Datatilsynet

Chairman of the board on behalf of the board,
Grindr LLC
PO Box 69176
West Hollywood
CA 90069

Exempt from public disclosure:
Offl. § 13 jf. fvl. § 13 (1) nr. 2

Your reference	Our reference	Date
	20/02136-18	13.12.2021

Administrative fine - Grindr LLC

1. Introduction

We refer to the advance notification of an administrative fine against Grindr LLC (hereinafter "Grindr") of 24 January 2021 in case 20/02136, previously 20/00100, of the Norwegian Data Protection Authority (hereinafter "NO DPA", "we"). We also refer to the reply to the advance notification that the law firm Schjødt submitted to the NO DPA on behalf of Grindr on 8 March 2021.

2. Decision

Pursuant to Article 58(2)(i) GDPR, the Norwegian Data Protection Authority imposes an administrative fine against Grindr LLC of NOK 65 000 000 – sixty-five million – for

- *having disclosed personal data to advertising partners without a valid legal basis, which constitutes a violation of Article 6(1) GDPR*

  and

- *having disclosed special category personal data to advertising partners without a valid exemption from the prohibition set out in Article 9(1) GDPR*

3. Facts and background of the case

3.1. About Grindr LLC

Grindr LLC is a U.S. company founded in 2009. Grindr markets its mobile application (hereinafter "app" or "Grindr app") as the world's largest social networking app for gay, bi, trans and queer people.[1]

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 states that the app has approximately [redacted] million active users worldwide.[2]

The app has a version that may downloaded and used free of charge (hereinafter "free version"). Users can upgrade to the "XTRA" or "Unlimited" versions of the app, which include various premium features, for a paid subscription (hereinafter "paid version").

3.2. Complaints from the Norwegian Consumer Council

On 14 January 2020, the NO DPA received three complaints against Grindr from the Norwegian Consumer Council (hereinafter "NCC"), in collaboration with noyb – European Center for Digital Rights, submitted on behalf of a complainant.

The complaints addressed concerns regarding the data sharing between Grindr and the following advertising partners (collectively referred to as "advertising partners", together with any other advertising companies or advertisers Grindr shared personal data to for advertising purposes):

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

The complaints were accompanied by the NCC's own report "Out of control: How consumers are Exploited by the Online Advertising Industry", and a related technical report prepared by the company Mnemonic, which the NCC had commissioned (hereinafter "Mnemonic technical report").

The NCC's inquiry showed that Grindr shared ("disclose" and "share" will be used interchangeably throughout this decision to describe the same action) certain categories of personal data to several advertising partners, including advertising ID, IP address, GPS

[1] https://www.grindr.com/, last visited 7 December 2021.
[2] Grindr's response to the order to provide information, 22 May 2020, page 2.

location, gender, age, device information and app name.[3] The NCC stated that Grindr shared such data through software development kits ("SDKs") included in the Grindr app. According to the NCC, in the case of mobile advertising, SDKs are often provided in order to facilitate communication between the apps and the advertising vendors.[4]

Grindr's consent mechanism in use at the time of the NCC's inquiry (hereinafter "previous CMP") displayed the full privacy policy, asking the data subject to click on "Proceed". If the data subject clicked on "Proceed", a pop-up appeared with the phrase "I accept the Privacy Policy", where Grindr gave the data subject the option to press "Cancel" or "Accept". If the data subject pressed "Cancel", further registration was not possible, and the data subject would be unable to use the app.

According to the complaints, Grindr's consent mechanism infringed most of the requirements for valid consent in Articles 4(11), 6(1)(a), 7 and 9(2)(a) of the General Data Protection Regulation ("GDPR").[5] As a result, the NCC argued that Grindr lacked a legal basis for sharing personal data on its users with third party companies when providing advertising in the free version of the Grindr app. Furthermore, the NCC claimed that Grindr had infringed the prohibition set out in Article 9(1) of the GDPR by sharing data "concerning" a natural person's "sexual orientation".

3.3. The NO DPA's investigation

Based on the NCC's complaints and findings, on 24 February 2020, the NO DPA sent Grindr an order to provide information. Grindr asked for an extended deadline to reply to the order to provide information, and as per Grindr's request, the NO DPA extended Grindr's deadline from 25 March 2020 to 22 May 2020. Grindr submitted its response to the NO DPA on 22 May 2020.

In its response, Grindr stated that its legal basis for sharing data subjects' personal data with third party advertising partners for advertising purposes is consent. Grindr further argued that its previous CMP was in line with the GDPR and exceeded industry standards and practices at the time. However, Grindr stated that it started exploring a new consent management platform in June 2019 and eventually entered into contract with One Trust for the creation of a new consent management platform. Grindr deployed its new consent mechanism for data subjects in the European Economic Area ("EEA") on 8 April 2020 (hereinafter "current CMP" or "new CMP").

Grindr further stated that it does not share data on any particular data subject's sexual orientation, and that any keywords transmitted to advertisers like "gay", "bi" or "bi-curious"

[3] Mnemonic technical report, page 27-29.
[4] Ibid. page 16.
[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ [2016] L 119/1.

would only describe the Grindr app. Grindr held that the fact that a data subject is a Grindr app user is not indicative of that user's sexual orientation.

The information provided by Grindr did not mitigate our concerns regarding the lawfulness of Grindr's personal data sharing with advertising partners. Hence, on 24 January 2020, the NO DPA sent Grindr an advance notification of our intent to impose an administrative fine of NOK 100 000 000 against Grindr 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 set out in Article 9(1) GDPR.

The NO DPA received Grindr's reply to the advance notification on 8 March 2021. We will go through Grindr's arguments in more detail below, but Grindr's main legal arguments are:

- The principle of legal certainty (in Norwegian: "*legalitetsprinsippet*") under EEA law and Norwegian administrative law requires that in order to impose an administrative fine, there must be a clear legal basis and "objective, non-discriminatory criteria which are known in advance to the undertakings concerned". The requirements in Articles 6 and 9 GDPR, when applied to Grindr's previous consent mechanism, do not suffice as legal basis for imposing the notified administrative fine. Guidelines from the European Data Protection Board ("EDPB") cannot be the legal basis for administrative sanctions.
- Grindr obtained consent in line with the requirements of the GDPR.
- Grindr did not share users' sexual orientation with advertising partners.
- The NO DPA has not given adequate attention to the many measures taken by Grindr to fine-tune its mechanism for obtaining consent, and to the fact that Grindr began working on a new CMP in June 2019 and implemented it in April 2020.
- The size of the administrative fine indicated in the advance notification is not proportionate to the alleged breach, nor would a fine be effective in protecting the privacy of the users, as Grindr had already further enhanced its consent mechanisms. The advance notification sets out the largest GDPR-related fine throughout the EU/EEA relative to the alleged infringer's annual turnover. The proposed fine is neither proportionate nor justified by the asserted gravity, duration, scope, or nature of the alleged breach.

On 15 March 2021, the NO DPA received the NCC's comments on the NO DPA's advance notification. The NCC supported the conclusions and the notified intent of the NO DPA to impose an administrative fine, but also argued that Grindr had breached Articles 5(2), 13, 14, 24 and 25 of the GDPR.

The NO DPA sent another order to provide information to Grindr 29 April 2021, concerning Grindr's controllership and data protection relationships with Twitter's Mopub, Xandr, OpenX and AdColony. This order was also in relation to the complaints received against these advertising partners. Grindr asked for a deadline extension, and the deadline was extended from 19 May 2021 to 2 June 2021. Grindr submitted its response to the NO DPA on 2 June 2021.

In its response, Grindr stated that as regards to the processing operations subject to the NCCs complaint, it considers OpenX to be a processor for Grindr, and AdColony and Twitter's Mopub to be separate controllers. OpenX has also previously stated that they consider OpenX to be a processor for Grindr.[6] Grindr denied that it directly shared data with Xandr, but advised [redacted]

The NO DPA received further comments from the NCC on 6 October 2021 related to the data protection relationship between Grindr and its advertising partners. The NCC requested the NO DPA to determine which type of data protection relationship Grindr has with its some of its advertising partners, also in relation to the complaints filed against these companies.

The NO DPA sent Grindr a letter on 11 October 2021 in order to clarify a potential misunderstanding on Grindr's part related to advance notification of our intent to impose an administrative fine. The NO DPA clarified, as clearly set out in the advance notification, that our intent to impose an administrative fine against Grindr pertains to data subjects on Norwegian territory, and we have only take into consideration affected users in Norway in the context of calculating the notified administrative fine. We also informed Grindr of the comments we received from the NCC and provided copies of these. We gave Grindr until 1 November 2021 to provide any further comments or remarks to the advance notification.

Grindr once again asked for a deadline extension, and the deadline was extended from 1 November 2021 to 19 November 2021. Grindr submitted its comments to the NO DPA on 19 November 2021. In its comments, Grindr reiterated some of its main legal arguments from its reply to the advance notification on 8 March 2021. Grindr argued that it obtained lawful consents from its users, that it did not share personal data concerning users' sexual orientation, and that the size of the proposed fine in the advance notification is disproportionate.

[6] Letter from OpenX to the NO DPA dated 26 September 2020.

4. Relevant GDPR provisions

4.1. Material Scope

Article 2(1) GDPR provides that the Regulation applies to "the processing of personal data wholly or partly by automated means […]".

Article 4(1) GDPR defines "personal data" as:

> *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier.*

Article 4(2) GDPR defines "processing" as:

> *any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means […]*

4.2. Controller

Pursuant to Article 4(7) GDPR, "controller" means:

> *the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data* [...].

4.3. Territorial Scope

The Norwegian Personal Data Act incorporates the GDPR into Norwegian law. [7] The Personal Data Act and the GDPR entered into force in Norway on 20 July 2018.

Pursuant to Section 4 of the Norwegian Personal Data Act, the Act applies to the processing of personal data of data subjects in Norway conducted by controllers that are not established in the EEA, where the processing activities are related to (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in Norway; or (b) the monitoring of their behaviour as far as their behaviour takes place within Norway.

Article 3(2) GDPR provides that:

> *This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the*

[7] LOV-2018-06-15-38.

processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

4.4. The Supervisory Authority

Pursuant to Article 51(1) GDPR:

> *Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').*

The NO DPA (in Norwegian: "*Datatilsynet*") is the national GDPR supervisory authority in Norway, pursuant to Section 20 of the Norwegian Personal Data Act.

Article 55(1) GDPR regulates the supervisory authority's competence:

> *Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State*

Article 57(1) GDPR sets forth the tasks of the supervisory authority:

> *Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:*
>
> *(a) monitor and enforce the application of this Regulation;*
>
> [...]
>
> *(h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;*

Article 58(2) GDPR regulates the supervisory authority's corrective powers:

> *Each supervisory authority shall have all of the following corrective powers:*
>
> [...]

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

4.5. Principles relating to processing of personal data

According to Article 5(1) GDPR:

> *Personal data shall be:*
>
> *(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')*
>
> *(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes* [...] *('purpose limitation')*

Pursuant to Article 5(2) GDPR:

> *The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').*

4.6. Legal basis and valid consent

Pursuant to Article 6(1) GDPR:

> *Processing shall be lawful only if and to the extent that at least one of the following applies:*
>
> *(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;*
>
> *(b) processing is necessary for the performance of a contract to which the data subject is party* [...]*;*
>
> *(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*

Article 4(11) GDPR provides that:

'consent' of the data subject means 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.

Article 7 GDPR on the conditions for consent provides that:

1. *Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.*

2. *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.*

3. *The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.*

4. *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.*

4.7. Processing of special categories of data

Article 9(1) GDPR provides that:

Processing of 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 shall be prohibited.

Article 9(2) GDPR further provides that:

Paragraph 1 shall not apply if one of the following applies

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes [...]

(e) processing relates to personal data which are manifestly made public by the data subject;

4.8. General conditions for imposing administrative fines

Article 83 GDPR provides that:

1. *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.*

2. *Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:*

    (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;

    (b) the intentional or negligent character of the infringement;

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

    (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;

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

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

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

    (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;

(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;

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

(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.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

5. Our assessment of the case

5.1. Scope of the investigation of the NO DPA

We have limited our investigations to Grindr's previous CMP. The new CMP was deployed for data subjects in Norway as of 8 April 2020.

We have also limited our investigation to the time period following the entry into effect of the GDPR in Norway. As mentioned above in section 4.3, the GDPR entered into force in Norway on 20 July 2018.

Accordingly, our investigation is limited to the time period between 20 July 2018 and 7 April 2020.

As mentioned above in section 3.2, Grindr's consent mechanism consisted of a two-layered approach in this time period. First, the full privacy policy was displayed, asking the data subject to click on "Proceed". If the data subject proceeded, a pop-up appeared with the phrase "I accept the Privacy Policy", where Grindr gave the data subject to option to press "Cancel" or "Accept". If the data subject pressed "Cancel", further registration was not possible.

Although we have chosen to focus our investigation on the lawfulness of the previous CMP in the Grindr app, there might be additional issues in the previous and/or in the current consent mechanism platform. We have limited our investigation to the scope of the complaints, and the complaints addressed concerns regarding the lawfulness of the previous CMP in the app. The fact that potential issues have fallen outside the scope of our investigation does not preclude those issues from being investigated in the future.

5.2. The NO DPA's competence

According to Grindr's privacy policy, Grindr LLC, a U.S.-based company, is the controller for the processing of personal data regarding EEA data subjects.

The Grindr app monitors its users' behaviour, including movement and location, within Norway and the EEA. Therefore the Norwegian Data Protection Act and the GDPR applies to Grindr pursuant to the Norwegian Data Protection Act Section 4(2)(b) and Article 3(2)(b) GDPR respectively. Grindr also offers its services to data subjects in Norway and the EEA pursuant to the Norwegian Data Protection Act Section 4(2)(a) and Article 3(2)(a) GDPR respectively.

According to Grindr's response of 22 May 2020 to the NO DPAs order to provide information, Grindr does not have any offices or employees located in Norway or other EEA countries, and consequently it does not process personal data in the context of the activities of any European establishments. In line with Article 27 GDPR, Grindr have appointed a representative located in Ireland.

Based on this, we consider that Grindr does not have any establishments in the EEA. Consequently, there is no "main establishment" pursuant to Article 4(16) GDPR, and the processing of personal data in question does not qualify as "cross-border processing" pursuant to Article 4(23) GDPR. Therefore, the cooperation mechanism set out in Article 56(1) and Chapter VII Section 1 of the GDPR does not apply. For this reason, we are competent to perform our tasks under the GDPR in relation to the complaints in accordance with Article 55(1).

Please note that our competence in this case is limited to safeguarding the data protection rights of users within Norwegian territory. Therefore, this decision is without prejudice to the competence of GDPR supervisory authorities in other EEA territories.

5.3. Data controllership and the personal data processed

According to Grindr, the categories of personal data shared to advertising partners during the period of the alleged infringement were:[8]

[8] Grindr's response to the advance notification, 8 March 2021, page 15-16

- Advertising ID provided by the mobile operating system;
- IP address;
- Information about the computing environment (operating system version, model, screen resolution, etc.);
- Self-reported age (in whole years);
- Gender; and
- Location.

Grindr also disclosed the app name or app ID together with the above-mentioned data. This is further addressed in section 5.5.1 below.

Online identifiers are explicitly mentioned as an example of information relating to an identifiable natural person in Article 4(1) GDPR.

Moreover, recital 30 GDPR further elaborates on online identifiers as a type of personal data as follows:

> *Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.*

The information disclosed by Grindr to advertising partners constitutes "personal data" pursuant to Article 4(1) GDPR, as it could identify natural persons, directly or indirectly. This is further supported by the conclusion reached by Personvernnemnda (The Privacy Appeals Board) in the OpenX case.[9]

Disclosing personal data to advertising partners is a "processing" pursuant to article 4(2) GDPR, and Grindr is the "data controller" in relation to such processing pursuant to Article 4(7) GDPR, as it decided the means and purposes of the processing at hand.

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

5.4.1. Introduction

Processing of personal data is only lawful if the controller has a valid legal basis pursuant to Article 6(1) GDPR.

[9] PVN-2020-12.

As such, disclosing personal data to advertising partners who are not a processor for Grindr, requires a valid legal basis pursuant to Article 6(1) GDPR in order to be lawful.

Grindr states that its legal basis for sharing personal data to advertising partners for advertising purposes in the relevant time period was consent pursuant to Article 6(1)(a), and argues that their consent mechanism at the time was compliant with the GDPR.

We agree that consent is the appropriate legal basis for assessment in this case. For instance, 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.[10] Furthermore, in the Article 29 Working Party ("WP29") guidelines on automated decision-making and profiling,[11] which have been endorsed by the EDPB,[12] the WP29 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 advertising 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 in this context.

The NO DPA shall therefore assess whether the consents that Grindr collected for the disclosure of personal data to advertising partners for advertising purposes in its previous CMP were compliant with the requirements for consent under the GDPR.

As mentioned in section 4.6 above, consents must meet several cumulative requirements in order to be a valid under the GDPR. Article 4(11) stipulates four cumulative requirements for a valid consent. It must be "freely given", "specific", "informed" and "unambiguous". The validity of the consents that Grindr collected for the disclosure of personal data to advertising partners depends on whether such consents fulfilled all these requirements. Article 7 GDPR also outline how the controller must act to comply with the main elements of the consent requirements. These requirements should also be read in the light of recitals 32, 33, 42 and 43.

In the following, we will assess Grindr's collection of consents under the previous CMP against these requirements.

Guidance from the WP29/EDPB on consent

---

[10] EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, 8 October 2019, pp. 51-56.
[11] 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.
[12] EDPB Endorsement 1/2018.

The EDPB has provided guidance on the notion of consent under the GDPR. The EDPB Guidelines 05/2020 on consent, adopted on 4 May 2020, are just a revision of the WP29 Guidelines on consent under Regulation 2016/679 (WP259), adopted for the first time on 28 November 2017 and subsequently revised on 10 April 2018. These WP29 Guidelines were endorsed by the EDPB on 25 May 2018.[13]

The EDPB Guidelines in question did not entail any changes relevant to our case, compared to the guidelines of the WP29 of 2018. The rationale behind the EDPB's 2020 revision of the WP29 Guidelines was to provide further guidance on so-called "cookie-walls" and scrolling, but the rest of the Guidelines was left unchanged except for some editorial edits.[14] Thus, for the purpose of the present case, it should be stressed that the guidance on the notion of consent that was available at the time when Grindr's previous CMP was in use was essentially identical to the one issued by the EDPB in 2020.

It should be noted that the EDPB is an independent body of the Union established in accordance with Article 68 GDPR. Pursuant to Article 70(1)(e) GDPR, EDPB guidelines are issued for the purpose of encouraging a consistent application of the GDPR.[15] While such guidelines are not binding, they cannot be regarded as having no legal effect.[16] Indeed, the Court of Justice of the European Union (CJEU) has made clear that even non-binding instruments may produce legal effects, and should be taken into account as interpretative aids.[17] The CJEU has also directly cited Opinions from the EDPB in its judgements.[18] In particular, the adoption and application of EDPB guidelines is a key means for EEA supervisory authorities to fulfil their legal obligation to "contribute to the consistent application of [the GDPR] throughout the [EEA]".[19] Furthermore, the adoption of such non-binding instruments generates the legitimate expectation that the institutions that contributed to their devising will not depart from them without giving reasons that are compatible with the principle of equal treatment.[20] Thus, in essence, supervisory authorities are expected to follow EDPB guidelines when enforcing the GDPR in concrete cases.

---

[13] Ibid.
[14] See the preface to the *Guidelines 05/2020 on consent under Regulation 2016/679,* Version 1.1, Adopted 4 May 2020.
[15] See also recital 10 GDPR.
[16] For instance, this kind of guidelines are regularly used as interpretative aids by European courts, including the European Court of Human Rights ("ECtHR"). See e.g. e.g. ECtHR, Case of M.L. and W.W. v. Germany, App. Nos. 60798/10 and 65599/10, judgment of 28 June 2018, para. 63.
[17] Case C-322/88, Grimaldi v Fonds des maladies professionnelles, judgment of 13 December 1989, paras. 16-18; Case C-188/91, Deutsche Shell, judgment of 21 January 1993, para. 18.
[18] Case C-645/19, Facebook Ireland and others v Gegevensbeschermingsautoriteit, judgement of 15 June 2021, para. 74.
[19] Art. 51(2) GDPR.
[20] See, by analogy, Joined Cases C-189/02 P, C-202/02 P, C-205/02 P to C-208/02 P and C-213/02 P, Dansk Rørindustri and Others v Commission, judgment of 28 June 2005, para. 211; Case C-520/09 P, Arkema v Commission, judgment of 29 September 2011, para. 88.

However, contrary to Grindr's arguments, EDPB and WP29 guidelines are not the legal bases of our decision in the present case. The legal bases of our decision are exclusively the provisions of the GDPR. Guidance from the EDPB/WP29 has only has been used throughout this decision as an interpretive aid in our analysis of the requirements for a valid consent in the provisions of the GDPR. This is also to ensure that the NO DPA contributes to the uniform application of the GDPR across the EEA, and that our interpretation of the requirements for a valid consent under the GDPR is in line with the understanding of the other data protection authorities.

5.4.2. Freely given

The NO DPA shall first assess whether the consents that Grindr collected for the disclosure of personal data to advertising partners for behavioural advertisement purposes were "freely given" pursuant to Article 4(11) GDPR.

"Freely given" implies a genuine and free choice when deciding whether or not to give consent. This is confirmed by Recital 42, which states that consent should not be regarded as freely given if the data subject has no genuine or free choice. The CJEU has also found that as for the criterion of "freely given", the data subject must enjoy "genuine freedom of choice".[21] According to EDPB, the element "free" implies real choice and control for data subjects.[22] This requirement necessitates that the data subject enjoys a high degree of autonomy when deciding whether or not to give consent.[23]

Grindr argues that their previous CMP was compliant with the requirement in Article 4(11) GDPR for consent to be "freely given".

Article 7 GDPR and several GDPR recitals provide some clarifications as to when a consent may be considered to be "freely given", some of which are relevant in the present case, as outlined below.

<u>Not allowing for separate consents to be given to different personal data processing operations</u>

As established above, for a consent to be "freely given" pursuant to article 4(11), the data subject must have genuine freedom of choice.

Where the controller has several different purposes for processing personal data, and it does not allow for separate consents to be given, there is a lack of freedom and control for the data subject. If the data subject cannot identify and opt in to the processing purposes for which the data subject wishes to give his or her consent, and refuse consent to other processing purposes

[21] Case C-61/19, Orange Romania, judgement of 11 November 2020, para. 41.
[22] European Data Protection Board, *Guidelines 05/2020 on consent*, Version 1.1, adopted on 4 May 2020, para. 13, corresponding to Article 29 Working Party, *Guidelines on consent under Regulation 2016/679*, adopted on 10 April 2018, page 5.
[23] Kuner et al., *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020), p. 182.

for which the data subject does not agree with, there is no genuine free choice or control. The data subjects would find themselves in a "take it or leave it" situation, whereby they may feel forced to accept additional processing operations. In such cases, allowing for separate consents is appropriate, and in our view necessary to comply with Article 4(11) GDPR. In other words, consent should be granular.

This understanding of the requirement for a consent to be "freely given" is confirmed by recital 43 of the GDPR, which states that:

> *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 […]*

As Advocate General Szpunar stated in his Opinion in the *Planet49* case, "[t]he need for separate consent is […] stressed explicitly in this recital."[24] Recital 32 further states that consent should cover all processing activities carried out for the same purpose or purposes, and when processing has multiple purposes, consent should be given for all of them.

The EDPB guidelines on consent have elaborated on this point by stating that: "If the controller has conflated several purposes for processing and has not attempted to seek separate consent for each purpose, there is a lack of freedom. This granularity is closely related to the need of consent to be specific",[25] which is discussed below in section 5.4.3.

Grindr argues that "granularity" is not mentioned in the GDPR, and that this requirement is merely a result of the EDPB's own interpretation of the criteria for a valid consent. Therefore, Grindr argues that granularity is a recommendation, and not a legal requirement for a freely given consent.

EDPB guidelines are indeed non-binding, though as mentioned above, they are not without legal value and weight. They provide an expression of the administrative practises of EEA data protection authorities and their common understanding of the requirements of the GDPR.

However, "granularity", is merely a term used by the EDPB to clarify the meaning of the term "freely given" used in Article 4(11) GDPR, read also in the light of recital 43. As such, the relevant legal requirement does not stem from EDPB guidance as Grindr argues, but from the Article 4(11) GDPR. The term "granularity" is not new to EU/EEA data protection regime, as it was employed by the WP29 already back in 2011 under the previous regulation.[26]

---

[24] Opinion of Advocate General Szpunar, Case C-673/17, *Planet 49*, para. 75.
[25] EDPB, *Guidelines 05/2020 on consent*, Version 1.1, adopted on May 2020, para. 44, corresponding to Article 29 Working Party, *Guidelines on consent under Regulation 2016/679*, adopted on 10 April 2018, page 10.
[26] Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, adopted on 13 July 2011, p. 17-19.

Grindr further holds that under the GDPR, it is possible to obtain consent to a set of processing activities as long as the data subject receives information specific to each of the purposes of the data processing in advance. Grindr argues that Decision No 434684 of the French Council of State ("Conseil d'État") regarding the validity of the guidelines on cookies of the French data protection authority (CNIL) is a relevant court decision in this regard. Grindr has also referred to CNIL's current guidelines on cookies.[27]

The NO DPA's view is that Grindr's above-mentioned understanding is inaccurate, and we refer to the above-mentioned recital 43, which confirms our understanding that 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.

Our view is that the mentioned decision of The Council of State on the cookie-regulation in France has very limited relevance and weight for the present case. In any event, the court did not invalidate the part of CNIL's guidelines that stated that the data subject must be able to give his or her consent independently and specifically for each distinct purpose. The Council of State exclusively overturned the provision of the guidelines prohibiting in a general and absolute manner the practice of "cookie walls", ruling that such a prohibition could not be included in a soft law instrument.[28]

Furthermore, the CNIL guidelines on cookies is not a binding document for other supervisory authorities. In any event, the CNIL guidelines does not generally accept a practice where consent must be given for a set of processing purposes globally, but merely does not preclude the possibility of requesting the users to consent to a set of purposes. The EDPB guidelines however, which provides an expression of the administrative practises of EEA data protection authorities and the common understanding of the consent requirements of the GDPR that EEA supervisory authorities share, state that:

> *If the controller has conflated several purposes for processing and has not attempted to seek separate consent for each purpose, there is a lack of freedom.* [...] *When data processing is done in pursuit of several purposes, the solution to comply with the conditions for valid consent lies in granularity, i.e. the separation of these purposes and obtaining consent for each purpose.*[29]

Grindr's previous consent mechanism displayed the full privacy policy, asking the data subject to click on "Proceed". When the data subject clicked on "Proceed", a pop-up appeared with the phrase "I accept the Privacy Policy", where Grindr gave the data subject the option to

---

[27] Commission Nationale de l'Informatique et des Libertés, Délibération n° 2020-092 du 17 septembre 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux « cookies et autres traceurs »

[28] https://www.cnil.fr/en/cookies-and-other-tracking-devices-council-state-issues-its-decision-cnil-guidelines, last visited 7 December 2021.

[29] EDPB, *Guidelines 05/2020 on consent*, Version 1.1, adopted on 4 May 2020 para 44, corresponding to Article 29 Working Party Guidelines on consent under Regulation 2016/679, adopted on 10 April 2018, page 10.

press “Cancel” or “Accept”. By pressing “Cancel”, further registration was not possible, and the Grindr user would be excluded from using the app.

Accordingly, the consents to sharing personal data with its advertising partners that Grindr collected through the previous CMP 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 social networking services. To illustrate, Grindr’s privacy policy effective from 31 December 2019 listed 25 processing purposes with legal bases ranging from Article 6(1)(b), Article 6(1)(c), Article 6(1)(f) to consent in Article 6(1)(a).

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, and the processing operations serve distinctly different purposes.

Grindr’s consent requests for sharing personal data with advertising partners were bundled with requests for consent for other processing operations and other purposes, despite separate consents being appropriate and practical. The consent requirements aim to give data subjects control over their personal data and provide them with a genuinely free choice. However, in Grindr’s case, the data subject could not identify and opt in to the processing purposes for which the data subject really wanted to give his or her consent, and refuse consent to other processing purposes to which the data subject did not agree with. When bundling a consent to sharing personal data with advertising partners with acceptance of the full privacy policy including processing necessary to interact with other users, Grindr deprived data subjects of free choice and control over their personal data.

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

However, even though Grindr did not ask the data subject to accept the privacy policy and accept the terms of use through the same motion, this does not imply that Grindr allowed for separate consents to be given to different purposes or processing operations. As shown above, Grindr asked data subjects to accept the full privacy policy, and the privacy policy contained all of the different processing operations – including processing necessary for providing social networking services.

Furthermore, in our view, the way Grindr bundled consent to sharing personal data with advertising partners with acceptance of the privacy policy as a whole, does not significantly differ from bundling consent with terms of use in the context of lack of free choice and control for the data subject. In both cases, the data subject is presented with large amounts of information at once, and they are asked to accept all of it. The lack of granularity in this regard can also “nudge” the data subjects to proceed without familiarizing themselves with the provided information, which also deprives them of real control.

For the reasons discussed above, we can establish that Grindr’s previous consent mechanism did not allow for separate consents to be given to different purposes or processing operations despite it being appropriate, indicating that consent was not “freely given”.

Making the provision of the service conditional on consent to processing of personal data that is not necessary for the performance of the service

Article 7(4) GDPR provides 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.*

Recital 43 of the GDPR further 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.

The EDPB has held that 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.[30]

As stated above in section 5.4.1, processing personal data for online behavioural marketing purposes cannot generally be considered necessary for the performance of the service. The term "necessary for the performance of a contract" needs to be interpreted strictly.[31] The processing must be necessary to fulfil the contract with each individual data subject.[32]

The Grindr app is a LGBTQ+ social networking and dating service. On Google Play and App Store, the app is marketed as "Grindr – Gay chat", and described as follows:

> *"Grindr is the world's #1 FREE mobile social networking app for gay, bi, trans, and queer people to connect. Chat and meet up with interesting people for free, or upgrade to Grindr XTRA or Grindr Unlimited for more features, more fun, and more chances to connect."*

Users sign up to the Grindr app to connect with other members of the LGBTQ+ community, and this is the essence of the service from the perspective of the data subjects. Provision of behavioural advertisement is not an essential or objectively necessary part of the service, nor a reason why data subjects use Grindr's services. Grindr itself states that the app "would still work equally well" without behavioural advertisement.[33] Sharing Grindr users' personal data

---

[30] EDPB, *Guidelines 05/2020 on consent*, Version 1.1, adopted on 4 May 2020 para. 27, corresponding to Article 29 Working Party, *Guidelines on consent under Regulation 2016/679*, adopted on 10 April 2018, page 8.
[31] Article 29 Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* (WP217), page 16–17, and, EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects,* Version 2.0, 8 October 2019, Sections 2.4-2.5 (paras. 23-39)
[32] EDPB, *Guidelines 05/2020 on consent*, Version 1.1, adopted on 4 May 2020, para. 30, corresponding to Article 29 Working Party, *Guidelines on consent under Regulation 2016/679*, adopted on 10 April 2018, page 8.
[33] Grindr's response to the advance notification 8 March 2021, page 3 and 30

with advertising partners for online behavioural advertising purposes was not necessary for the performance of Grindr's services.

Grindr's previous consent mechanism displayed the full privacy policy, asking the data subject to click on "Proceed". When the data subject clicked on "Proceed", a pop-up appeared with the phrase "I accept the Privacy Policy", where Grindr gave the data subject to option to press "Cancel" or "Accept". Grindr users who chose not to accept behavioural advertising, would press "Cancel". By pressing "Cancel", further registration was not possible, and the Grindr user would be excluded from using the app.

Consequently, gaining access to the Grindr services within the free version of the app was made conditional on "consenting" to sharing personal data with advertising partners for advertising purposes which was not necessary for the performance of Grindr's services. This indicates that consent was not "freely given".

Grindr argues that it provided data subjects with information on how they could "opt-out" from data sharing with advertising partners on their own device. Grindr states that withdrawal of consent at the operating system level ensured that users could continue using the free version of the app with contextual ads served by advertising partners. As a result, Grindr argues that the free version of the app was not conditional on consent to sharing personal data for advertising purposes.

However, "opting-out" is not equivalent to a consent pursuant to the GDPR. An "opt-out" solution would not meet the requirements for a valid consent, as it would not be an "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", cf. Article 4(11) GDPR. We discuss this further under the section on unambiguous consent in 5.4.5 below.

Furthermore, the NCC stated "opting-out" through an Android device showed limited impact on the data flow.[34]

Grindr states that if a user would "opt-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.[35]

In our view, this mechanism is not in line with the principle of accountability in Article 5(2) GDPR. In the cases of Smaato, AdColony and others, Grindr "only" transmitted a signal conveying the data subject's "opt-out" preference together with the personal data.[36] We understand that advertising partners could potentially choose to ignore that signal. In any case, Grindr would have to rely on the action of others, either the user, the operating system,

[34] Mnemonic technical report, page 67-69.
[35] Grindr's reply to the order to provide information, 22 May 2020, page 21.
[36] Ibid, page 21.

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 was not necessarily effective.

In addition, for a user to opt out of interest-based ads on his or her device, the user would have to opt out from interest-based ads in general, and not just specifically for the Grindr app. This is something the user may not wish to do, further indicating lack of control and free choice for the data subject.

Article 7(3) states that it shall be as easy to withdraw as to give consent, and this requirement is further discussed in its own section in 5.4.6 below. In our view, for a consent to be "freely given", the same principle must apply to refusing consent. The choice should be intuitive and fair. By making it more difficult and time-consuming to refuse consent than to give consent, the controller "nudges" the data subject to consent to the processing operation even if they may not wish to, and it thus deprives the data subject of genuine freedom of choice.

This view has been endorsed by the CJEU in the *Orange Romania* case concerning the conditions that must be fulfilled in order for consent to be valid under both Article 2(h) DPD and Article 4(11) GDPR. The CJEU stated the following concerning the requirement for a consent to be "freely given":

> *Furthermore, as the Advocate General observed in point 60 of his Opinion, the free nature of that consent appears to be called into question by the fact that, if that consent is refused, Orange România, departing from the normal procedure for concluding the contract, required the customer concerned to declare in writing that he or she did not consent to a copy of his or her identity document being collected or stored. As the Commission observed at the hearing, such an additional requirement is liable to affect unduly the freedom to choose to object to that collection and storage, which it is also for the referring court to determine.*[37]

In point 60 of his Opinion in the same case, the Advocate General made reference to the *Planet49* case, and stated that:

> *[…] Turning once more to the judgment in Planet49, if unticking a pre-ticked checkbox on a website is considered too much a burden for a customer, then a fortiori a customer cannot reasonably be expected to refuse his or her consent in handwritten form.*[38]

We understand that Grindr could not take into account the *Orange Romania* judgement during the period of the infringement, as it was issued after the period in question. However, in the NO DPA's view, these statements from the CJEU only state requirements that could be directly derived from Article 4(11) GDPR, also read in light of recital 42 and 43.

---

[37] Case C-61/19, Orange Romania, judgement of 11 November 2020, para. 50.
[38] Opinion of Advocate General Szpunar, Case C-61/19, Orange Romania, para. 60.

In our case, consenting to personal data sharing for advertising purposes was two clicks away, while declining required the data subject to take the time to read a lengthy 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". Thus, refusal of consent was a lot more difficult and time consuming compared to accepting.

Moreover, if the data subject does not have clear information on the possibility of accessing a service even if he or she refuses to consent, choice becomes illusory. This has also been confirmed in the *Orange Romania* case, where the Court stated that:

> *[…] in order to ensure that the data subject enjoys genuine freedom of choice, the contractual terms must not mislead him or her as to the possibility of concluding the contract even if he or she refuses to consent to the processing of his or her data. Without information of that kind, the data subject's consent to the processing of his or her personal data cannot be regarded as having been given freely or, moreover, as having been given in an informed manner.*[39]

When presented with a full privacy policy, data subjects may easily choose not to acquaint themselves with the information. Consequently, the data subject would not read the information about Grindr's suggested "opt out" method, and they could easily get the impression that accepting the privacy policy and all the processing of personal data it describes was mandatory to access the service.

Moreover, even if the data subject did take the time to read the full privacy policy, the Privacy Policy in effect until 31 December 2019 was ambiguous as to the possibility of revoking consent and still access the Grindr app, which may also have had an impact on the data subject's understanding of the possibility to refuse consent:

> *Revocation Of Consent. The Grindr Services relies on the processing of Personal Data that you have provided. If you revoke your consent for the processing of Personal Data, in accordance with this Privacy Policy and applicable Terms and Conditions of Service, then you must discontinue all use of the Grindr Services and delete any accounts that you created, as we will no longer be able to provide the Grindr Services. In some cases, we may limit or deny your request if the law permits or requires us to do so, or if we are unable to adequately verify your identity.*

In sum, refusing consent under Grindr's previous CMP was dependent on the user's patience and technological understanding, and it did not demonstrate a fair, intuitive and genuine free choice.

Grindr further argues that users who pressed "Cancel" when asked to accept the Privacy policy, could upgrade to the paid version. Grindr holds that it offered its users a genuine

[39] Case C-61/19, Orange Romania, judgement of 11 November 2020, para. 41.

choice between the free version of the App, which required consent for the use of personal data for advertising purposes, and the paid version of the App.

However, as the NCC points out, at the time of registration the users were not given the choice to opt for the paid version of the app. The user would first have go through the above described consent mechanism and accept the privacy policy to access the app. It was only after this process that the user could decide to upgrade to the paid version. Access to the services was therefore conditional to consenting to sharing of data to advertising partners, and upgrading to the paid version would be an "opt-out" solution after "consent" was already given. As such, this method of opting out should be considered a form of withdrawal of "consent", and not a refusal. In any case, as discussed above, an "opt-out" solution would not meet the requirements for a valid consent, as it would not be an "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", cf. Article 4(11) GDPR.

Furthermore, the paid version of the app was marketed as a premium service with emphasis on added features like being able to view more profiles, advanced filters, chatting with users globally – in addition to no third party ads. However, it was not made clear by Grindr to data subjects that they could "opt-out" of sharing of data to advertising partners by upgrading to the paid version. This further indicates a lack of a fair, intuitive and genuine free choice.

Grindr further holds that offering a paid version of the service as an alternative to a free version conditional on consenting to sharing of personal data for advertising purposes is aligned with the EDPB guidelines on consent, and quotes the following paragraph of the guidelines in support of this claim:

> *The controller could argue that his organisation offers data subjects genuine choice if they were able to choose between a service that includes consenting to the use of personal data for additional purposes on the one hand, and an equivalent service offered by the same controller that does not involve consenting to data use for additional purposes on the other hand. As long as there is a possibility to have the contract performed or the contracted service delivered by this controller without consenting to the other or additional data use in question, this means there is no longer a conditional service. However, both services need to be genuinely equivalent.*[40]

Grindr further states that as set out by both EU institutions and by the NO DPA in a number of reports, legislative instruments and proposals, personal data may be used to pay for digital services.

[40] EDPB, *Guidelines 05/2020 on consent*, Version 1.1, adopted on 4 May 2020, para. 37, corresponding to Article 29 Working Party, *Guidelines on consent under Regulation 2016/679*, adopted on 10 April 2018, page 9.

However, the NO DPA has never endorsed the view that personal data may be used to pay for digital services. The quote Grindr uses from *The Great Data Race* is taken out of context and merely illustrates a potential claim that could be made at the time.[41] In fact, the very next sentence of the report following the quote Grindr uses states that this view cannot be said to have had a significant impact.[42]

Regarding EU institutions, recital 24 of directive 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services states that:

> *While fully recognising that the protection of personal data is a fundamental right and that therefore personal data cannot be considered as a commodity, this Directive should ensure that consumers are, in the context of such business models, entitled to contractual remedies.*

In its Opinion on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, the European Data Protection Supervisor (EDPS) stated that:

> *There might well be a market for personal data, just like there is, tragically, a market for live human organs, but that does not mean that we can or should give that market the blessing of legislation. One cannot monetise and subject a fundamental right to a simple commercial transaction, even if it is the individual concerned by the data who is a party to the transaction.*[43]

The EDPB has also stated that personal data cannot be considered as a tradeable commodity.[44] In regards to conditionality and freely given consent, the EDPB specifically states:

> *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. In doing so, the GDPR ensures that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract.*[45]

---

[41] Datatilsynet, *The Great Data Race. How commercial utilisation of personal data challenges privacy*, November 2015, page 31.
[42] Ibid. The quote in context reads: *It may be claimed that the use of various internet-based services – for example social media – represents a form of mutual contract in which the individual gains access to and can use the service in exchange for being exposed to advertising. As an extension of this, it may be argued that the processing of personal data in order to adapt the marketing to the individual is a necessary part of the contract. The individual then pays for the service indirectly with their personal data. This view cannot be said to have had a significant impact.*
[43] EDPS, *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, p. 17.
[44] EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, Version 2.0, 8 October 2019, para. 54.
[45] EDPB, *Guidelines 05/2020 on consent*, Version 1.1, adopted on 4 May 2020, para. 26, corresponding to Article 29 Working Party, *Guidelines on consent under Regulation 2016/679*, adopted on 10 April 2018, page 8.

As mentioned above, the paid version of the app was marketed as a premium service with emphasis on the added features like being able to view more profiles, advanced filters and chatting with users globally. Grindr acknowledges that at the time of the previous CMP, upgrading to the paid version cost about one USD per day (approximately 9,00 NOK).[46] This sums up to approximately 30 USD a month (approximately 270 NOK), and 360 USD a year (approximately 3 240 NOK). In our view, the paid version of the app could not be considered genuinely equivalent to the free version of the app.

For the reasons stated above, our conclusion is that the provision of the Grindr's services were conditional on consenting to processing operations that were not necessary for the performance of the service, indicating that consent was not "freely given".

Data subjects unable to refuse or withdraw consent without detriment

As established above, for a consent to be "freely given", the data subject must have genuine freedom of choice. If the data subject is unable to refuse or revoke consent without negative consequences and detriment, the choice is not genuine or free.

Recital 42 of the GDPR confirms this understanding, and states that consent should not be regarded as "freely given" if the data subject is unable to refuse or withdraw consent without detriment.

Grindr states that data subjects in their previous CMP could choose whether they wanted to consent.

However, the NO DPA has established above that the provision of Grindr's free version of the app was conditional on consenting to sharing of personal data to advertising partners for advertising purposes, and that requiring the data subject to "opt-out" on his or her device is not equivalent to a consent pursuant to GDPR. We have also established that how data subject would likely not have read the information about Grindr's suggested "opt out" method, and could easily get the impression that accepting the privacy policy and all the processing of personal data it describes was mandatory to access the service. If the data subject did not click "Accept" to the full privacy policy during registration, further registration was not possible, and the Grindr user would be excluded from the app. Consequently, the data subject was unable to refuse consent without detriment.

Grindr further 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, which Grindr holds is in line with EDPB guidance.

Firstly, as stated above, at the time of registration the users were not given the choice to opt for the paid version of the app. The user would first have to go through the above described consent mechanism and accept the privacy policy to access the app. It was only after this

[46] Response to the order to provide information, 22 May 2020, page 12-13 (footnote 18).

process that the user could decide to upgrade to the paid version. As a result, upgrading to the paid version was an "opt-out" solution and, if anything, must be regarded as a withdrawal of 'consent'. Consequently, the data subject could not refuse consent at the time consent was requested by enrolling to the paid version of the app.

Furthermore, contrary to what Grindr argues, according to EDPB guidelines withdrawing consent must not lead to "any costs" for the data subject.[47] The same standard would also presumably apply for refusal of consent, as there is no objectively jusified reasons to apply a different standard to refusing than withdrawing consent.

At the time of the previous CMP, upgrading to the paid version cost a fee of about one USD per day (approximately 9,00 NOK), which Grindr describes as a "nominal fee". This sums up to approximately 30 USD a month (approximately 270 NOK), and 360 USD a year (approximately 3 240 NOK).

In this regard, it is important to bear in mind that data subjects may face different financial circumstances, meaning that for some, this fee may be substantial and thus deterring. This could in turn unduly affect their decision as to whether to give, or to revoke, consent. In our view, the price of the paid version of the app constitutes detriment for the data subject.

For these reasons, Grindr's users could not refuse or withdraw consent without detriment, indicating that consent was not "freely given".

Summary and conclusion

In the proceeding sections we have illustrated why, in our view, Grindr's previous CMP for the disclosure of personal data to advertising partners did not offer data subjects a genuine free choice.

As we have established above:

- Grindr did not allow separate consents to different personal data processing operations despite it being appropriate;
- Access to services in the free version of the app was made conditional on consenting to Grindr sharing personal data with advertising partners despite this not being necessary for the performance of the service; and
- Data subjects could not refuse or withdraw consent without detriment.

For these reasons, consents collected through the previous CMP for the disclosure of personal data to advertising partners were not "freely given".

[47] EDPB, *Guidelines 05/2020 on consent*, Version 1.1, adopted on 4 May 2020, paras. 46 and 48, corresponding to Article 29 Working Party, *Guidelines on consent under Regulation 2016/679*, adopted on 10 April 2018, page 10-11.

The requirements for a valid consent in Article 4(11) are cumulative. When Grindr did not comply with the requirement of "freely given", the consents collected through the previous CMP for the disclosure of personal data to advertising partners for advertising purposes were not valid. As a result, Grindr disclosed personal data to its advertising partners without a valid 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.

5.4.3. Specific

The NO DPA shall assess whether the consents that Grindr collected for the disclosure of personal data to advertising partners in its previous CMP were compliant with requirement of "specific" in Article 4(11) GDPR.

Grindr has argued that it obtained consent to its processing separate and apart from other matters, as it was separate from accepting the terms of use.

Article 6(1)(a) provides that consent from a data subject must be given in relation to "one or more specific purposes".

The requirement for a consent to be "specific" must be viewed in conjunction with Article 5(1)(b) GDPR, which sets forth the principle of purpose limitation. According to Article 5(1)(b) GDPR, personal data shall be collected for "specified, explicit and legitimate" purposes.

The CJEU tackled the requirement of "specific" in the *Planet49* judgement of 1 October 2019, where the CJEU stated that:

> *It should be added that the indication of the data subject's wishes referred to in Article 2(h) of Directive 95/46 must, inter alia, be 'specific' in the sense that it must relate specifically to the processing of the data in question and cannot be inferred from an indication of the data subject's wishes for other purposes.*
>
> [...] *A fortiori, the preceding interpretation applies in the light of Regulation 2016/679.*[48]

In our view, the requirement for a consent to be "specific" entails that the consent request for a specific processing purpose must not only be separate from accepting terms of use, but must also be separate from indications of wishes concerning other data processing purposes.

[48] CJEU, C-673/17, Planet49, judgement of 1 October 2019, paras. 58 and 60.

The EDPB has also stated that consent mechanisms must not only be granular to meet the requirement of "free", but also to meet the element of "specific".[49] This means that a controller that 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. As discussed above in section 5.4.2, we have concluded that Grindr did not provide separate "opt-in" for each purpose.

Grindr's previous consent mechanism displayed the full privacy policy, asking the data subject to click on "Proceed". When the data subject proceeded, a pop-up appeared with the phrase "I accept the Privacy Policy", where Grindr gave the data subject the option to press "Cancel" or "Accept".

Accordingly, Grindr's previous consents to sharing personal data with its advertising partners were bundled with acceptance of the privacy policy as a whole, which should contain all the information Grindr was required to provide pursuant to Article 12-14 GDPR.

As a result, Grindr's consent mechanism was not 'specific' in the sense that it related to specifically to the sharing of personal data for advertising purposes. The consent was instead inferred from an indication of the data subject's wishes for all of the different processing operations and purposes described in the privacy policy, including processing necessary for providing social networking services. To further illustrate this point, the NO DPA recalls that Grindr's privacy policy effective from 31 December 2019 listed 25 processing purposes. The consents Grindr collected for sharing of personal data for advertising purposes were not distinguishable from indications of wishes from the data subjects on other data processing purposes.

For these reasons, Grindr has failed to comply with the requirement of "specific" consents in Article 4(11).

5.4.4. Informed

The NO DPA shall assess whether the consents that Grindr collected for the disclosure of personal data to advertising partners for advertising purposes through its previous CMP were compliant with requirement of "informed" in Article 4(11).

"Informed" implies that the data subject must receive prior information to enable them to understand the data processing they are asked to consent to and make an informed decision.

The requirement of "informed" consent must be viewed in conjunction with Article 5(1)(a), which constitutes the basic principle of transparency. This principle is also closely related to

[49] EDPB, *Guidelines 05/2020 on consent*, Version 1.1, adopted on 4 May 2020, para. 60, corresponding to Article 29 Working Party, *Guidelines on consent under Regulation 2016/679*, adopted on 10 April 2018, page 12.

the principle of fairness. Personal data must be processed fairly and in a transparent manner in relation to the data subject.

Article 7(2) provides that "[i]f 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."

Recital 42 of the GDPR further states that in order for consent to be "informed", it should be presented in "an intelligible and easily accessible form", and the data subject should "be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended."

It is clear from the words "at least" that this list is not exhaustive. This interpretation has been supported by the CJEU in *Orange Romania* through the use of "inter alia" in the following statement:

> *As regards the requirement arising from Article 2(h) of Directive 95/46 and Article 4(11) of Regulation 2016/679 that consent must be 'informed', that requirement implies, in accordance with Article 10 of that directive, read in the light of recital 38 thereof, and with Article 13 of that regulation, read in the light of recital 42 thereof, that the controller is to provide the data subject with information relating to all the circumstances surrounding the data processing, in an intelligible and easily accessible form, using clear and plain language, allowing the data subject to be aware of, inter alia, the type of data to be processed, the identity of the controller, the period and procedures for that processing and the purposes of the processing.* [50]

The CJEU goes on to state:

> *Such information must enable the data subject to be able to determine easily the consequences of any consent he or she might give and ensure that the consent given is well informed* [...].[51]

In light of the principles of transparency and fairness, for a consent to be informed, the controller must ensure that the data subject is able to easily determine the consequences of the consent they might give.

The EDPB has also stated that to comply with the requirement of "informed", the controller must provide information to data subjects prior to obtaining consent, so the data subjects can

[50] Case C-61/19, Orange Romania, judgement of 11 November 2020, para 40.
[51] Ibid, para. 40.

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.[52]

What information the controller must provide to enable the data subject to be able to determine the consequences of any consent they might give and ensure that the consent given is well informed, will in our view depend on the nature of the processing.

As held also by the EDPB[53], our view is that when personal data is disclosed to other controllers, the controller should at least provide information on recipients of the personal data with information on who controls any further processing. Pursuant to Article 7(3) it should also be clear how the data subject can withdraw consent, and where it can find more information about the processing under Article 13-14.

The EDPB further refers to Article 7(2) GDPR and states that:

> *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. This requirement essentially means that information relevant for making informed decisions on whether or not to consent may not be hidden in general terms and conditions.*[54]

As Grindr argues, its previous consent requests provided information on the controller, and the legal basis for the processing operation and 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 the other information regarding the other processing operations for different purposes.

This approach makes it difficult for the data subject to filter and access key information. The privacy policy effective before 31 December 2019 contained 3 793 words, and the privacy policy effective from 31 December 2019 contained even more. This information would take a substantial amount of time for the data subject to read. When requesting "consent" through a long privacy policy, data subjects may end up in a situation where they do not acquaint themselves with the information. In this likely scenario, the data subject would not even acquire information on what data processing they are consenting to, in this case Grindr sharing personal data with advertising partners. As a result, consent would not be an informed decision, and user control would be illusory.

---

[52] EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679,* Version 1.1., Adopted on 4 May 2020, para. 62, corresponding to Article 29 Working Party*, Guidelines on consent under Regulation 2016/679*, adopted on 10 April 2018, page 13.

[53] EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679,* Version 1.1., Adopted on 4 May 2020, paras. 64-65, corresponding to Article 29 Working Party, *Guidelines on consent under Regulation 2016/679*, adopted on 10 April 2018, page 13.

[54] EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679,* Version 1.1., Adopted on 4 May 2020, paras. 66-67, corresponding to Article 29 Working Party, *Guidelines on consent under Regulation 2016/679*, adopted on 10 April 2018, page 14.

The information Grindr provided on the processing in question was not distinguishable from other matters. Our view is that the way Grindr bundled consent with the whole privacy policy does not differ significantly from bundling consent with terms of use in the context of enabling data subjects to make informed decisions and understand what they are agreeing to.

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. Grindr did not present the information in an easily accessible form, and it did not enable the data subject to be able to easily determine the consequences of any consent they might give. We conclude that Grindr did not ensure that the consent given was informed.

In addition, even if the data subject took the time to read the Grindr's full privacy policy, both the privacy policy in effect before 31 December 2019 and the privacy policy in effect from 31 December 2019 merely stated the following regarding sharing of personal data with advertising partners:

> *Third Party Advertising Companies. We share your hashed Device ID, your device's advertising identifier, a portion of your Profile Information, Distance Information, and some of your demographic information with our advertising partners. These third parties may also collect information directly from you as described in this Privacy Policy through technology such as cookies. The privacy policy of these third party companies applies to their collection, use and disclosure of your information. 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.*

Except for the example of Twitter's MoPub, there was no information available for the data subject on which recipients or the number of recipients the personal data was disclosed to for the purpose of targeted advertisement. Grindr disclosed personal data to multiple advertising partners, who would further share the personal data with third or fourth parties within different ad networks, including advertisers and other participants of the adtech ecosystem. The adtech and real time bidding ecosystems are complex for data subjects to understand, and scope of data sharing was not transparent to the data subject. Without further accessible information on the scope of the data sharing, Grindr did not enable the data subject to be able to easily determine the consequences of any consent they might give. As a result, the consents were not informed.

Grindr did not comply with the requirement of "informed".

5.4.5. Unambiguous

The Norwegian DPA shall assess whether the consents that Grindr collected for the disclosure of personal data to advertising partners through its previous CMP were compliant with the requirement of "unambiguous" in Article 4(11).

Pursuant to Article 4(11), consent must be given by an "unambiguous indication of the data subjects wishes" by which he or she, by "a statement" or by "a clear affirmative action", "signifying agreement to the processing" of the data subject's personal data.

Recital 42 further states, "[w]here processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given."

As supported by the EDPB, for the consent to be "unambiguous", it must be obvious that the data subject has consented to the particular processing.[55]

Grindr argues that data subjects made an affirmative action when consenting to their privacy practises. Data subjects could read the information about the processing activities in the full privacy policy, 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 phrase "I accept the Privacy Policy" entailed consenting sharing data with advertising partners for behavioural advertisement. An acceptance of a privacy policy can also entail an acknowledgement of the fact that information has been provided. It was not clear from the wording or the context of the request that the data subject was asked to provide a consent nor that the acceptance of the privacy policy would have the legal consequences of giving a consent. Furthermore, as established above in 5.4.4, when presenting the data subject with the full privacy policy, one does not even know if the information about the processing in question was read and digested, and the data subject cannot be required to proactively read all privacy policies just in case a request for consent is hidden within them. In other words, it was not obvious that the data subject consented to the particular processing, and the situation was not unambiguous.

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 5.4.2-5.4.4, we cannot see how bundling consent to sharing of personal data with advertising partners, with the acceptance of all other privacy practises described in a full privacy practice, differs significantly from bundling consent with acceptance of general terms and conditions. This also applies in the context of whether it was obvious that the data subject has consented to the particular processing, and whether the consent was unambiguous.

---

[55] EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679,* Version 1.1., Adopted on 4 May 2020, para. 75, corresponding to Article 29 Working Party, *Guidelines on consent under Regulation 2016/679*, adopted on 10 April 2018, page 15.

Even if Grindr argues it'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 accept 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's social networking features to function.

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 giving data subjects the option to "opt-out" is equivalent to a consent pursuant to the GDPR, as it does not meet the element of unambiguous as described above. The data subject not "opting-out" is not a clear affirmative action, cf. Article 4(11). Recital 32 describes that "[s]ilence, pre-ticked boxes or inactivity should not therefore constitute consent."

This has also been confirmed by the CJEU. In the *Planet49* case, the CJEU stated that "only active behaviour on the part of the data subject with a view to giving his or her consent may fulfil that requirement."[56] Furthermore, as stated in the *Orange România* case, data controllers "cannot require [data subjects] actively to express their refusal."[57]

For these reasons, Grindr failed to meet the criteria of soliciting "unambiguous" consents.

5.4.6. Withdrawal of consent shall be as easy as to give consent

Article 7(3) concerning conditions for consent provide that "[i]t shall be as easy to withdraw as to give consent".

The requirement of being able to withdraw consent as easily as giving consent, is a condition and a necessary aspect of valid consent in the GDPR. This is also held by the EDPB.[58] If the withdrawal right does not meet the GDPR requirements in Article 7(3), then the consent mechanism of the controller does not comply with the GDPR.

Grindr has argued that users could opt out of behavioural advertisement on their device, or upgrade to the paid version of the app. The NO DPA have in section 5.4.2 above established several issues with these opt out mechanisms.

Irrespective of this, NO DPA shall assess whether it was "as easy to withdraw as to give consent" to sharing personal data to advertising partners in Grindr's previous CMP, cf. Article 7(3) GDPR.

---

[56] CJEU, Case C-673/17, Planet49, judgement of 1 October 2019, para. 54.
[57] CJEU, Case C-61/19, Orange Romania, judgement of 11 November 2020, para 51
[58] EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679,* Version 1.1., Adopted on 4 May 2020, para. 116, corresponding to Article 29 Working Party, *Guidelines on consent under Regulation 2016/679*, adopted on 10 April 2018, page 22.

In the previous CMP consenting to personal data sharing for advertising purposes was two clicks away. Withdrawing "consent" 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, and going through the required steps of opting out in their device settings. This method of withdrawal of consent was a lot more difficult and time consuming compared to giving 'consent'.

The only other options to effectively withdraw "consent" was limited to the data subject deleting his or her Grindr account, or going through the necessary steps to upgrade to the paid version of the app. Neither of these options could be considered as easy as giving "consent", which as mentioned was two clicks away.

We conclude that withdrawing "consent" to sharing personal data to advertising partners in Grindr's previous CMP was not as easy as giving consent. As a result, Grindr has failed to meet the requirement in Article 7(3) GDPR.

5.4.7. Concluding remarks

The requirements for a valid consent in Article 6(1)(a), Article 4(11) and Article 7(3) are cumulative, and failing to meet one of these requirements, the consents collected are not valid pursuant to the GDPR.

As we have concluded above, Grindr failed to fulfil the requirements of "freely given", "specific", "informed", "unambiguous" and "as easy to withdraw as to give consent", cf. Article 4(11) and Article 7 when collecting consents for sharing personal data to advertising partners in the previous CMP.

Grindr's consents collected in the previous CMP for the disclosure of personal data to advertising partners for advertising purposes were not valid.

As a result, Grindr disclosed personal data to advertising partners without a valid legal basis in Article 6(1) GDPR.

5.5. Special categories of data under Article 9

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

Article 9(1) GDPR prohibits processing of personal data "concerning a natural person's sex life or sexual orientation", but this prohibition does not apply if one of the exemptions in Article 9(2) applies to the processing.

Consequently, in order to lawfully process special categories of data, the controller must fulfil one of the exemptions in Article 9(2), in addition to having a valid legal basis pursuant to Article 6(1).

As established in section 5.4 above, the consents collected in the previous CMP for the disclosure of personal data to advertising partners for advertising purposes were not valid. Thus, Grindr disclosed personal data to advertising partners without a valid legal basis in Article 6(1) GDPR.

As a result, Grindr's sharing of personal data to advertising partners, including any special categories of data, was unlawful irrespective of Article 9.

However, the NO DPA shall still assess whether Grindr failed to comply with Article 9 GDPR, as this would constitute an additional violation of the GDPR.

The NCC argues that Grindr needed to fulfil one of the exceptions in Article 9(2) GDPR in addition to a legal basis under article 6(1) GDPR, because it shared a special category of personal data with its advertising partners. When Grindr shared personal data linked with the app name or app identifier, keywords like "gay", "bi" and "bi-curious", or all of the aforementioned, the NCC argues Grindr shared data on the data subject's sex life or sexual orientation.

Grindr on the other hand, claims it did not share data concerning a user's sexual orientation, and holds that the fact that a data subject is a Grindr user does not qualify as data "concerning" a natural person's "sexual orientation". Grindr further claims the keywords are not the equivalent of audience segmentation, but a general description of the app.

After studying the "Mnemonic technical report" provided by the NCC, we agree that Grindr shares information on a data subject being a Grindr user, and that any keywords shared on different sexual orientations 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 ID, the generic keywords describing the app, or both, qualifies as "data concerning a natural person's […] sex life or sexual orientation" pursuant to Article 9(1).

The NO DPA shall assess whether Grindr processed data "concerning" a natural person's "sexual orientation" in the context of Article 9(1) by sharing personal data on a specific user alongside app name or ID to advertising partners.

Grindr argues that it is wrong to assume that Grindr's users are "presumably gay" or that being a Grindr user means that the user "belongs to a sexual minority". Grindr argues that a 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". The app is open for all sexual orientations, including those who are unsure about their own sexual orientation.

To the NO DPA's knowledge and understanding, Grindr is not intended to be used, or in practice customarily used, by cis men looking to interact with cis women and vice versa.

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 "sex life" and "sexual orientation". According to the GDPR commentary by Kuner et al., Article 9 stipulates a broad definition of sensitive data.[59] The CJEU has also stated this in relation to other categories of sensitive data under the previous Directive 95/46/EC.[60] This indicates that contradictory to Grindr's argumentation, Article 9 does not require disclosure of the data subject's particular sexual orientation.

Grindr markets itself as the largest social networking app for "gay, bi, trans and queer" people[61], and the app is marketed as "Grindr – Gay chat" on both the App Store and Google Play. Grindr explicitly targets data subjects belonging to a sexual minority through its marketing. When Grindr discloses information on the data subject alongside the fact that the data subject is a Grindr user, or generic keywords related to the Grindr app like "gay" or "bi", it strongly indicates to the recipient that the data subject belongs to a sexual minority – and one of the particular sexual orientations Grindr targets with their marketing.

The indication of the Grindr user's sexual orientation becomes further evident through news articles about the Grindr app. Our own investigation shows that the app is regularly described a "gay" dating app.[62] We find that by public perception, being a Grindr user indicates that the data subject belongs to a sexual minority – gay, bi, trans or queer.

Concerning special categories of data, recital 51 states:

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

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

---

[59] Kuner, Bygrave and Docksey (eds.), *The EU General Data Protection Regulation (GDPR), A Commentary* (OUP 2020), p. 374.
[60] C-101/01, *Lindqvist*, para. 50-51.
[61] https://www.grindr.com/, last visited 7 December 2021.
[62] To illustrate: https://www.nytimes.com/2021/08/20/nyregion/pillar-grindr-catholic-church.html, https://www.washingtonpost.com/lifestyle/2018/12/06/grindr-was-first-big-dating-app-gay-men-now-its-falling-out-favor/, https://www.forbes.com/sites/korihale/2020/03/26/grindrs-chinese-owner-sells-gay-dating-app-over-us-privacy-concerns-for-600-million/?sh=2de4ef86551c, https://techcrunch.com/2016/01/11/chinese-gaming-firm-buys-60-of-gay-dating-app-grindr-for-93m/, https://apps.apple.com/us/app/grindr-gay-dating-chat/id319881193, last visited 7 December 2021.

Discrimination against sexual minorities is unfortunately a fact in most countries, including Norway.[63] Prejudice and discrimination is a breach of fundamental rights and freedoms, as established by the European Convention for the Protection of Human Rights and Fundamental Freedoms[64] and The Constitution of the Kingdom of Norway.[65]

Furthermore, Grindr users in Norway may have ties to territories where sexual minorities face persecution. For example, the rights and freedoms of a person seeking asylum or temporarily residing in Norway may be at risk if they return to such a territory and the fact that they belong to a sexual minority becomes known. Risks may also apply if the individual belongs to certain conservative religious communities in Norway or abroad.

Grindr has argued that the fact that a data subject is a Grindr user is not likely to lead to prejudice or discrimination against the data subject in the real world. Grindr holds that although there are places where sexual minorities are at risk of being discriminated against, this is not a type of discrimination that is evident in the digital world. According to Grindr, the only link between Grindr and the physical world is those situations where two Grindr users agree to meet in-person.

While it is not necessary to demonstrate that a specific processing has led or is likely to actual harm or damage in order to fall within the scope of Article 9(1), we do not agree with Grindr's argument of a segregated digital and physical world. Grindr disclosed personal data to advertising partners who may process and share personal data further outside of Grindr's control. As mentioned, one of Grindr's advertising parties, Twitter's MoPub, alone lists more than 160 partners. The more personal data is spread, the larger the risk for data breaches or misuse becomes. To illustrate this risk, Grindr itself has faced allegations of security issues and exposed data in the past, though we underline that the NO DPA has not verified these allegations.[66] It is our view that spreading the data in question could put the data subject's fundamental rights and freedoms at risk, such as the right to privacy and non-discrimination. This does not only apply in the digital wold, but also in the physical world. As the WP29 has stated, "[m]isuse of sensitive data, such as health data or sexual orientation (e.g. if publicly revealed), may be irreversible and have long-term consequences for the individual as well as his social environment."[67]

---

[63] 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 8 December 2021).

[64] 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).

[65] Section 98.

[66] https://www.forbes.com/sites/janetwburns/2018/03/29/report-says-grindr-exposed-millions-of-users-private-data-messages-locations/?sh=252a00865c4c, https://www.nbcnews.com/feature/nbc-out/security-flaws-gay-dating-app-grindr-expose-users-location-data-n858446, last visited 7 December 2021.

[67] Article 29 Working Party, *Advice paper on special categories of data ("sensitive data")*, 2011, page 4.

An example of this is the media reports of the summer 2021 concerning a top U.S. Catholic church official resigning after location data reportedly tied to Grindr was used to show that he had frequented gay bars.[68] We do not have evidence that the data in question stemmed from Grindr, and we have noted that Grindr denies this.[69] However, this case clearly illustrates how data from the digital world can put the data subject's fundamental rights and freedoms at risk in the physical world.

Being a Grindr user strongly indicates, and appears in most cases to accurately reflect, that the data subject belongs to a sexual minority. Furthermore, the fact that a data subject belongs to a sexual minority may lead to prejudice and discrimination even without revealing their specific sexual orientation. As established above, the wording of Article 9 does not require a revealing of a particular "sexual orientation", and the purpose behind Article 9 discourages a narrow interpretation.

For these reasons, we find that information that a data subject is a Grindr user is data "concerning" the data subject's "sexual orientation".

Grindr further holds it did not share data concerning a particular data subject's sexual orientation within the scope of Article 9. Grindr argues that EDPB confirms in its *Guidelines 3/2019 on processing of personal data through video devices* that the revealing of the data is not sufficient to trigger the applicability of Article 9(1), as long as the purpose of such processing is not to deduce special categories of data.

These statements relate specifically to processing through video surveillance systems, which by its nature usually collect massive amounts of personal data indiscriminately, and which may reveal data of a highly personal nature and even special categories of data. The special circumstances related to data processing through of photographs and video is illustrated by recital 51 GDPR:

> *"The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person."*

The EDPB states that video surveillance is *not always* considered to be processing of special categories of personal data even if they reveal special categories of data, and it uses video

---

[68] https://www-vice-com.cdn.ampproject.org/c/s/www.vice.com/amp/en/article/pkbxp8/grindr-location-data-priest-weaponization-app, https://www-inquirer-com.cdn.ampproject.org/c/s/www.inquirer.com/news/nation-world/monsignor-jeffrey-burrill-resigns-grindr-20210720.html?outputType=amp or https://www.washingtonpost.com/religion/2021/07/20/bishop-misconduct-resign-burrill/ last visited 7 December 2021.

[69] https://blog.grindr.com/blog/in-response-to-a-small-blogs-witch-hunt-to-out-a-gay-priest last visited 7 December 2021.

footage showing the data subject with glasses or in a wheelchair as an example of this.[70] However, the EDPB states that if the video footage is processed to deduce special categories of data, then Article 9 applies, and it uses an image showing the data subject engaging in a strike as an example of this.[71]

The situation described by the EDPB is in contrast to a situation where a video surveillance system is directed specifically and exclusively towards an area that would systematically reveal special category data. For example, video surveillance inside a mosque or a hospital cancer ward would clearly reveal sensitive personal data falling within Article 9(1), even if the purpose of the video surveillance is purely security related. In this situation, there is no longer an indiscriminate collection of data where any processing of special category data is merely coincidental and difficult to foresee. Instead, the processing would necessarily always entail a foreseeable processing of special category data, and the processing would entail a much greater risk for the data subjects' fundamental rights and freedoms, as contemplated in recital 51.

Grindr has further quoted an excerpt and a footnote from the GDPR commentary of Kuner et al., but the full quote is made in reference to the above-mentioned EDPB statements related to video devices, and reads:

> *"More generally, it has also been argued in the scholarly literature that information about an individual obtained in everyday situations should not be considered sensitive data unless there is an intention to use it based on one of the particular elements of sensitivity obtained in the law, but this view has yet been added affirmed by courts or regulators"*

As established above, we hold that the fact that the data subject is a Grindr user is data "concerning" the data subject's "sexual orientation", i.e. belonging to a sexual minority. In our view, the sharing of personal data in this case was not an everyday situation, or comparable to the examples in the EDPB guidance on video devices. The examples in the guideline refers to situations where the revealing of special categories of personal data coincidentally happens and is difficult for the controller to foresee or control. This is not the case with Grindr. Grindr is a dating app that explicitly targets sexual minorities. The app name or ID was disclosed to advertising partners together with the personal data of a specific user. The purpose was to display behavioural advertisement to the data subject within the specific app and potentially elsewhere.

Grindr further argues that they would be surprised if any ad company can or would profile based on "special categories" of personal data.

---

[70] EDPB, *Guidelines 3/2019 on processing of personal data through video devices*, version 2.0, adopted on 29 January 2020, para. 62.
[71] Ibid, para 64-65.

The NO DPA notes that the sharing of personal data concerning a natural person's "sexual orientation" to advertising partners is sufficient to trigger Article 9, irrespective of how the data is further processed by the data controllers the data was disclosed to.

Furthermore, irrespective of its legality or accuracy, we do not agree with the argument that a data subjects "sexual orientation" is not a category of data that could potentially be used by advertisers to target ads.

To illustrate this, on Grindrs own website, Grindr markets advertising on their platform with "Advertise on Grindr and connect with the world's largest and most active, engaged and influential queer audience."[72] This illustrates that the fact that a data subject is a Grindr user can be viewed as relevant for audience segmentation for an advertiser.

Furthermore, in a blog post from Grindr on 3 September 2021, Grindr presented a new privacy feature called "Ad Targeting Opt-Out",

> *which allows people to opt out of having their use of Grindr remembered by our Ad Partners—meaning they won't receive LGBTQ+ ads outside their use of the Grindr app based on the fact that they have used the Grindr app. Grindr and our partners already honor the device-wide opt-out features in iOS and Android, but this new setting is for those users who want to receive targeted ads for most of their activities but not targeted ads based on their use of the Grindr app.*[73]

Grindr also argues that Grindr's advertising partners – in the event they would ever theoretically receive sensitive personal data – must "blind" themselves to any sensitive personal data pursuant to GDPR Article 25. Grindr states that its contracts with its advertising partners have contractual commitments to comply with applicable laws.

Grindr further states that many of the ad tech companies operating in the EU have, throughout the last decade, devised "blinding methods" to obfuscate which app the ad call is coming from. Grindr holds that participants in the ad tech ecosystem would likely only receive a "blinded" app-ID and not the corresponding app name. According to Grindr, it is a common practice in the EU for ad networks to nullify the app name and use a random App ID in the ad call so that downstream bidders are "blind" to the actual name of the app where the ad is to be served.

However, as established above, Grindr's understanding of Article 9 was not correct, and the fact that a data subject is a Grindr user qualifies as data "concerning" a natural person's "sexual orientation", cf. Article 9(1) GDPR. The Mnemonic technical report shows that app

[72] https://www.grindr.com/advertise/ last visited 7 December 2021.
[73] https://blog.grindr.com/blog/new-privacy-features-for-grindr-users, last visited 7 December 2021.

name was shared to MoPub, who further shared this within their mediation network.[74] It further shows that app name was shared from Grindr to multiple other advertising partners.[75]

Grindr's above-mentioned statement on "blinding practices" for the app-ID in the reply to the advance notification, is contradictory to the information given by Grindr in its response 22 May 2020 to the NO DPA's order to provide information, where Grindr stated on page 25:

> *It is Grindr's understanding that all apps and all website that serve advertising necessarily share the identity of the app and/or the website with their advertising partners. Simply put, it is highly unlikely any advertiser would purchase advertising on an unknown app or an unknown website. Reasonable users understand that advertising-supported applications and websites cannot exist without disclosing the app's or website's name to advertising partners. Indeed, that assumption is ubiquitous in the industry. While most apps and websites disclose within their privacy notices that they share personal data with their advertising partners, Grindr (and BCLP) are not aware of any applications or websites that explicitly disclose within their privacy notice that the application's or website's name is shared alongside personal data with advertisers. Controllers trust that data subjects understand that part of "sharing" is for the controller to disclose its own identity to the entity to whom the data will be disclosed.*

In the connected footnote, Grindr further states:

> *Even if a website or app did not share its name, advertisers must necessarily share their URL and IP address with adtech partners in order for the adtech partner to render and serve an advertisement. As a result, the identity of a website or app is readily discernable to an adtech partner.*

Grindr's current privacy policy even explicitly states that "[o]ur advertising partners are aware that such data is being transmitted from Grindr."

Even if some advertising partners or other participants in the ad tech ecosystem would "blind" themselves or only receive an obfuscated app ID, this is not line with the principle of accountability in Article 5(2) GDPR. Grindr would have to rely on the action of advertising partners or other participants in the ad tech ecosystem to halt its sharing of the data in question.

We further understand that even if the app-ID in some instances was "blinded", the recipient could still receive keywords relating to the Grindr app. An example of this practice is described in the *ICO Update report into adtech and real time bidding* from 20 June 2019 that

[74] Mnemonic technical report, page 26-28
[75] Ibid, page 29-30.

Grindr has referenced, and describes that a proportion of the bid requests in TCF[76], OpenRTB and Authorized Buyers involve the processing of special category data – directly or inferred.[77]

The Mnemonic technical report further shows that OpenX, who Grindr consider to be its processor, appended keywords "gay", "bi" and "bi-curious" in ad calls.[78] Use of such keywords would have a similar effect to disclosing that the data subject is a Grindr user, and also constitute processing of personal data "concerning" a natural person's "sexual orientation", cf. Article 9(1) GDPR.

Regardless, Grindr shared information on a specific user alongside app name or ID to advertising partners, as shown in the Mnemonic technical report.

The NO DPA finds that Grindr processed data "concerning" a natural person's "sexual orientation" pursuant to Article 9(1) by sharing personal data on a specific user alongside app name or app ID to advertising partners.

As a result, it is unnecessary for the NO DPA to assess whether Grindr processed data "concerning" a natural person's "sex life" pursuant to Article 9(1) by sharing information on a specific user alongside app name or app ID to advertising partners. For the record, according to the GDPR commentary of Kuner et al. to the GDPR, "sex life" is to be broadly construed to include not only sexual orientation, but also information on sexual practices and intimate personal details.[79]

Grindr states that the NO DPA's assessment of Article 9 would 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 in their response to the NO DPA's order to provide information.[80]

Grindr further states that the NO DPA's reasoning would impose a higher threshold for apps which serve the LGBTQ+ community when collecting and sharing data for advertising purposes than for the rest of other players in the market for social network or dating apps, which process the same categories of data for the same purposes. This includes travel agencies specializing in LGBTQ+ travel, "gay friendly" hotels, organizers of LGBTQ+ events, or any organization that markets to or provides any product or service for the LGBTQ+ community.

---

[76] Grindr has described in point 1.2.7 of the response to the advance notification 8 March 2021 that it strived to implement versions of Transparency and Consent Framework (TCF), and that many of its advertising partners are members of the TCF working group.
[77] ICO, Update report into adtech and real time bidding 20 June 2019, page 16: https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf.
[78] Mnemonic technical report, page 28, Grindr's response to the advance notification 8 March 2021, page 36.
[79] Kuner, Bygrave and Docksey (eds) (2020), *The EU General Data Protection Regulation (GDPR), A Commentary* (OUP 2020), p. 376.
[80] Response to the NO DPA's order to provide information, pages 27-28.

We do not agree with Grindr's comparison and argumentation. Most of Grindr's examples show weaker indications of special categories of personal data. Grindr, on the other hand, is a dating app that explicitly targets sexual minorities.

Furthermore, for the instances where Article 9 applies, valid consent is already the appropriate legal basis pursuant to Article 6(1) for intrusive profiling and tracking practices for advertising purposes, as established in 5.4.1 above. As such, the controller would only need to fulfil the additional requirement for the consent to be explicit, cf. Article 9(2)(a). As established in 5.4, Grindr failed to fulfil several of the requirements for a valid consent pursuant to Article 6(1)(a) when collecting consents for sharing personal data to advertising partners in the previous CMP.

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.

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

Article 9(2)(a) GDPR 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.

As established in section 5.4 above, Grindr did not fulfil the requirements for valid consents under Article 6(1)(a) GDPR when collecting consents for sharing personal data to advertising partners in the previous CMP.

As Article 9(2)(a) GDPR also requires consents for processing special categories of personal data to fulfil the requirements in Articles 4(11) and 7 GDPR, in addition to the requirement of "explicit", we conclude that Grindr did not have valid consents under Article 9(2)(a).

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

The NO DPA shall assess whether the fact that the data subjects were Gindr users entail that they "manifestly made public" data concerning their sexual orientation.

Article 9(2)(e) GDPR requires that the data have been "manifestly" made public. The wording implies that it must be obvious that the data subject has meant to make the information in

question available to the public. The word "manifestly" implies a high threshold for relying on this exception.[81] According to the GDPR commentary of Kuner et al., "making public"

> *should be construed to include publishing the data in the mass media, putting them on online social network platforms or similar actions. However, the data must have been "manifestly" made public, which requires an affirmative act by the data subject, and that he or she realised that this would be the result.*[82]

Grindr is a social networking app with approximately [redacted] million daily users. Grindr explains that anyone can download the free version of the app and gain access to other Grindr users, and that this is an essential part of the Grindr services.

Grindr further argues that 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 argues that it warns the data subjects that the information they explicitly share through their profile will be made public. The privacy policy states:

> *"Remember that if you choose to include information in your Grindr community profile, that information will become public to other Grindr users. As a result, you should carefully consider what Personal Data to include in your profile."*

Grindr holds that by accepting the Privacy Policy and creating a Grindr profile, the users must be deemed to have taken an affirmative action, and the fact that the data subject is a Grindr user has been "manifestly made public".

However, the above-mentioned information in the Privacy Policy was not easily visible to the data subjects. As established above in 5.4.4, when presented with a full privacy policy, data subjects may easily choose not to acquaint themselves with the information. Furthermore, Grindr is a LGBTQ+ dating and social networking app, used for creating intimate relations or connecting with other users in the LGBTQ+ community. In our view, there is a distinct difference between making information solely available to a community of peers, and making information available to the general public.

As Grindr states, the data subject's profile could be available to (i) free users (ii) paid users who have access to Unlimited profiles, or (iii) paid users who use the Explore feature to find users in other regions.

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.

---

[81] This is also supported by the European Data Protection Board in *Guidelines 8/2020 on the targeting of social media users,* Version 1.0, Adopted on 2 September 2020, para. 120.
[82] Kuner, Bygrave, and Docksey (eds),*The EU General Data Protection Regulation (GDPR), A Commentary* (OUP 2020)*,* p. 378.

The Unlimited profiles feature was introduced in August 2019 and has only been available for a part of the duration of the infringement. Moreover, we understand that this feature would still sort users by distance from the user's actual or chosen location.

Furthermore, the Grindr app does not have any search functionality for finding specific users.

As a result, even though Grindr has approximately [redacted] million daily users, the data subject's Grindr profile would in practice only be shown to a limited amount of users, and most of these would be Grindr users near the user's actual or chosen location. This also shows that a Grindr user may not necessarily have intended to make the information "public", but only available to a limited number of relevant users. The data subjects did not publish the information on an open platform, which in our view points to the direction that they have not manifestly made their sexual orientation public.

Furthermore, the data subjects choose their own nickname and whether they want to upload a profile image in the Grindr app. Thus, it is possible to have an anonymous approach vis-à-vis other users in the app. A survey by NRK showed that out of 500 profiles in five Norwegian cities, only half choose to share a picture of their face.[83] In these instances, the data subject has not made their identity together with their sexual orientation available to other Grindr users.

At any rate, it goes beyond the reasonable expectations of the data subject that Grindr would disclose information concerning their sexual orientation to advertising partners. Though information about someone merely being a Grindr user must be considered a special category of personal data under Article 9(1), becoming a Grindr user is not an affirmative act by the data subject to make the information public.

The EDPB guidelines on the targeting of social media users list five elements that may be relevant to help inform the assessment under Article 9(2)(e). A combination of these elements or other elements may need to be considered.[84] As these guidelines were not available at the time of the infringement, Grindr could not refer to these guidelines. However, they can still provide an expression of the administrative practises of EEA data protection authorities and their common understanding of the GDPR.

We have established above that the Grindr app is intrinsically linked with the idea of creating intimate relations, or connecting with other users in the LGBTQ+ community. The guidelines on targeting of social media users also indicate that in these kinds of situations, the data has not been manifestly made public by the data subject.[85]

---

[83] https://nrkbeta.no/2021/08/07/menn-uten-ansikt/ last visited 7 December 2021.
[84] EDPB, *Guidelines 8/2020 on the targeting of social media users,* Version 2.0, Adopted on 13 April 2021, Section 8.2.
[85] Ibid. para. 127, element (ii).

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.[86] In the Grindr app, the data subjects may trust that their profile will only be visible to other users who have also created an account. Furthermore, as established above, the Grindr app does not have any search functionality for finding specific users and the data subject's Grindr profile would in practice only be shown to a limited amount of users, and most of these would be Grindr users near the user's actual or chosen location.

We have further established that when presented with a full privacy policy, data subjects may easily choose not to acquaint themselves with the information, and that the information in Grindr's privacy was not easily accessible 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.[87]

As such, the EDPB guidelines support our understanding of "manifestly made public".

In sum, and irrespective of the elements listed in the EDPB guidelines, it was not obvious that the data subjects meant to make the information in question available to the public. Even for the cases where data subjects identified themselves to other users through full name and pictures, they would presumably only have meant to make the data concerning their sexual orientation available to a limited amount of other members of the LGBTQ+ community, and most of these would be Grindr users near the user's actual location. The information was not published on an open platform, and there was no search functionality for finding specific users. By using a LGBTQ+-dating app like Grindr, the data subject does not forfeit the specific protection the GDPR offers to particularly sensitive data, processing of which can create significant risks in relation to their fundamental rights and freedoms.

For these reasons, the fact that the data subjects were Gindr users were not "manifestly made public" by the data subjects, cf. Article 9(2)(e).

As a result, Grindr did not fulfil one of the exceptions in Article 9(2) when it disclosed personal data on a specific user alongside app name or app ID to advertising partners.

Consequently, we have concluded that Grindr breached the prohibition in Article 9(1) when Grindr disclosed personal data linked with the app name or app ID to advertising partners.

[86] Ibid. para. 127, element (iii).
[87] Ibid. para. 127, element (iv).

6. Corrective measures

6.1. 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 (or "punishment", in Norwegian: *straff*) pursuant to the European Convention on Human Rights (ECHR).[88]

The Norwegian Supreme Court (Rt. 2012 p. 1556) has concluded that an administrative fine is a punishment under Article 6 in the ECHR. As a result, we can only impose a fine where there is clear preponderance of probability (in Norwegian: *klar sannsynlighetsovervekt*) of breaches of the GDPR.

In HR-2021-797-A, the Supreme Court stated that objective culpability based on the wording in the Penal Code section 27 concerning enterprise penalty, is not in conformity with the punishment term in the ECHR as it is currently applied in ECtHR case law. The Supreme Court held that imposing penalties for enterprises requires that a person acting on behalf of the enterprise, has at least acted negligent. Based on this decision, we hold that the same principle applies for imposing administrative fines against an undertaking pursuant to Article 83 GDPR.

In order to impose administrative sanctions, such as an administrative fine, the principle of legal certainty must be satisfied. The principle of legal certainty (also called the principle of legality, and in Norwegian: *Legalitetsprinsippet*) is a general principle in both EEA Law and Norwegian constitutional and administrative law.[89]

6.2. The culpability requirement for administrative fines

As mentioned above in section 6.1, in HR-2021-797-A the Supreme Court stated that imposing penalties for enterprises requires that a person acting on behalf of the enterprise, has at least acted negligent. Based on this decision, we hold that the same principle applies for imposing administrative fines against an undertaking pursuant Article 83 GDPR.

Grindr argues that there has not been an intentional or negligent breach of the GDPR and states that it exceeded industry standards and guidelines at the time of the infringement.

In our view, it is clear that Grindr, through its board members or executives which acted on behalf of it and were responsible for the previous CMP, intended to use its previous CMP at the time of the infringement. Our assessment in section 5.4 and 5.5 above shows that the previous CMP clearly did not meet the applicable GDPR requirements in Articles 4(11), 6, 7 and 9(2)(a).

---

[88] Section 43 of the Norwegian Public Administration Act.
[89] Grl. § 113.

Intent exists even if Grindr, through its board members or executives acting on behalf of it, was unaware that the act is unlawful due to ignorance of legal rules, as long as the ignorance was negligent.[90]

Pursuant to the requirement of due care, businesses and the responsible persons acting on behalf of it needs to examine what legal requirements that apply to their field and implement these. Grindr is a large professional actor operating across the EU market, and according to its website it is "the world's largest social networking app for gay, bi, trans, and queer people." The requirement for lawfulness of processing, special categories of data and valid consents are basic and fundamental requirements in the GDPR. At the time, there was also guidance available from the Article 29 Working Party, endorsed by the EDPB, on the relevant consent requirements. As established in sections 5.4 and 5.5.2 above, Grindr violated several of the cumulative requirements for a valid consent, and in our view, the inadequacy of the consent mechanism and the unlawfulness of the processing pursuant to Articles 6(1) and 9(1) GDPR should have been clear to Grindr, through the board members or executives acting on behalf of it. Any ignorance of the law on Grindr's part in this case, through its board members or executives acting on behalf of it, has been negligent.

Concerning the breaches of the GPDR in this case, we therefore find that a person acting on behalf of Grindr has at least acted negligent, and in our view, intentional.

6.3. Whether to impose an administrative fine

As established in 5.4 and 5.5 above, we have found that there is clear preponderance of probability that Grindr has breached Articles 6(1) and 9(1) GDPR. We deem it necessary to react to these breaches of the GDPR and issue an administrative fine pursuant to Article 83, cf. Article 58(2)(i), cf. Personal Data Act 2018 § 1.

Pursuant to Article 83(1), administrative fines "shall in each individual case be effective, proportionate and dissuasive".

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 purpose of the GDPR is to ensure a consistent and homogenous application of the GDPR and a high level of data protection throughout all of the Member States, including the application of administrative fines.[91]

For the purpose of achieving a consistent approach to the imposition of the administrative fines, the WP29 adopted guidelines concerning the application of the criteria in article 83(2)

[90] Principles of intent and ignorance of the law is codified in the Penal code section 22 and 26.
[91] GDPR Recital 10 and 150.

GDPR in 2017, which the EDPB endorsed in 2018.[92] Article 70(1)(k) specifically lists that for the purpose of ensuring a consistent application of the GDPR, the EDPB shall draw up guidelines for supervisory authorities concerning the setting of administrative fines pursuant to Article 83.

The guidelines state that

> *like all corrective measures in general, administrative fines should adequately respond to the nature, gravity and consequences of the breach, and supervisory authorities must assess all the facts of the case in a manner that is consistent and objectively justified. The assessment of what is effective, proportional and dissuasive in each case will have to also reflect the objective pursued by the corrective measure chosen, that is either to reestablish compliance with the rules, or to punish unlawful behavior (or both).*[93]

(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 breached Articles 6(1) and 9(1) GDPR, which are basic and fundamental requirements for processing pursuant to the GDPR.

As established above in 5.4, Grindr failed to fulfil the cumulative requirements of "freely given", "specific", "informed", "unambiguous" and "as easy to withdraw as to give consent", cf. Article 4(11) and Article 7 when collecting consents for sharing personal data to advertising partners in the previous CMP. Consent is a tool that gives data subjects control over whether or not personal data concerning them will be processed. Grindr's failure to fulfil the requirements for a valid consent under the previous CMP resulted in data subjects having limited or no control over their personal data flow. These circumstances meant that data subjects' control and choice over their personal data became illusory.

Grindr processed personal data illegally when it disclosed personal data about its users to advertising partners for the purpose of behavioural advertisement. These recipients subsequently disclosed the data to other recipients. As mentioned and illustratively, Grindr has disclosed the data to Twitter's MoPub, and Twitter's MoPub lists more than 160 partners.[94] This alone entails that over 160 partners could potentially access personal data from Grindr without a legal basis. We consider that the scope of the infringements adds to the gravity of them.

---

[92] Article 29 Working Party, *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679* (WP253), EDPB Endorsement 1/2018.
[93] Article 29 Working Party, *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679* (WP253), page 6.
[94] The NCC report p. 74.

The purpose of the particular processing operations in question was for providing behavioural advertisement. WP29 describes some challenges concerning profiling in their profiling guidelines:

> *The process of profiling is often invisible to the data subject. It works by creating derived or inferred data about individuals – 'new' personal data that has not been provided directly by the data subjects themselves. Individuals have differing levels of comprehension and may find it challenging to understand the complex techniques involved in profiling and automated decision-making processes.* [95]

The EDPB also summarises some of the risks to fundamental rights that are involved in profiling and targeting based on personal data in paragraph 8-17 of the *Guidelines 8/2020 on the targeting of social media users*. One of the risks the EDPB describes is the potential manipulation of users:

> *A second category of risk relates to potential possible manipulation of users. Targeting mechanisms are, by definition, used in order to influence the behaviour and choices of individuals, whether it be in terms of their purchasing decisions as consumers or in terms of their political decisions as citizens engaged in civic life. Certain targeting approaches may however go so far as to undermine individual autonomy and freedom (e.g. by delivering individualized messages designed to exploit or even accentuate certain vulnerabilities, personal values or concerns).*[96]

The invalid consents resulted in large-scale data sharing for the purpose of providing behavioural advertisement, which involves tracking and profiling. Profiling for targeting advertisement is an intrusive form of processing that can often seem opaque for the data subject. The adtech ecosystem is complex to understand for data subjects, and as stated by the EDPB, "a lack of transparency regarding the role of the different actors and the processing operations involved may undermine, complicate or hinder the exercise of data subject rights."[97] The processing could inter alia lead to potential manipulation of data subjects.[98] This also adds to the gravity of the infringements.

The data subjects did not initiate the particular processing operations in question. As discussed in Section 5.4, they presumably wanted to access the services provided in the app, and they did not necessarily intend to share their personal data to Grindr's advertising partners for targeted marketing purposes. To illustrate, in the NO DPA's privacy survey of 2019-2020, 43 % of respondents were very negative to personal data being used to target them with

---

[95] Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, p. 9.
[96] EDPB, *Guidelines 8/2020 on the targeting of social media users*, version 2.0, adopted 13 April 2021, para. 12
[97] Ibid. para. 10
[98] As also described in the NCC "Out of control" report page 46-47.

advertisement, and further 30 % of the respondents were somewhat negative.[99] In a survey by YouGov commissioned by the NCC, 30 % of the respondents were very negative towards receiving ads based on their personal data, and further 22 % of the respondents were somewhat negative.[100] The data subjects were subject to Grindr's and its advertising partners' commercial interests, with the potential of their personal data being disseminated or further processed without a valid consent and without clear information about this further processing. This adds to the gravity of the infringements.

The number of data subjects affected are one of the relevant conditions when considering whether to impose an administrative fine. According to the WP29 guidelines endorsed by the EDPB, 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.[101]

We do not consider the breach to be an isolated event, but something that affected almost all of the Grindr users in Norway over time.

Grindr's understanding in the response to the advance notification seemed to be that the NO DPA seeks to sanction Grindr's alleged breach against all users in the EEA. However, as clearly set out in our advance notification, this is not the case. This was also specifically clarified to Grindr in a letter from the NO DPA dated 11 October 2021. As explained above in section 5.2, this decision pertains to data subjects on Norwegian territory, and it is therefore without prejudice to the competence of GDPR supervisory authorities in other EEA territories. For the purpose of the administrative fine, we only take into consideration affected users in Norway.

Grindr has stated that for calendar years 2018, 2019, and 2020, the Grindr app had an average of [redacted] active monthly users of in Norway, respectively.[102] Of those users, approximately [redacted]% used the free version of the app and received third-party advertising.

These figures show that the number of data subjects in Norway that was affected by the infringements is substantial, which adds to the gravity of the infringements. It would appear that a large proportion of the LGBTQ+ community has been affected. Grindr further states in its marketing that it is "the world's largest social networking app for gay, bi, trans and queer people", and we presume that Grindr had a significant dating app market share in the LGBTQ+ community in Norway.

---

[99] https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/personvernundersokelser/personvernundersokelsen-20192020/personopplysninger-til-reklame-tjenester-og-produkter/, last visited 7 December 2021.
[100] https://fil.forbrukerradet.no/wp-content/uploads/2021/06/202106-befolkningsundersokelse-holdninger-til-overvakningsbasert-markedsforing.pdf, last visited 7 December 2021.
[101] 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. 10.
[102] Letter from Grindr to the NO DPA 19 November 2021, page 3.

The type of data shared illegally also illustrates the gravity of the infringements. Special categories of personal data, such as data concerning sexual orientation, merit specific protection under the GDPR. The affected data subjects wanted to join a dating app and social networking app, with the opportunity to connect with others in the LGBTQ+ community nearby. The disclosure of the data without the data subjects' valid consent has breached the data subjects' trust and violated their fundamental rights. Contrary to Grindr's arguments, as we have established in 5.5.1, misuse of the data concerning sexual orientation could put the data subject's fundamental rights and freedoms at risk, such as the right to privacy and non-discrimination.

Grindr also disclosed these data alongside the users' exact GPS location, which further adds to the gravity of the infringements. GPS location is particularly revealing of the life habits of data subjects, and can be used to infer sensitive information. Grindr argues that data subjects also had the possibility of opting out of sharing their location, but as established in 5.4.2 and 5.4.5, "opting-out" is not equivalent to a consent pursuant to GDPR. The invalidity of the collected consents under the previous CMP as described in 5.4, also applies to the sharing of GPS location. Furthermore, Grindr describes itself as a GPS based social networking app and "opting-out" of the Grindr App's access to location would according to the Privacy Policy result in the non-functioning of key features like displaying nearby user profiles.[103] As a result, the sharing of location data with advertising partners for behavioural advertisement purposes was bundled with processing of location data for the proper function of the app, depriving the user of genuine free choice as established in 5.4.2.

Grindr argues that only one data subject filed a complaint to the NCC, and that this implies a low level of damage suffered by the data subjects. We do not find this relevant, as in practice, only a select few data subjects choose to send complaints to a supervisory authority. It cannot be expected that a data subject has knowledge of the legal requirements in the GDPR. In addition, as established in 5.4.4, the consents given by data subjects were not "informed", and the data subjects were not made able to understand the consequences of Grindr's data processing. Furthermore, the data flow from the Grindr app was practically impossible for a data subject to understand, and the complaints from the NCC was accompanied by a thorough technical report prepared by a security company commissioned by the NCC. A data subject would normally never have opportunity get such an overview the relevant data processing operations.

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

[103] The privacy policy effective from 31 December 2019 stated that: *Should you choose not to allow the Grindr App to access your Location, certain features (such as displaying nearby user profiles or features that include Live Location Sharing) of the Grindr Services will not function properly*.

appropriate preventive measures, or inability to put in place the required technical and organisational measures.[104]

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 more than 21 months. Although the GDPR entered into force in July 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. The duration of the infringement is an aggravating factor.

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

(b) the intentional or negligent character of the infringement

As established in section 6.2 above, we consider that Grindr's infringements of the GDPR were intentional. This is an aggravating factor.

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

Grindr argues that if any user had suffered any damage due to the alleged breach of Article 6(1) and/or Article 9(1) under the previous CMP, Grindr mitigated such damage when it implemented the current CMP in April 2020.

We have not assessed Grindr's new CMP, but even if it would have been found to be GDPR compliant, we do not agree that the introduction of a new CMP ex post would be able to mitigate the damage suffered by the data subjects who already had their personal data shared illegally throughout the period of the infringements and thus has lost control of their data. The new CMP would only prevent further infringements from Grindr.

Grindr still holds that the collection of consents under its previous CMP was lawful, and has not informed the NO DPA that it has taken any action to inform recipients of the illegally disclosed data to ensure that the data is erased and further use of the data is halted.

We do not see any mitigating factors relevant to Article 83(2)(c).

However, we have further addressed the relevance of Grindr's implementation of the new CMP in the section on Article 83(2)(k) below.

---

[104] 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.

(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

According to the WP29 guidelines, the question that the supervisory authority must 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.[105]

Article 24 GDPR requires that "the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with [this Regulation]."

Moreover, Article 25(1) GDPR provides that:

> [...] *the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures,* [...]*, which are designed to implement data-protection principles,* [...]*, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.*

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 shared personal data from a large number of users, including data concerning sexual orientation, and the risks involved for the rights and freedoms of the data subjects was substantial. The nature of the processing and the number of users shows the importance of integrating necessary measures to ensure that data were not shared with advertising partners unlawfully.

Article 25(2) GDPR further provides that

> *[t]he controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.*

As established in section 5.4.2 above, even in the cases where data subjects would "opt-out" of data sharing on their device, Grindr would in some cases "only" transmit a signal conveying the data subject's "opt-out" preference together with the personal data. Again, 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 was not necessarily effective.

---

[105] Ibid. p. 13.

Grindr argues it had adopted a series of technical and organizational measures to ensure the security of the sharing of the data with the advertising partners as required by article 32, and lists examples of these on page 53 in the response to our advance notification. While we do find these measures somewhat mitigating, it seems that Grindr lacked control of the data flow and recipients, as it disclosed personal data with limited or no control over subsequent processing.

Concerning Article 9, Grindr further argues that it in many cases the user's use of the Grindr App is not provided to downstream participants in the ad ecosystem by "blinding" the app ID. However, as established in section 5.5 above, Grindr shared the data in question to advertising partners. Even if some advertising partners or other participants in the ad tech ecosystem would "blind" themselves or only receive an obfuscated app ID, this is not in line with the principle of accountability in Article 5(2) GDPR. Grindr would have to rely on the action of advertising partners or other participants in the ad tech ecosystem, to halt its sharing of the data in question.

This shows that Grindr has not sufficiently taken responsibility pursuant Articles 5(2), Articles 24 and Articles 25, and this is an aggravating factor.

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

We are not aware of any previous infringements.

Grindr argues that it must be taken into account as a mitigating factor that it has not previously violated the GDPR.

However, before the GDPR entered into force in Norway, the NO DPA did likely not have the competence to enforce the national data protection regulation against US-based companies like Grindr because of the territorial scope of the previous Personal Data Act. The infringement in question was ongoing from the GDPR entered into force in Norway 20 July 2018.

As a result, we do not assess the fact that Grindr has not been proven to have committed previous infringements as a meaningful mitigating factor.

(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 neither an aggravating nor a mitigating circumstance in the present case.[106]

[106] According to the Article 29 Working Party, *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679* (WP253) 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.

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

As discussed under (a) and 5.5 above, Grindr disclosed special categories of personal data unlawfully to advertising partners. As established above in 5.5, 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, such as the right to privacy and non-discrimination. Combined with exact location data, Grindr puts the data subject at even greater risk. This adds to the gravity of the infringement.

Exact GPS position is in itself a category of data that should be processed with due consideration. As mentioned above, GPS location is particularly revealing of the life habits of data subjects, and can be used to infer large amounts of information. For example, location data can reveal place of work and residence. It can also be used to reveal potentially sensitive data like religion through place of worship or sexual orientation through places visited. 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.

While the data shared was normally indirectly identifiable, it contained several online identifiers, and the personal data Grindr shared could potentially be combined with other data collected from other services, and from other devices through cross-device tracking.

Grindr argues that the personal data Grindr shared was [redacted] prevent unauthorised access to user information. However, the infringement in question relates to unlawful sharing personal data to advertising partners as authorised recipients. As a result, Grindr's partners were given access to the user information illicitly despite Grindr's [redacted]

In sum, we consider categories of personal data affected by the infringement as an aggravating factor.

(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 corrective 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 holds that in the event that it has breached Article 6(1) and Article 9, the content of these provisions are unclear. Grindr also argues that it should not be held to the latest standard immediately after promulgation by legislators. Grindr has further argues that the NO DPA has interpreted the GDPR in light of the EDPB Guidelines 05/2020 on consent and Guidelines 8/2020 on the targeting of social media users, which are non-binding and post-dates the period of the infringements.

As established above in sections 5.4 and 5.5, we hold that Grindr has infringed clear and precise legal requirements in Article 6(1) and Article 9, cf. Article 4(11) and Article 7 GDPR, which should clearly have been foreseeable for Grindr.

The GDPR was already announced on 4 May 2016.[107] Accordingly, Grindr had two years to adapt the GDPR requirements. Contrary to Grindr's arguments, the requirements for a valid consent has not been unclear from the start. For example, the legal assessment of "freely given", inter alia the requirement to allow for separate consents and not making the provision of the service conditional on consent to processing of personal data that is not necessary for the performance of the service, has not evolved since the announcement of the regulation. The requirements for a valid consent stem from GDPR Article 6(1)(a), Article 4(11) and Article 7, interpreted in light of the relevant recitals.

As elaborated on in section 5.4.1 above, EDPB and WP29 guidelines on consent are not the legal bases of our decision in the present case. The legal bases of our decision are exclusively the provisions of the GDPR. Guidance from the EDPB/WP29 has only has been used throughout this decision as an interpretive aid in our analysis of the requirements for a valid consent in the provisions of the GDPR. These guidelines support our interpretations of the relevant GDPR requirements.

As regards to Grindr's argument that Guidelines 05/2020 post-dates the period of infringements, as stated above in section 5.4.1, these guidelines 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 that was available during the

[107] See the Official Journal of the European Union, L 119, Volume 59, 4 May 2016.

period of the infringement. 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.[108] Thus, for the purpose of the present case, it should be stressed that the guidance on the notion of consent that was available at the time when Grindr's previous CMP was in use was essentially identical to the one issued by the EDPB in 2020. For all references to Guidelines 05/2020 throughout this decision, we have included in the footnotes the corresponding reference to the Article 29 Working Party Guidelines on consent under Regulation 2016/679 (WP259) that was available during the period of the infringement.

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 arguments 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 disclosed data concerning 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. This is an aggravating factor.

Grindr has argued that the NO DPA has not given regard to the changes Grindr has made in their current CMP, which it began exploring in June 2019 and deployed for users in Norway April 2020.

As mentioned above, we have not assessed Grindr's new CMP, but even if the new CMP was found to be GDPR compliant, the NO DPA notes that the implementation of the new CMP cannot annul the infringements under the previous CMP. However, we do find the fact that Grindr has taken steps with the aim to remedy the deficiencies in their previous CMP to be a mitigating factor.

Grindr also refers to guidance on consent provided by the Irish supervisory authority (DPC) from April 2020,[109] 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.

---

[108] See the preface in EDPB, *Guidelines 05/2020 on consent*, version 1.1, adopted 4 May 2020.
[109] DPC, *Guidance Note: Cookies and other technologies,* April 2020.

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.[110]

Furthermore, in the *Contribution of the EDPB to the evaluation of the GDPR under Article 97*, adopted 18 February 2020, the EDPB mentioned that between May 2018 and November 2019, European DPAs had issued approximately 785 fines altogether. In addition, it noted that:

> *Most of the fines related to principles relating to processing of personal data (Art. 5 GDPR); lawfulness of processing (Art. 6 GDPR); valid consent (Art. 7 GDPR); processing of special categories of personal data (Art. 9 GDPR); transparency and rights of the data subjects (Art. 12 to 22 GDPR); security of processing and data breaches (Art. 32 to 34 GDPR)*

As shown, Article 6, 7 and 9 are some of the Articles with the most fines issued by DPAs.

In addition, 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 already noted above, the GDPR entered into force in Norway on 20 July 2018, and it was already announced in April 2016. We do not consider Grindr's arguments as mitigating factors.[111]

According to the WP29[112], profit from infringements is a strong indication that a fine should be imposed:

> *Information about profit obtained as a result of a breach may be particularly important for the supervisory authorities as economic gain from the infringement cannot be compensated through measures that do not have a pecuniary component. As such, the fact that the controller had profited from the infringement of the Regulation may constitute a strong indication that a fine should be imposed.*

Grindr has stated that the total amount of advertisement revenue related to Norwegian users was less than [redacted] from May 2018 through the end of March 2020.[113] We find it aggravating that Grindr have gained financial benefits from the infringements. Grindr users had their personal data shared and re-shared with a potentially vast amount of advertising

---

[110] https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc, last visited 7 December 2021. CNIL also found that Google had violated the provisions in Articles 12 and 13.
[111] 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.
[112] Article 29 Working Party, *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679* (WP253) p. 16
[113] Grindr's response to the advance notification 8 March 2021, page 59.

companies and advertisers without a legal basis, while Grindr and its advertising partners profited.

The financial situation of the controller is also relevant. According to Grindr, its annual turnover for 2020 was [redacted] We find that Grindr's financial situation calls for an administrative fine in the present case.

We also note that the time the NO DPA has used to prepare this case is not excessive relative to the scope and complexity of the present case, and we refer to the description of the timetable of the NO DPAs investigation in section 3.3 above. We therefore do not find time used to prepare the case of any significance for the questions of whether to impose an administrative fine or deciding the amount of the administrative fine.

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

6.4. Deciding the amount of the administrative fine

Article 83(1) GDPR establishes the following 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.*

Article 83(2) further provides that when deciding on the amount of the administrative fine in each individual case due regard shall be given to the factors listed in Article 83(2)(a)–(k) GDPR.

Recital 148 of the GDPR emphasizes that administrative fines should be imposed "in order to strengthen the enforcement of the rules of this Regulation".

Grindr has argues that, in the advance notification, the NO DPA's reasoning regarding the amount of the fine was excessively short. However, as stated above, in accordance with Article 83(2) the NO DPA must also take due regard to the arguments in 6.3 above when deciding the amount of the fine. This was also clearly stated in the advance notification page 27. As a result, the NO DPA's reasoning regarding the amount of the fine included section 5.3.2 of the advance notification, and was not short.

As established in section 6.3 on Article 83(2)(a) above, Grindr illegally disclosed personal data on its users to advertising partners for the purpose of behavioural advertisement, who in

[114] Based on the USD to NOK daily exchange rate 9 December 2021 of 8,978, quoted by Norges Bank: https://www.norges-bank.no/en/topics/Statistics/exchange_rates/, last visited 10 December 2021.

turn would further process and share the personal data with their own partners and advertisers. As a result, the scope of the processing was substantial. To process and share data for the purpose of behavioural advertisement must be considered a core-activity for Grindr, and the processing in question was for the commercial interests of Grindr and its partners. Thousands of data subjects were affected by the unlawful processing and had their personal data, including location data and the fact that they are Grindr users, unlawfully spread. Furthermore, the duration of the infringement was over 21 months. In sum, the nature, gravity and duration of the infringement taking into account the nature, scope and purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them, indicates that a high amount is appropriate.

As established in section 6.3 on Article 83(2)(b), the intentional character of the infringement is aggravating circumstance.

We have further established in section 6.3 on Article 83(2)(d) that Grindr did not sufficiently take responsibility pursuant to Articles 5(2), Articles 24 and Articles 25, which is also aggravating.

As established in section 6.3 on Article 83(2)(g), Grindr disclosed special categories of personal data, which merit special protection under the GDPR, unlawfully to advertising partners. Disclosure of such data could put the data subjects' rights and freedoms at risk, such as the right to privacy and non-discrimination. Grindr further shared GPS location, which is particularly revealing of the life habits of data subjects, and which can be used to infer large amounts of private information. The categories of personal data affected by the infringement is a clearly aggravating factor.

As established in section 6.3 on Article 83(2)(k), we find the changes Grindr has made with the aim to remedy the deficiencies in their previous CMP to be a mitigating factor. However, we find it aggravating that Grindr has gained financial benefits from the infringements.

We do not find Article 83(c), (e), (f), (h), (i), and (j) relevant for the assessment of the amount of the administrative fine in the present case, as we have not established mitigating or aggravating factors in regard to these elements.

The argumentation above and in section 6.3 establishes several aggravating factors and suggests that a high amount is appropriate.

Infringements of Article 6 and 9 qualifies for the maximum amount for administrative fines as set out in Article 83(5). The maximum amount in Article 83(5) is 20 000 000 EUR or up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. However, as mentioned, the amount must be "effective, proportionate and dissuasive" in each individual case.

We therefore find Grindr's annual turnover relevant in our assessment. In our advance notification, we assumed that Grindr's annual turnover was at least USD $100 000 000 based

on interviews with Grindr's Chief Operating Officer.[115] Other sources indicated a substantially higher annual turnover.[116] In the reply to the advance notification, Grindr informs that its annual turnover for 2020 was [redacted]

When determining the maximum amount of the fine in accordance with Article 83(5), 20 000 000 EUR is higher than 4 % of Grindr's total worldwide annual turnover. Thus, the maximum amount of the fine is 20 000 000 EUR, and Grindr's annual turnover is only relevant for assessing what amount is effective, proportionate and dissuasive in the present case. Grindr's annual turnover indicates that a substantial fine is needed to be effective, proportionate and dissuasive in the present case.

Grindr has argued that what matters is the company's EBITDA, and not the turnover. The NO DPA notes that Article 83 GDPR explicitly provides that the turnover is a potential deciding factor for determining the maximum amount of the fine. This clearly indicates that turnover is relevant for determining the actual amount of the administrative fine.

In any case, Grindr has not provided information on the company's EBITDA in the response to the advance notification. According to an article published on 7 July 2020, Grindr generated a net profit of about 31 million USD (approximately 278 318 000 NOK[118]) in 2019, with reference to Kunlun Technology's annual report.[119] 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. We cannot see Grindr's EBITDA as indicative of a reduction of the amount of the fine.

Grindr further argues that it has been negatively impacted by COVID-19, which should be taken into account when determining the amount of the administrative fine. Grindr states it has been hit by the pandemic like all other companies through a reduction in the speed of product releases with a need for more time, money, and effort to organize, develop, and release its product roadmap.

The NO DPA agrees that a negative financial impact of COVID-19 may be relevant for determining the amount of the fine. In the advance notification, the NO DPA specifically

---

[115] https://www.latimes.com/business/story/2020-07-02/grindr-new-ownership-american-investors-interview and https://www.reuters.com/article/us-health-coronavirus-ppp-grindr/grindr-dating-app-valued-at-620-million-cleared-for-small-business-loan-idUSKBN247308?edition-redirect=in last visited 10 December 2021.
[116] https://www.forbes.com/sites/korihale/2020/03/26/grindrs-chinese-owner-sells-gay-dating-app-over-us-privacy-concerns-for-600-million/?sh=5fc0abca551c, quote: "The Financial Times found that during the first three months of 2019 Grindr's total revenues were Rmb 553 million ($77.9 million)."
[117] Based on the USD to NOK daily exchange rate 9 December 2021 of 8,978, quoted by Norges Bank: https://www.norges-bank.no/en/topics/Statistics/exchange_rates/, last visited 10 December 2021.
[118] Based on the USD to NOK daily exchange rate 9 December 2021 of 8,978, quoted by Norges Bank: https://www.norges-bank.no/en/topics/Statistics/exchange_rates/, last visited 10 December 2021.
[119] https://in.reuters.com/article/us-health-coronavirus-ppp-grindr/grindr-dating-app-valued-at-620-million-cleared-for-small-business-loan-idUSKBN247308 last visited 7 December 2021.

asked Grindr to explain why and provide relevant documentation if the COVID-19 situation has affected it in a way that is relevant to our notified decision. However, Grindr has not presented any documentation of how and to what extent it has been negatively impacted by COVID-19 financially, and the NO DPA notes [redacted] Therefore, we do not find that Grindr's argument that it has been negatively impacted by COVID-19 as indicative of a reduction of the amount of the fine.

Grindr has further referenced the Danish DPA's guidelines on the size of administrative fines as relevant for this case.[121] Grindr states that for a breach of Article 6, the base amount according to the Danish Data Protection Authority's guidelines constitutes 10% of the maximum administrative fine imposable – approximately NOK 20 000 000. For a breach of Article 9 the base amount according to the Danish Data Protection Authority's guideline would be 20% of the maximum administrative fine – approximately NOK 40 000 000.

As previously stated in relation to guidance documents by the Irish and French DPAs, the guidance provided by the Danish DPA is not a binding document for other supervisory authorities, and it does not reflect a harmonized approach on an EEA level. In any event, the sizes Grindr mentions are merely base sizes which can be adjusted based on the factors listed in Article 83(2) according to the Danish DPAs guidance. As mentioned above, we have established several aggravating factors which suggests that a high amount is appropriate.

Grindr further argues the current highest fine issued by the NO DPA is the fine of NOK 3 000 000 against the municipality of Bergen, and that the difference between this fine and the fine the NO DPA notified our intent to impose against Grindr, cannot be justified by the factors listed in Article 83(2).

The NO DPA does not find the case against the municipality of Bergen comparable to the present case. For example, the infringements identified in the Bergen case concern different provisions of the GDPR, and the infringements in this case is of a much larger scope. Additionally, Grindr is a large commercial company with an annual turnover of [redacted] NOK. For large commercial companies that may profit financially from GDPR violations, it is important that the administrative fine is not set too low in order to ensure a sufficient financial incentive for the perpetrator and other companies in the market to avoid further violations. Otherwise, the risk of an administrative fine (e.g. the likelihood of a fine multiplied with the expected size of the fine) could become an expense item in their budget which they would be comfortable with in order to gain financially from a violation. The municipality of Bergen, however, is a public body that receives its funding from public taxes. It did not enjoy a commercial benefit from the infringement, and it is not subject to the same economical or financial logic as private companies operating on the open market. As such, the assessments of what constitutes an "effective, proportionate and dissuasive" amount in the two cases are completely different.

---

[120] Grindr's response to the advance notification, page 60

[121] Datatilsynet, *Bødevejledning, Udmåling af bøder til virksomheder*, January 2021: https://www.datatilsynet.dk/Media/1/9/B%C3%B8devejledning.pdf

We also note that in the time period following the advance notification, the NO DPA has issued decisions and advance notifications of larger fines. This includes an advance notification of our intent to impose a fine of NOK 25 000 000 against Disqus Inc,[122] and a decision of an administrative fine of NOK 5 000 000 against Ferde AS.[123]

Lastly, Grindr argues the notified fine constitutes [redacted] of Grindr's global annual turnover, which according to Grindr would be the largest relative fine ever issued under the GDPR throughout the EEA. Grindr has provided a list of nine fines they argue are comparable, where the fines constitute between 0,0028% to 0,32 % of annual turnover.

As we have established above, the maximum amount of the fine is 20 000 000 EUR, and not 4% of Grindr's annual turnover.

Furthermore, we do not find the nine selected decisions provided in Grindr's list as representative of the general practice in the EU when it comes to administrative fines imposed under the GDPR. Moreover, we do not find any of the decisions that Grindr lists comparable to the present case. For example, none of the listed fines concern infringements of Article 9. Concerning administrative fines for infringements of Article 9, the Swedish DPA issued a fine against MedHelp AB for violating Articles 5(1)(a) and (f), 6, 9, 13 and 32 of SEK 12 000 000, which corresponded to 5,38 % of the undertakings annual turnover.[124]

The NO DPA has previously issued fines against both Radio Grenland AS and Cyberbook AS for breaches of Articles 6, 13, 17 and 21 corresponding to between 2-3 % of annual turnover of the these companies.[125] Furthermore, we have issued fines against Lindstram Trading AS for breach of Article 6(1) and Gveik AS for breaches of Articles 5(2) and 6(1), and in both cases the companies' turnover was 0 NOK.

All the above-mentioned fines issued by the NO DPA concerned infringements where only one data subject was affected. The infringements in the present case concerns thousands of data subjects, and the illegal processing in question was a part of Grindr's core business model. Compared to the previous fines issued by the NO DPA, the gravity of the infringement in the present case suggests that a high amount is appropriate.

However, we find that a reduction of the amount of the fine previously notified is justified. In particular, we have considered that Grindr's revenue [redacted] and that we find the changes Grindr has made with the aim to remedy the deficiencies in their previous CMP to be a mitigating factor.

---

[122] https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2021/varsel-om-overtredelsesgebyr-til-disqus-inc/
[123] https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2021/varsel-om-overtredelsesgebyr-til-ferde-as/
[124] https://www.imy.se/globalassets/dokument/beslut/2021/2021-06-07-beslut-medhelp.pdf, last visited 7 December 2021.
[125] https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2021/cyberbook-as-far-gebyr/

In light of all the relevant criteria of Article 83 described above in sections 6.3-6.4, we consider that the imposition of a fine of **NOK 65 000 000** is effective, proportionate and dissuasive in the present case.

More specifically, we find this amount to be effective in light of Grindr's very serious infringements of Article 6(1) and Article 9(1) GDPR.

Furthermore, in order to be dissuasive, the fine must be dissuasive both to the controller concerned as well as other controllers carrying out similar processing operations from further engaging in or repeating the conduct concerned. The illegal sharing of personal data for the purpose of behavioural advertisement was part of Grindr's core business model, and this business model is very common in the digital economy. As mentioned, it is important that the administrative fine is not too low in order to ensure a sufficient financial incentive for the perpetrator and other companies in the market to avoid further violations. This underlines the need for the amount of the fine in the present case to be substantial in order to be dissuasive. We find this amount to be dissuasive.

Lastly, this fine is approximately 32 % of the maximum amount of 20 000 000 EUR.[126] [127] We find this fine to be proportionate both to the severity of the infringement and to Grindr's financial situation, and it does not exceed what is necessary to achieve the objectives pursued by the GDPR in the present case.

7. Information on the right to appeal

You may lodge an appeal against the NO DPAs decision. An appeal must be lodged within three weeks after having received this letter, cf. the Norwegian Public Administration Act Section 28 and 29. If you need the deadline for an appeal extended, you need to contact us regarding this before the deadline expires.

If we uphold our decision, we will send the appeal case to Personvernnemnda, our appeal body, cf. the Norwegian Personal Data Act Section 22.

If you do not lodge an appeal against this decision to impose an administrative fine against Grindr LLC, the deadline for paying the fine is four weeks after the end of the time limit for lodging appeals, cf. the Norwegian Personal Data Act Section 27.

[126] Based on the EUR to NOK daily exchange rate 9 December 2021 of 10,155, quoted by Norges Bank: https://www.norges-bank.no/en/topics/Statistics/exchange_rates/, last visited 10 December 2021.
[127] NOK 65 000 000 also amounts to [redacted] of Grindr's turnover for 2020. Based on the USD to NOK daily exchange rate 9 December 2021 of 8,978, quoted by Norges Bank: https://www.norges-bank.no/en/topics/Statistics/exchange_rates/, last visited 10 December 2021.

Kind regards

Bjørn Erik Thon
Data Protection Commissioner

Anders Sæve Obrestad
Senior legal adviser

This letter has electronic approval and is therefore not signed

Copy to: FORBRUKERRÅDET, Finn Myrstad
ADVOKATFIRMAET SCHJØDT AS, Eva Jarbekk