limit specified below.

2. Advance notification

In line with the Norwegian Public Administration Act Section 16, we hereby provide advance notification of our intent to make the following decision:

> *Pursuant to Article 58(2)(i) GDPR, we impose an administrative fine against Grindr LLC of 100 000 000 – one hundred million – NOK for*
>
> - *having disclosed personal data to third party advertisers without a legal basis, which constitutes a violation of Article 6(1) GDPR*
>
> *and*

- *having disclosed special category personal data to third party advertisers without a valid exemption from the prohibition in Article 9(1) GDPR*

Although we have chosen to focus our investigation on the legitimacy of the previous consents in the Grindr application ("app"), there might be additional issues regarding e.g. data minimization in the previous and/or in the current consent mechanism platform. We have limited our investigation to the scope of the complaints. As described below, the complaints addressed concerns regarding the previous consents in the app. The fact that some issues have fallen outside the scope of our investigation does not preclude those issues from being addressed in the future. Grindr must make sure that all processing of personal data on its users in the EEA is compliant with the GDPR at all times. We may decide to investigate additional issues later on, following individual complaints or *ex officio*, see the tasks and powers of the supervisory authorities laid down in Articles 57 and 58 GDPR.

The NO DPA is the supervisory authority established in line with Article 51(1) GDPR to monitor the application of the GDPR on the territory of the Kingdom of Norway. This follows from the Norwegian Personal Data Act Section 20.

3. Facts and background of the case

According to Grindr, the Grindr app is a GPS based social networking app designed to permit users to share information about themselves with other users in order to facilitate user interactions and connections. Grindr markets itself as the world's largest social networking app for gay, bi, trans and queer people.

In January 2020, the we received three complaints from The Norwegian Consumer Council ("the NCC") in collaboration with noyb — European Center for Digital Rights, on behalf of a complainant.

According to the complaints, Grindr lacked a legal basis for sharing personal data on its users with third party companies when providing advertising in its free version of the Grindr application ("app"). The NCC stated that Grindr shared such data through software development kits ("SDKs").

The complaints addressed concerns on the data sharing between Grindr and the following advertising partners (collectively referred to as "advertising partners" or "third party advertising partners"):

- Twitter Inc. ("Twitter's MoPub")
- Xandr Inc. ("Xandr", previously AppNexus Inc.)
- OpenX Software Ltd. ("OpenX")
- AdColony Inc. ("AdColony")
- Smaato Inc. ("Smaato")

According to its privacy policy, Grindr shares the following data with third party advertising companies:

> *[…] your hashed Device ID, your device's advertising identifier, a portion of your Profile Information, Location Information, and some of your demographic information with our advertising partners*[1]

In the same document, Grindr states that it shares the following personal data with its advertising partners:

> *Hardware and Software Information; Profile Information (excluding HIV Status and Last Tested Date and Tribe); Location and Distance Information; Cookies; Log Files and Other Tracking Technologies.*
> *Additional Personal Data we receive about you, including: Third-Party Tracking Technologies.*

In its report,[2] the NCC refers to the Grindr privacy policy which only names one such advertising partner, namely Twitter's MoPub. Twitter's MoPub lists 160 partners.

The NCC have concerns over Grindr's statement that it does "not control the use of these tracking technologies" while asking users to read the privacy policies of any third parties that may receive personal data. The NCC claims it is not clear how the user would be able to read the privacy policy of any other advertising partners, and that Grindr does not take adequate responsibility as a controller of any personal data collected and shared through its services.

According to the NCC, Grindr's processing does not meet the transparency requirement in the GDPR.

Grindr claims its consents were valid pursuant to the GDPR, and that its efforts to obtain consents exceeded industry standards already in 2017 and later on in 2018.

Grindr further argues controllers should not be held to the latest standard immediately upon the new standard's promulgation by legislators.

Grindr implemented a new Consent Management Platform ("CMP") 8 April 2020. Grindr began exploring new possibilities in June 2019, and selected OneTrust LLC in December–January to develop the new platform.

As mentioned, we have limited our investigations to the previous CMP. This consent mechanism used a two-layered approach. After first displaying the full privacy policy, the app asked the data subject if it wanted to "proceed". Data subjects were then asked to "opt-in" to processing activities by clicking "accept".

Grindr argues it was one of, if not the only, popular app that provided the full privacy policy within the app and that obtained specific, informed and unambiguous consents to its privacy

[1] Found on grindr.com/privacy-policy, last accessed 7 February 2020.
[2] *Out of control, How consumers are exploited by the online advertising industry,* 14 January 2020, p. 74.

practises in mid-2018. The industry standard at that time was to either (1) provide no disclosure of privacy practises, or (2) bundle a request to consent with consent to terms of use.

After surveying the top-rated free dating apps and "gay" dating apps identified in the Google Play Store, you found that Grindr was the only app that provided a full copy of the privacy notice prior to soliciting personal data. Although every app collected special category information, Grindr was the only surveyed app that asked for consent prior to the collection of any information.

Furthermore, Grindr maintains to be the only surveyed app that did not bundle consent to privacy policies with consent to contractual terms.

Finally, Grindr claims to be one of only a few of the surveyed apps that solicited affirmative consents from data subjects. While most apps indicated that processing was based on consent, they did not require data subjects to take any affirmative actions to demonstrate consent.

4. Relevant GDPR requirements

4.1. The principle of lawfulness, fairness and transparency

According to Article 5(1)(a), personal data must be processed "lawfully, fairly and in a transparent manner in relation to the data subject".

4.2. Consent pursuant to Article 6(1)(a)

Pursuant to Article 6(1), processing shall be lawful only if and to the extent that at least one of the requirements in (a) to (f) applies.

If the controller relies on Article 6(1)(a), *consent* is defined in Article 4(11) as

> *[…] any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*

Accordingly, Article 4(11) stipulates four requirements for a valid consent. It must be "freely given", "specific", "informed" and "unambiguous".

Article 7 and recitals 32, 33, 42 and 43 also outline how the controller must act to comply with the main elements of the consent requirements.[3]

In addition, The European Data Protection Board ("EDPB") has provided guidance with an analysis of the notion of consent in GDPR.[4]

[3] European Data Protection Board, *Guidelines 05/2020 on consent*, Version 1.1, adopted on 4 May 2020, para. 9.

[4] Ibid. para. 1.

"Freely given"
According to EDPB, the element "free" implies real choice and control for data subjects.[5]

EDPB's analysis shows that the criteria "freely given" contains four requirements: i) granularity, ii) data subject must be able to refuse or withdraw consent without detriment, iii) no conditionality, and iv) no imbalance of power.

i) Granularity

GDPR recital 32 highlights that

> *Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them.*

According to recital 43,

> *Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case,* […]

ii) Refusal or withdrawal of consent without detriment

According to recital 42,

> *Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.*

EDPB states the following in its guidelines:

> *For example, the controller needs to prove that withdrawing consent does not lead to any costs for the data subject and thus no clear disadvantage for those withdrawing consent.*[6]

EDPB further affirms that

> *If a controller is able to show that a service includes the possibility to withdraw consent without any negative consequences e.g. without the performance of the service being downgraded to the detriment of the user, this may serve to show that the consent was given freely. The GDPR does not preclude all incentives but the onus would be on*

[5] Ibid. para. 13.
[6] Ibid. para. 46.

the controller to demonstrate that consent was still freely given in all the circumstances.[7]

iii) Conditionality

Recital 43 states that

> *Consent is presumed not to be freely given […] if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.*

Article 7(4) GDPR constitutes that

> *When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.*

Article 7(4) seeks to ensure that the purpose of personal data processing is not disguised nor bundled with the provision of a contract of a service for which these personal data are not necessary.[8] The term "necessary for the performance of a contract" needs to be interpreted strictly.[9] The processing must be necessary to fulfil the contract with each individual data subject.[10]

Compulsion to agree with the use of personal data additional to what is strictly necessary limits data subject's choices and stands in the way of free consent.[11]

iv) Imbalance of power

Recital 43 highlights that consent should not provide a valid legal basis for processing in a specific case where there is a clear imbalance between the data subject and the controller.

In this regard, EDPB states:

> *As highlighted by the WP29 in several Opinions, consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences (e.g. substantial extra costs) if he/she*

[7] Ibid. para. 48.
[8] Ibid. para. 26.
[9] Article 29 Working Party, *Opinion 06/2014* and 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,* Version 2.0, 8 October 2019, Section 2.4.
[10] European Data Protection Board, *Guidelines 05/2020 on consent*, Version 1.1, adopted on 4 May 2020, para. 30.
[11] Ibid. para 27.

> *does not consent. Consent will not be free in cases where there is any element of compulsion, pressure or inability to exercise free will.*[12]

"Specific"
Article 6(1)(a) confirms that consent from a data subject must be given in relation to "one or more specific purposes" and that a data subject has a choice in relation to each of them. The requirement aims to ensure a degree of user control and transparency.[13]

According to guidance provided by EDPB, to comply with the element of "specific" the controller must apply:

i) *Purpose specification as a safeguard against function creep,*
ii) *Granularity in consent requests, and*
iii) *Clear separation of information related to obtaining consent for data processing activities from information about other matters.*[14]

"Informed"
According to guidelines provided by EDPB, the requirement for consents to be "informed" is reinforced through the GDPR and aims to provide user control. EDPB further states

> *Based on Article 5 of the GDPR, the requirement for transparency is one of the fundamental principles, closely related to the principles of fairness and lawfulness. Providing information to data subjects prior to obtaining their consent is essential in order to enable them to make informed decisions, understand what they are agreeing to, and for example exercise their right to withdraw their consent. If the controller does not provide accessible information, user control becomes illusory and consent will be an invalid basis for processing.*[15]

The guidelines further state:

> *Controllers cannot use long privacy policies that are difficult to understand or statements full of legal jargon. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form.*[16]

Article 7(2) GDPR also asserts how the controller should provide the information:

> *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. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.*

[12] Ibid. para. 24.
[13] Ibid. para. 55.
[14] See para. 55.
[15] Ibid. para. 62.
[16] Ibid. para. 67.

If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.[17]

"Unambiguous"
EDPB sets out guidance on the "unambiguous" criterion. For example, it must be obvious that the data subject has consented to the particular processing.[18]

EDPB further states:

> *A controller must also beware that consent cannot be obtained through the same motion as agreeing to a contract or accepting general terms and conditions of a service. Blanket acceptance of general terms and conditions cannot be seen as a clear affirmative action to consent to the use of personal data.*[19]

4.3. Processing special categories of personal data under Article 9

Processing of special categories of personal data needs additional legal basis in Article 9 GDPR.

Article 9 applies to

> *personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation[…]*..

Article 9(1) prohibits controllers from processing such data, unless the controller can demonstrate that the processing falls within one of the exemptions in Article 9(2). One of the exemptions applies if the data subject has given "explicit consent to the processing of those personal data for one or more specified purposes," pursuant to Article 9(2)(a).

5. Our assessment of the case

5.1. Whether Grindr's previous consent mechanism was compliant with Article 6

Grindr states its legal basis for sharing personal data to third party advertisers is consent pursuant to Article 6(1)(a).

[17] GDPR recital 32.
[18] Ibid. para. 75.
[19] Ibid. para. 81.

We agree that consent is the appropriate legal basis for assessment in this case. In its guidelines on Article 6(1)(b) in the context of digital services, the EDPB clarified that online behavioural advertising is generally not necessary for the performance of a contract with a data subject.[20] Furthermore, in the Article 29 Working Party profiling guidelines,[21] which have been endorsed by the EDPB, the Working Party Stated that

> *[…] it would be difficult for controllers to justify using legitimate interests as a lawful basis for intrusive profiling and tracking practices for marketing or advertising purposes, for example those that involve tracking individuals across multiple websites, locations, devices, services or data-brokering.*

As a rule, any extensive disclosure to third parties of personal data for marketing purposes should be based on the data subject's consent, as the other legal bases in Article 6(1) would not seem fit or adequate.

The Norwegian DPA shall assess whether the consents that Grindr collected for the disclosure of personal data to third party advertising partners in its *previous* CMP were compliant with Article 6(1)(a). We have not assessed Grindr's *current* CMP at this point, as this is beyond the scope of the complaint.

As mentioned, consents must meet several criteria according to the provisions explained above. In the following, we will assess the previous consents against these requirements.

5.1.1. Freely given

According to Article 4(11), consent must be "freely given". As mentioned, the GDPR recitals and guidance provided by EDPB give several clarifications as to when a consent is "freely given".

Granularity

Recital 43 states that a consent is presumably not given freely if it does not allow separate consents to be given to different personal data processing operations.

As Grindr argues, their previous consent mechanism displayed the full privacy policy, asking the data subject to "Proceed". When the data subject proceeded, Grindr asked if the data subject wanted to "Cancel" or "Accept" the processing activities.

Accordingly, Grindr's previous consents to sharing personal data with its advertising partners were bundled with acceptance of the privacy policy as a whole. The privacy policy contained all of the different processing operations, including processing necessary for providing services and products associated with a Grindr account.

---

[20] 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*, 8 October 2019, pp. 14–15.

[21] Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 6 February 2018, pp. 14–15.

Sharing personal data with advertising partners is a different processing operation than e.g. processing that is necessary for providing the main services in the app. The processing operations also serve different purposes.

Grindr's consent requests were bundled with other processing operations *and* other purposes.

The consent requirements aim to give data subjects control and equip them to make informed decisions. When bundling a consent to necessary processing with consent to sharing personal data with advertising partners, Grindr deprives data subjects of real control over their personal data.

Grindr has argued that it did not bundle consent with agreeing to terms of use.

In our view, the way Grindr bundled consent with the whole privacy policy does not differ significantly from bundling consent with terms of use. In both cases, the data subject is presented with a lot of information at once. The lack of granularity in this regard can "nudge" the data subjects to proceed without familiarizing themselves with the provided information, which also deprives them of real control.

For these reasons, we can establish that Grindr's previous consent mechanism did not allow for separate consents to be given to different purposes or processing operations. Therefore, Grindr's previous consents to sharing personal data with advertising partners were not given "freely".

Conditionality

The performance of a contract, including the provision of a service, cannot be dependent on consent to processing personal data if such processing is not strictly necessary for the performance of that contract.

As mentioned above, processing personal data for online behavioral marketing purposes cannot generally be considered necessary for the performance of the service.

The previous consent mechanism in the Grindr app displayed the full privacy policy, asking the user to "Accept" or "Cancel". It is our understanding that Grindr users who chose not to accept to behavioural advertising, would press "Cancel". By pressing "Cancel", the Grindr user would be excluded from the free version of the app, but could upgrade to the paid version.

Consequently, gaining access to the Grindr services within the *free version* of the app seemed dependent on consenting to sharing personal data for marketing purposes. This implies breach of the element of conditionality.

Grindr states that it provided data subjects with information on how it could "opt-out" on sharing data with advertising partners from its own device.

However, “opting-out” is not equivalent to a consent pursuant to GDPR. An “opt-out” solution would not meet the requirements for a valid consent. We discuss this further under the unambiguous section below.

In addition, the NCC stated “opting-out” through an Android device showed limited impact on data flow.

Grindr argues that the technical report provided by the NCC is misleading. When “opting-out” through an Android device, Grindr would either a) transmit a signal conveying the user’s “opt-out” preference, b) remove or obfuscate the user’s Advertising ID from its transmissions, or c) do both of the abovementioned.

However, in our view, providing data subjects with information on how they could “opt-out” on their own device is not in line with the principle of accountability in Article 5(2) GDPR. In the cases of Smaato, OpenX and AdColony, Grindr “only” transmitted a signal conveying the data subject’s “opt-out” preference. We understand that advertising partners could choose to ignore that signal. In any case, Grindr would have to rely on the action of others, either the user, the operating system, Grindr’s partners, or a combination of the aforementioned, to halt its sharing of data where so required. In consequence, Grindr failed to control and take responsibility for their own data sharing, and the “opt-out” mechanism is not necessarily effective.

Furthermore, for a consent to be “freely given”, accepting to the particular processing operation should be as easy as declining, and the choice should be intuitive and fair.

In our case, refusal of consent seemed a lot more difficult and time consuming compared to accepting. Accepting to personal data sharing for advertising purposes was only two clicks away, while declining required the data subject to take the time to read a long privacy policy, eventually gaining relevant information on how to “opt-out” on his or her own device, exiting the app and follow the instructions, then re-entering the app and click “Accept”. This method is dependent on the user’s patience and technological understanding, and it does not demonstrate a fair, intuitive and real choice.

For these reasons, we can establish that the provision of the Grindr services were dependent on consenting to processing operations that were not strictly necessary for the performance of the service. Therefore, Grindr’s previous consents were not given “freely”.

<u>Refusal or withdrawal of consent without detriment</u>
A valid consent must give data subjects the opportunity to refuse or withdraw consent without detriment.

In this regard, Grindr states that data subjects in their previous CMP could choose whether they wanted to consent, and that the new CMP assures no negative impact when declining.

Our discussion above on conditionality concludes that data subjects who did not consent to sharing personal data with advertising partners were excluded from the free version of the app. Consequently, the data subjects could not refuse to consent without detriment.

Grindr argues that refusal or withdrawal of consent had no negative consequences for data subjects, because they could choose to enrol in the Grindr paid app. The paid app does not include any third party advertising, and costs 155,00 NOK/month (Android) or 209,00 NOK/month (iOS).

However, in a footnote connected to a different paragraph, Grindr acknowledges that the option under the *previous* CMP, was upgrading to the paid version for a "nominal fee" of about one USD per day (approximately 9,00 NOK). This sums up to approximately 30 USD a month (approximately 270 NOK), and 360 USD a year (approximately 3 240 NOK).

According to EDPB guidelines, withdrawing consent must not lead to "any costs" for the data subject.[22] The same standard would presumably apply for refusal of consent. In this regard, it is important to have in mind that data subjects may face different financial circumstances, meaning that for some, even a small fee may be deterring. This could in turn unduly affect their decision as to whether to give, or to revoke, consent.

As refusal or withdrawing consent to sharing personal data with advertising partners would lead to extra costs for Grindr's users, Grindr's users could not refuse or withdraw consent without detriment.

Summary and conclusion

The argumentation above stipulates that consents in the previous platform were not "freely given".

Specifically, they were not sufficiently granular, access to services in the free version of the app was illegally made dependent on consenting to behavioral advertising, and data subjects could not refuse or withdraw consent without detriment.

When not complying with the requirement of "freely given", consents were not valid in accordance to Article 4(11), and Grindr shared personal data with its advertising partners without a legal basis in Article 6(1)(a).

The following assessment of compliance with the other requirements for a valid consent is additional to the one above.

5.1.2. Specific

As mentioned under Section 4, consents must be "specific" pursuant to Article 4(11) GDPR. The EDPB has stated that this requires purpose specification as a safeguard against function creep.[23]

[22] *Guidelines 05/2020,* Version 1.1., Adopted on 4 May 2020, para. 46 and 48.
[23] Ibid. para. 55.

Article 5(1)(b) GDPR sets forth the principle on purpose limitation. Personal data shall be collected for "specified, explicit and legitimate" purposes.

According to Grindr's privacy policy, the purpose in question is to "Share your Personal Data with our advertising partners".

A statement of purpose must say something about *why* the controller sees the need to process personal data. Grindr's statement of purpose describes a processing operation, and not the purpose behind the processing operation. The wording of the stated purpose is ambiguous, vague and general, in other words the purpose is not specified.

The EDPB has also stated that a controller who seeks consent for various different purposes should provide a separate "opt-in" for each purpose, to allow users to give specific consent for specific purposes, i.e. granularity in consent requests.[24] As discussed under Section 5.1.1, we have concluded that Grindr did not provide separate "opt-in" for each purpose.

In sum, Grindr has failed to comply with the principle on purpose limitation in Article 5(1)(b) and the requirement of "specific" consents in Article 4(11).

5.1.3. Informed

To comply with the requirement of "informed", the controller must provide information to data subjects prior to obtaining consent, so the data subjects can make informed decisions and understand what they are agreeing to. If the controller does not provide accessible information, user control becomes illusory and consent will be invalid.[25].

Article 5(1)(a) constitutes the basic principle of transparency. Personal data must be processed in a transparent manner in relation to the data subject.

In our view, the controller should at least provide information on what type of personal data are required for the particular processing, the specific purpose for the particular processing, i.e. behavioural advertising, and recipients of the personal data with information on who controls any further processing. It should also be clear how the data subject can withdraw consent and where it can find more information about the processing under Article 13.

Grindr's previous consent requests provided information on the controller, and the legal basis for the processing operation, as well as what type of personal data it processes.

However, the request for consent contained the full privacy policy. When presented in this form, information on sharing personal data with advertising partners was bundled with all other information regarding other processing operations for different purposes.

[24] Ibid. para. 55 and 60.
[25] Ibid. para. 62.

This approach makes it difficult for the data subject to filter and access key information. When requesting consents through a long privacy policy, data subjects may easily choose not to acquaint themselves with the information. As discussed above, the lack of granularity could "nudge" the data subjects to proceed without familiarizing themselves with the information.

This indicates that Grindr did not present the information in an easily accessible manner, nor was it distinguishable from other matters.

According to the guidelines provided by EDPB, informed consents should enable data subjects to make informed decisions, and understand what they are agreeing to.[26]

The NCC states that the complainant was "factually uninformed" about the fact that his personal data would be processed for advertisement and disclosed to third parties.

Grindr's privacy policy describes what type of personal data it shares with advertising partners. Grindr further informs that

> *These third parties may also collect information directly from you as described in this Privacy and Cookie Policy through tracking technologies such as cookies. The privacy policies of these third-party companies apply to their collection, use and disclosure of your Personal data. One of these advertising partners is MoPub that helps Grindr deliver personalized advertising. You can follow the links to MoPub's privacy notice and partner page.*

Accordingly, Grindr has disclosed personal data to third party advertising partners, who must be considered controllers for further processing.

The fact that third parties may process personal data further and that this will happen outside of Grindr's control is in our view crucial information to the data subject for it to make informed decisions and understand what it is agreeing to.

In our view, to be able to make informed decisions in the present case, the data subject must have easily accessible information on this fact. Grindr provided some of the information, but it was not easily accessible. This also indicates a lack of "informed" consent requests.

As described above, information that is relevant for the particular consent request should be highlighted in the request and not solely appear amongst all other information in a long privacy policy.

Therefore, we conclude that the data subjects were not equipped to make informed decisions and understand what they were agreeing to.

This means that Grindr did not comply with the requirement of "informed".

[26] Ibid. para. 62.

5.1.4. Unambiguous

Pursuant to Article 4(11), consent must be given by "a statement" or by "a clear affirmative action", signifying agreement to the processing of the data subject's personal data. A valid consent must be "unambiguous", meaning it must be obvious that the data subject has consented to the particular processing.[27]

As Grindr argues, data subjects made an affirmative action when consenting to their privacy practises. Data subjects could read the information about the processing activities, choose to proceed, and further to "Accept" the privacy policy or to "Cancel".

However, it did not seem clear to the data subject that pressing "Accept" to the whole privacy policy would include consent to behavioural advertising and sharing data with a wide range of advertising partners. This indicates that it was not obvious that the data subject consented to *the particular* processing.

Even if Grindr's previous approach exceeded industry practises, it seems clear that Grindr cannot demonstrate that data subjects consented to the *particular* processing under Article 7(1). Data subjects had to consent to the privacy policy in its entirety. As already stipulated, processing for advertising purposes is quite different from processing data necessary in order for the app to function.

On the requirement of unambiguousness, the EDPB also states that controllers cannot obtain consent through the same motion as agreeing to a contract or accepting general terms and conditions of a service.

Again, Grindr states that contradictory to industry practise, Grindr separated consents to its privacy practises from acceptance of general terms and conditions.

As discussed in Section 5.1.1, we cannot see how bundling consent to sharing of personal data with advertising partners with acceptance of all other privacy practises, differs from bundling consent with acceptance of general terms and conditions. In our view, this is inconsistent with the requirement of unambiguousness.

As mentioned under the section on "freely given", Grindr has argued that providing information on how to "opt-out" through data subjects' own device leads to "freely given" consents. However, we do not agree that "opting-out" is equivalent to a consent pursuant to the GDPR, as it does not meet the element of unambiguous as described above. "Opting-out" is not a clear affirmative action.[28]

[27] The requirement of unambiguous is constituted in Article 4(11) GDPR, and further explained in the EDPB guidelines pp. 18.

[28] The French supervisory authority (CNIL) has also concluded that "opt-out" mechanism was not a specific and unequivocal positive acceptance, see the *Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC, para. 158-161.*

In addition, clicking the "Accept" button in our present case would not necessarily signify an agreement, nor would it be unambiguous, as the data subject had to do so to use the app, and may still have wished to "opt-out" through the "opt-out" mechanism.

Therefore, Grindr failed to meet the criteria of soliciting "unambiguous" consents.

5.1.5. Concluding remarks

Based on our preliminary assessment above, we conclude that Grindr failed to comply with Article 6(1) when disclosing personal data of its users with third party advertisers.

5.2. Special categories of personal data under Article 9

5.2.1. Whether the processing falls within the scope of Article 9

The NCC claimed Grindr needed to fulfil one of the exceptions in Article 9(2) GDPR, because it shares a special category of personal data with its advertising partners. When Grindr shares personal data linked with the app name or the keywords "gay, bi, trans and queer" people, Grindr shares data on sexual orientation.

Grindr on the other hand, claims it does not share such data. Grindr claims keywords are not the equivalent of audience segmentation, but the general description of the app.

After studying the "mnemonic technical report" provided by the NCC, we agree that Grindr shares keywords on different sexual orientations, which are general and describes the app, not a specific data subject.

However, it is our understanding that the NCC claims that merely sharing information on a specific user alongside app name or the generic keywords qualifies as "data concerning a natural person's […] sexual orientation".

The NO DPA has to assess whether the fact that a data subject is a Grindr user qualifies as data "concerning" the user's "sexual orientation".

Grindr argues it does not "reveal" a particular data subject's sexual orientation within the scope of Article 9. A Grindr user could be homosexual, bisexual, transsexual or pansexual. A Grindr user could also be a heterosexual, but curious about other sexual orientations (often referred to as "bi-curious").

Article 9 connects the term "revealing" to "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership", while the term "concerning" is used in relation to "sexual orientation". According to Kuner's (et al.) commentary to the GDPR, Article 9 stipulates a broad definition of sensitive data.[29]

[29] Kuner, Bygrave and Docksey ed. (2020), *The EU General Data Protection Regulation (GDPR), A Commentary,* p. 374.

This indicates that contradictory to Grindr's argumentation, Article 9 does not require disclosure of the data subject's particular sexual orientation.

When Grindr discloses information on the data subject alongside the generic keywords "gay, bi, trans and queer", it indicates that the data subject belongs to a sexual minority, and to one of these particular sexual orientations.

Grindr markets itself as the biggest social networking app for "gay, bi, trans and queer" people. Consequently, when Grindr discloses information on the data subject alongside the fact that the data subject is a Grindr user, Grindr discloses information about the data subject and that he or she belongs to a sexual minority.

According to recital 51 GDPR,

> *Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms.*

This part of the recital expresses the fundamental objective behind Article 9, and the term "data concerning […] sexual orientation" should be interpreted in light of this purpose.

Discrimination against sexual minorities is unfortunately a fact in most countries, including Norway.[30]

Prejudice and discrimination is a breach of fundamental rights and freedoms, as established by the Convention for the Protection of Human Rights and Fundamental Freedoms[31] and The Constitution of the Kingdom of Norway.[32]

The fact that a data subject is a Grindr user may lead to prejudice and discrimination even without revealing their specific sexual orientation. Accordingly, spreading the information could put the data subject's fundamental rights and freedoms at risk.

Therefore, the purpose behind Article 9 also shows that Grindr has disclosed data "concerning" the data subject's "sexual orientation".

---

[30] The Norwegian Equality and Anti-Discrimination Ombud received 194 inquiries regarding discrimination against persons belonging to sexual minorities in the period of 2014-June 2017 (see the report *Seksuell orientering, kjønnsidentitet og kjønnsuttrykk, Ombudets fagoppsummering, Juni 2017,* p. 90). In 2019, the Norwegian Police Force received 122 police reports of hate crime because of sexual orientation (https://bufdir.no/Statistikk_og_analyse/lhbtiq/Hatkriminalitet_og_diskriminering/, last accessed 20 August 2020).

[31] Article 14 of the Convention prohibits discrimination on any ground. The European Court of Human Rights has found violations of Article 14 because of discriminatory treatment on the basis of sexual orientation (see for instance CASE OF E.B. v. FRANCE, 43546/02, and CASE OF X AND OTHERS v. AUSTRIA, 19010/07).

[32] Section 98.

Grindr argues in its response from 22 May 2020 that this would be contrary to the facts and create a far-reaching and unanticipated policy that would transform many different types of apps into processors of Article 9 special category data. Grindr further holds that it would affect a wide assortment of apps not necessarily thought of as handling special category data, giving several examples of different types of apps on pages 27-28.

We do not agree with Grindr's comparison and argumentation. Several of Grindr's examples show weaker indications of special categories of personal data.

The Grindr app on the other hand, explicitly targets data subjects belonging to a sexual minority through its marketing on its website, on the Apple App Store and on Google Play. The app's headline in the app stores is "Grindr – Gay Chat". The indication that the data subjects are "gay, bi, trans" or "queer" becomes clear.

The indication of the Grindr user's sexual orientation also becomes evident through several news articles about the Grindr app. Our own investigation shows that the app is regularly described a "gay" dating app.

An article by the Los Angeles Times published 2 July 2020 contains an interview with the new owners of Grindr, who bought the app company from its previous Chinese owners. In the interview, the new owners explain that 15 members of the senior team are part of the gay community, but they intend to recruit more members of the gay community so the business can hear from the real users of the site:

> *And we absolutely have the intention of recruiting more gay members of the community to every level of Grindr, from the lower levels to senior team to the board. I think it's important for the business to be able to hear from real users of the site, so that is a priority for us.*[33]

The interviewer then asks the new owners why they think they are the right people for the job of running "a gay dating company". The new owners answers the question without objection to the company description.

This indicates that by public perception, a Grindr user is presumably gay.

Based on the argumentation above, we conclude that the processing falls within the scope of Article 9. Consequently, Grindr should be able to demonstrate that one or more of the exceptions in Article 9(2) were applicable, in addition to having a legal basis in Article 6 for the disclosure of personal data linked with information about the app. Failing to do so, Grindr will have violated the prohibition laid down in Article 9.

[33] https://www.latimes.com/business/story/2020-07-02/grindr-new-ownership-american-investors-interview, last accessed 24 September 2020.

5.2.2. Whether the processing falls within the exceptions in Article 9(2)

Article 9(2)(a) provides that special category data can be processed where the data subject has given "explicit consent" to the processing of those personal data for one or more specified purposes.

The argumentation under Section 5.1 concludes that Grindr was in lack of valid consents under Article 6(1)(a).

As Article 9 requires consents as a legal basis for processing special categories of personal data to be explicit, we conclude that Grindr did not have valid consents under Article 9(2)(a).

Grindr states that any processing of special category of personal data would be legal in accordance with Article 9(2)(e), as processing relates to personal data which were "manifestly made public" by the data subject.

Grindr explains that anyone can download the free version of the app and gain access to the names of other Grindr users. This is an essential part of the Grindr services.

The word "manifestly" in Article 9(2)(e) implies a high threshold for relying on this exception.[34]

According to the commentary on GDPR, "making public"

> *should be construed to include publishing the data in the mass media, putting them on online social network platforms or similar actions.*[35]

The EDPB guidelines on targeting of social media users enlist five elements to help inform the assessment under Article 9(2)(e). A combination of these elements or other elements may need to be considered.[36]

Grindr is a social networking app. Its privacy policy informs its users that when creating a Grindr account, the data subject may choose to provide Grindr personal data for its "public" Grindr profile. Consequently, Grindr warns the data subjects that the information they explicitly share through their profile will be made public.

On the other hand, this information is not easily visible to the data subjects. The guidelines on targeting of social media users imply that there must be a clearer warning of the public nature of the information, for the information to be regarded as manifestly made public.[37]

---

[34] European Data Protection Board, *Guidelines 8/2020 on the targeting of social media users,* Version 1.0, Adopted on 2 September 2020, para. 120.

[35] Kuner, Bygrave, and Docksey ed. (2020) *The EU General Data Protection Regulation (GDPR), A Commentary,* p. 378.

[36] European Data Protection Board, *Guidelines 8/2020 on the targeting of social media users,* Version 1.0, Adopted on 2 September 2020, Section 8.2.

[37] Ibid. para. 120, element (iv).

In addition, the Grindr platform is intrinsically linked with the idea of creating intimate relations, or connecting with other users in the LGBTQ community. According to the guidelines on targeting of social media users, this indicates that the data has not been manifestly made public by the data subject.[38]

Furthermore, the data subjects choose their own nickname and whether they want to upload a profile image. Thus, it is possible to have an anonymous approach vis-à-vis other users in the app. In these instances, the data subject has not made their sexual orientation public. In any case, the users may trust that their profile will only be visible to other users, who are also presumably members of the LGBTQ community. That is something else than making the information public.

Although Grindr makes the data subject's profile available for other Grindr users, the free version of the app only displays a limited number of users at a time. Only users within a certain range from the user's actual or chosen location are visible to them. This also shows that a Grindr user who uploads a profile image may not necessarily have intended to make the information "public", but only available to a limited number of relevant users.

The guidelines on targeting of social media users also imply that the data has not been manifestly made public if creation of an account is necessary before accessing the information.[39]

At any rate, the data subject should not expect that Grindr would still share information on their sexual orientation with third party advertisers.

Article 9(2)(e) requires that the data have been "manifestly" made public. This requires an affirmative act by the data subject, and that they realized that public disclosure would be the result.[40]

Information about someone merely being a Grindr user may be a special category of personal data, but becoming a Grindr user is not an affirmative act by the data subject to make the information public. The data subjects do not publish the information on an open platform, which points to the direction that they have not manifestly made their sexual orientation public.[41]

Based on the argumentation above, we do not agree that Grindr would have fulfilled one of the exceptions in Article 9(2)(e).

[38] Ibid. para. 120, element (ii).
[39] Ibid. para. 120, element (iii).
[40] Kuner, Bygrave, and Docksey ed. (2020) *The EU General Data Protection Regulation (GDPR), A Commentary,* p. 378.
[41] See *Guidelines 8/2020 on the targeting of social media users,* para. 120, element (v).

Consequently, we have concluded that Grindr breached the prohibition in Article 9(1) when Grindr disclosed personal data linked with the app name or the keywords "gay, bi, trans and queer" to advertising partners.

5.3. Corrective measures

5.3.1. General principles when assessing administrative fines

An "administrative sanction" is a negative reaction that may be imposed by an administrative agency in response to an actual breach of a statute, regulation or individual decision, and which is deemed to be a criminal sanction pursuant to the European Convention on Human Rights.[42]

The Norwegian Supreme Court (Rt. 2012 p. 1556) has concluded that an administrative fine is a penalty under Article 6 in the Convention on Human Rights.

As a result, we can only impose a fine where there is clear and convincing evidence of breaches of GDPR.

Section 46 of the Norwegian Public Administration Act states the following regarding administrative sanctions against enterprises:

> *When a statute prescribes that administrative sanctions may be imposed against an enterprise, such sanction may be prescribed even if no individual person is at fault.*

5.3.2. Whether to impose an administrative fine

We have found that there is clear and convincing evidence that Grindr has breached Articles 6(1)(a) and 9. We deem it necessary to react to these breaches of the GDPR and therefore notify you that we are considering issuing an administrative fine.

When deciding whether to impose an administrative fine, the supervisory authority must take the factors listed in Article 83(2)(a)–(k) GDPR into consideration in each individual case. In the following, we will assess the case facts against these factors.

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them

Grindr has processed personal data illegally when it disclosed personal data about its users with a number of recipients. These recipients may have subsequently disclosed the data to other recipients. Grindr disclosed the data to Twitter MoPub's SDK, and Twitter MoPub lists more than 160 partners.[43] This means that over 160 partners could access personal data from

[42] Section 43 of the Norwegian Public Administration Act.
[43] The NCC report p. 74.

Grindr without a legal basis. We consider that the scope of the infringements adds to the gravity of them.

Furthermore, the data subjects did not initiate the particular processing operations in question. As discussed in Section 5.1, they presumably wanted to access the services provided in the app, and they did not necessarily intend to share their personal data to several third party advertisers. They were instead subject to Grindr's and third parties' commercial interests, with the potential of their personal data being disseminated, sold or further processed without a valid consent and without clear information about this further processing.

As discussed above, Grindr's given purpose of the data sharing in question did not uphold the requirements for purpose specification, and the lack of control over further processing caused a risk of incompatible use. The large scale data flow for tracking and profiling for providing behavioral advertisement could inter alia lead to manipulation of data subjects.[44] This also adds to the gravity of the infringements.[45]

Thus, the data subjects had limited or no control over the personal data flow through the SDK.

The number of data subjects affected are one of the relevant conditions when considering whether to impose an administrative fine. According to the EDPB's guidelines, the number of data subjects involved should be assessed, in order to identify whether this was an isolated event or symptomatic of a more systemic breach or lack of adequate routines in place.[46]

We do not consider the breach to be an isolated event, but something that affected all of the data subjects in Norway.

According to Grindr, approximately 13.7 million data subjects globally are active users of the app. An article from the BBC suggests Grindr had over 27 million users globally by 2017.[47] Grind explains in its letter of 22 May 2020 that the app has been downloaded over 12 million times globally since January 2020. Grindr states that users in Norway represent approximately 0.13% of downloads.

These figures show that the number of data subjects in Norway that were affected by the infringements is very high.

The type of data shared illegally also illustrates the gravity of the nature of the infringements. Special categories of personal data, such as data concerning sexual orientation, merit specific protection under the GDPR. Grindr received these data from data subjects who wanted to join a dating app or a social networking app, with the opportunity to connect with others in the LGBTQ community within close range. The further disclosure of the data without clear information and the data subjects' prior consent has breached the data subjects' trust and

[44] As described in the NCC report pp. 46-47.
[45] Article 29 Working Party, *WP 253, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679*, Adopted on 3 October 2017, pp. 10-11.
[46] Ibid. p. 10.
[47] https://www.bbc.com/news/business-45353789 (last accessed 23 September 2020).

violated their fundamental rights. Furthermore, misuse of data concerning sexual orientation could lead to discrimination against the data subject. Grindr also shared these data alongside the users' exact GPS location, which further adds to the gravity of the infringements.

We will also consider the duration of the infringements. The duration of an infringement may be illustrative of, for example, wilful conduct on the data controller's part, failure to take appropriate preventive measures, or inability to put in place the required technical and organisational measures.[48]

Grindr launched their new CMP in the EEA on 8 April 2020. By this time, Grindr had lacked a valid legal basis since the GDPR entered into force in Norway on 20 July 2018, which is almost two years. Although the GDPR entered into force in 2018, Grindr did not begin to explore alternatives to their previous CMP before June 2019. By this time, GDPR had been in force in Norway for almost a year.

According to the argumentation above, the nature, gravity and duration indicates several aggravating factors and points to the direction that an administrative fine is appropriate.

(b) the intentional or negligent character of the infringement

It seems clear that Grindr intended to use its previous consent mechanism and maintains that the consents were valid and in accordance with the GDPR. Our assessment shows that the consent mechanism clearly did not meet the applicable GDPR requirements. In our view, the inadequacy of the consent mechanism should have been clear to Grindr.

Furthermore, the in-app settings did not allow the user to proceed in the app without accepting the entire privacy policy, including the processing in question. This could indicate that Grindr intentionally made it impossible for the user to access the app without accepting behavioral advertising.

This indicates that the infringement were intentional.

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects

We consider that this factor is not relevant in the present case.

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32

We are not aware of any data protection measures taken by Grindr to secure the information shared with advertising partners. On the contrary, it seems that Grindr lacked control of the

[48] Article 29 Working Party, *WP 253, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679*, Adopted on 3 October 2017, p. 11.

data flow and recipients, as it shared personal data on its users through an SDK where Grindr has limited or no control over further processing.

The question that the supervisory authority must then answer is to what extent the controller "did what it could be expected to do" given the nature, the purposes or the size of the processing, seen in light of the obligations imposed on them by the GDPR.[49]

In our view, Grindr did not integrate appropriate measures through its in-app settings. More granularity and granular information in the consent mechanism would in particular contribute towards adherence to the GDPR requirements. Furthermore, Grindr collected a lot of personal data from a lot of users, including data concerning sexual orientation. The nature and size of the processing shows the importance of integrating necessary in-app settings to ensure that data were not shared with advertising partners without a valid consent.

This indicates that Grindr has not sufficiently taken responsibility pursuant to Articles 25 and 32.

(e) any relevant previous infringements by the controller or processor

We are not aware of any previous infringements.

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement

Grindr has cooperated with the NO DPA by providing information and answering our questions in its response to our order of providing us information. Therefore, we consider that this factor is not relevant in the present case.[50]

(g) the categories of personal data affected by the infringement

As discussed under (a), Grindr has disclosed special categories of personal data illegally to third party advertising partners. Data concerning sexual orientation merit special protection under the GDPR, as disclosure of such data could put the data subject's rights and freedoms at risk and cause grave harm. Combined with exact location data, Grindr puts the data subject at even greater risk.

Exact GPS position is in itself a category of data that should be processed with due consideration. The processing of a data subject's location information can be a highly intrusive act, depending on the circumstances. Combined with special categories or not, GPS location could put certain individuals at risk for different reasons, e.g. if they participate in an address confidentiality program.

[49] Ibid. p. 13.

[50] According to the guidelines in WP 253 p. 14, letter (f) could be a mitigating factor in some cases, however it would not be appropriate to give regard to cooperation that is already required by law.

Accordingly, we consider these factors as aggravating.

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement

We consider that this factor is not relevant in the present case.

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures

We are not aware of any previously corrected measures against Grindr with regard to the same subject matter.

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42

We consider that this factor is not relevant in the present case.

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement

Grindr argues that it should not be held to the latest standard immediately after promulgation by legislators.

The GDPR was already announced on 4 May 2016.[51]

The legal assessment of "freely given", inter alia the requirement of granularity and the opportunity to withdraw consent without detriment, has not evolved since the announcement of the regulation.

Accordingly, Grindr had two years to adapt to the GDPR requirements.

The EDPB Guidelines 05/2020 on consent, adopted on 4 May 2020, are just a revision of the Article 29 Working Party Guidelines on consent under Regulation 2016/679 (WP259), adopted for the first time on 28 November 2017 and subsequently revised and re-adopted on 10 April 2018. The EDPB Guidelines did not entail any changes relevant to our case, compared to the guidelines of the Article 29 Working Party. The rationale behind the EDPB's 2020 revision of the Article 29 Guidelines was to provide further guidance on so-called "cookie-walls" and scrolling, but the rest of the Article 29 Working Party Guidelines was left unchanged except from some editorial edits. [52]

[51] See the Official Journal of the European Unioin, L 119, Volume 59, 4 May 2016.
[52] See the preface in *Guidelines 05/2020 on consent*.

Even under the Directive (95/46/EC), consents had to be "freely given specific and informed", and collected for specified, explicit and legitimate purposes.

Consequently, Grindr has had enough time to comply with the consent requirements, and we do not consider Grindr's argument as mitigating.

Furthermore, the controller is responsible for, and must be able to demonstrate, compliance with the GDPR at any time, according to Articles 5(2) and 24.

Tech companies such as Grindr process personal data of data subjects on a large scale. The Grindr app collected personal data from thousands of data subjects in Norway, and it shared data on their sexual orientation. This enhances Grindr's responsibility to exercise processing with conscience and due knowledge of the requirements for the application of the legal basis on which it relies upon.

Grindr also refers to guidance on consent provided by the Irish supervisory authority (DPC) from April 2020,[53] where the DPC gives controllers six months to adapt before they start to take action against non-compliance.

The guidance provided by the DPC is not a binding document for other supervisory authorities. It should also be noted that neither the GDPR nor Norwegian law allows for grace periods. In addition, other supervisory authorities are enforcing the consent requirements. Most notably in this regard is the French supervisory authority (CNIL), which has imposed a € 50 000 000 fine on Google for relying upon invalid consents.[54]

Furthermore, the DPC issued the guidance on 20 April 2020, so it is not likely that this guidance has given Grindr any legitimate expectation of avoiding enforcement actions by supervisory authorities before it was issued.

As the GDPR entered into force in Norway on 20 July 2018, and the GDPR was already announced in April 2016, we do not consider Grindr's arguments as mitigating factors.[55]

We do find it aggravating that Grindr must have gained financial benefits from the infringements. Grindr users who did not want (or did not have the opportunity) to enroll in the paid version, had their personal data shared and re-shared with a potentially vast amount of advertisers without a legal basis, while Grindr and advertising partners presumably profited.

The argumentation above clearly shows that an administrative fine is proportionate in the present case.

---

[53] *Guidance Note: Cookies and other technologies.*

[54] https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc, last accessed 21 September 2020. CNIL also found that Google had violated the provisions in Articles 12 and 13.

[55] According to Article 99 GDPR, the regulation entered into force twenty days after its publication in the Official Journal of the European Union, and it became applicable from 25 May 2018.

5.3.3. Deciding the amount of the administrative fine

Article 83(1) provides the following guidance when deciding the amount of administrative fines:

> *Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.*

In accordance with Article 83(2), the NO DPA must also take due regard to the arguments in 5.3.2 above.

The argumentation above indicates several aggravating factors and suggests that a high amount is appropriate. The infringements found in the case qualifies for the maximum amount of administrative fines under Article 83(5). The maximum amount is 20 000 000 EUR or up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

As mentioned, the amount must be "effective, proportionate and dissuasive" in each individual case. We therefore find Grindr's annual revenue relevant in our assessment.

According to an article published 26 March 2020 on Forbes.com, The Financial Times found that during the first three months of 2019, Grindr's total revenue was 77.9 million USD (approximately 726 000 000 NOK).[56] This indicates an annual gross revenue at 312 million USD (approximately 2.8 billion NOK).

According to a second article published 7 July 2020, Grindr generated a *net profit* of about 31 million USD (approximately 278 463 700 NOK) in 2019, with reference to Kunlun Technology's annual report.[57] The same article quotes Grindr Chief Operating Officer from an interview the week before. He explains that Grindr is a company generating a revenue of well over 100 million USD (annually), and that the company is highly profitable and growing quickly.

Based on this, we can assume that Grindr's annual turnover for 2019 was at least 100 million USD (approximately 898 270 000 NOK).

In view of the foregoing, the amount of **100 000 000 NOK** seems effective, proportionate and dissuasive.

---

[56] https://www.forbes.com/sites/korihale/2020/03/26/grindrs-chinese-owner-sells-gay-dating-app-over-us-privacy-concerns-for-600-million/#7f250c73551c, last accessed 23 September 2020.
[57] https://in.reuters.com/article/us-health-coronavirus-ppp-grindr/grindr-dating-app-valued-at-620-million-cleared-for-small-business-loan-idUSKBN247308, last accessed 23 September 2020.

If the Covid-19 situation has affected you in a way that is relevant to our notified decision, please explain why and provide relevant documentation.

6. Process

If you have comments or remarks to this advance notification, you need to send them to us by **Monday 15 February 2021** at 12 noon Oslo time (CET). A final decision will then be taken.

7. Access to documents

Subject to the Norwegian Public Administration Act Section 18 and 19, you – as a party to this case – have the right to acquaint yourself with the documents in this case. As you have already been informed, correspondence with the NO DPA is subject to freedom of information requests under the Norwegian Freedom of Information Act.

Kind regards

Bjørn Erik Thon
Data Protection Commissioner

Jeanette Dyrkorn
Senior Legal Adviser

This letter has electronic approval and is therefore not signed

Copy to: FORBRUKERRÅDET, Gro Mette Moen
ADVOKATFIRMAET SCHJØDT AS, Eva Jarbekk Jarbekk