FORBRUKERRÅDET

Datatilsynet
Att. Tobias Judin
P.O. Box 458 Sentrum
0105 Oslo

Oslo, 15/03/2021

SUBMISSION ON THE ADVANCE NOTIFICATION OF AN ADMINISTRATIVE FINE OF 24 JANUARY 2021

In response to the advance notification of an administrative fine issued on 24 January 2021 by the Norwegian Data Protection Authority ('NO DPA') against Grindr LLC ('Grindr'), the Norwegian Consumer Council ('NCC') would like to submit the following observations.

We welcome the NO DPA's draft decision as the NO DPA generally follows the argumentation and the request made in our complaints of 14.01.2020.

We understand that the investigation of the NO DPA has focused on the consent mechanism which had been in place since the GDPR entered into force in Norway (20 July 2018) until 8 April 2020, when Grindr launched a new consent management platform ('CMP'). We also note that to date, the investigation has not assessed whether the subsequent changes made by Grindr comply with the GDPR and we reserve the right to make further submissions on the current CMP.

The NCC also filed complaints against five third parties which received data from Grindr: MoPub (owned by Twitter Inc.), Xandr Inc. (formerly known as AppNexus Inc.), OpenX Software Ltd., AdColony Inc., and Smaato Inc. We understand that these cases are still ongoing and assume that they will lead to further decisions by the NO DPA or by another supervisory authority in charge of those cases.

It follows from the NO DPA's draft decision that Grindr had disclosed the Complainant's personal data (incl. special category data) to third party advertisers without a valid legal basis.[1] While we share this conclusion, we

[1] Advance notification of an administrative fine, 24.01.2021, pp.1-2.

regret that the advance notification only mentions a fine as far as corrective measures are concerned. We fear that a fine as the only corrective measure, without additional order *(e.g.* to disclose the recipients, to stop the processing, or erase the data illegally shared by Grindr) will not be efficient in protecting and enforcing the subjective rights of the Complainant, whose personal data probably continues to be processed by various recipients today.

Therefore, we submit the following remarks to explain how the advance notification could be adapted to fully enforce the rights of the Complainant, to meet the request made by the Complainant in the complaints filed, and to reflect the reality of the processing of data by Grindr:

1. **Erasure of illegally shared personal data by Grindr and all the recipients**

The complaints filed on 14 January 2020 had requested the NO DPA that *"the Respondents are compelled to erase all unlawfully processed personal data without undue delay"*, as per Article 17(1)(d) and Article 58(2)(g) GDPR.
The rights of the individuals will not be effectively protected if the data already shared with the recipients is not deleted and can still be potentially used by the advertising partners who received that data. It is therefore crucial to include an order for the erasure of the data exchanged without a valid consent in the final decision.

Issuing a decision without such an order would send a signal that an illegal data sharing could take place with the sole risk of a fine as the "price" for the illegal data processing. Moreover, the right to erasure is an explicit Complainant's right under the GDPR, the enforcement of which was requested in the complaints. We are therefore concerned that a fine as the only corrective measure would not adequately remedy the violation of the Complainant's rights in this situation.

The final decision should order Grindr to delete all the data shared illegally with the advertising partners, in accordance with Article 17(1)(d) GDPR and point 4.3 of the complaint, in so far as Grindr still processes the said data.[2] As foreseen by Article 19 GDPR, Grindr is obliged to communicate the erasure of the data shared illegally to each recipient to whom the personal data had been disclosed. This obligation is a direct consequence of the requested

[2] It is indeed not excluded that Grindr still processes the data shared with third parties, *e.g.* through a recording of the data shared via the SDKs installed in the application.

erasure of data under Article 17 GDPR and does not require additional requests by the Complainant.

As the advance notification only concerns the processing operations of Grindr and is only addressed to Grindr, we submit that the decision to be issued at a later stage and concerning Grindr's advertising partners includes a similar order to delete the data received illegally as well as a communication of this request of erasure to the further recipients of the data.

2. Violation of Articles 24 and 25 GDPR and consequently of Article 5(2) GDPR

Grindr has shared the Complainant's data with several third and fourth parties. While Grindr claims to have collected the consent for these third parties, it did not implement any technical mechanism to ensure that the choice by the Complainant are communicated and complied with by these parties.

In the advance notification, the NO DPA concludes the breach of Article 5(2) GDPR: *"providing data subjects with information on how they could "opt-out" on their own device is not in line with the principle of accountability in Article 5(2) GDPR"*.[3]

To build on this conclusion, we submit that the violation of Article 5 (2) is even more substantiated by the violation of Articles 24 and 25 GDPR.
Indeed, 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."*

[3] Advance notification of an administrative fine, 24.01.2021, p. 11.

Article 25(2) GDPR provides:

> *"The 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."*

It seems that the only measure that Grindr implemented to prevent the unlawful processing of personal data was the transmission of an 'opt-out' signal to its advertising partners, which could choose to ignore that signal.

Clearly, these signals conveying a data subject's opt-out preference towards partners do not ensure actual compliance with such a signal. It is a mere message and expression of a wish of the data subject, but it does not guarantee necessary 'technical' or 'organisational' protections to ensure that the recipients act upon the receipt of the 'opt-out command'.

Grindr did not demonstrate any other methods of compliance, for example, credible contractual arrangement, combined with internal or external audits or settings in the system to prevent the unauthorised use of personal data. Moreover, no technical or organisational measures were adopted by Grindr to ensure that *by default* personal data are not made accessible to third parties without the individual's intervention.

This is all the more concerning considering that the appropriateness of the measure should be evaluated taking into account the level of risk posed by such data processing.[4] In the case of Grindr, the risk is high because Grindr allows a potentially unlimited number of unauthorised parties to get access to the user's highly sensitive data. The NO DPA makes this point in the advance notification:

> *"Tech companies such as Grindr process personal data of data subjects on a large scale. The Grindr app collected personal data from thousands of data subjects in Norway, and it shared data on their sexual orientation. This enhances Grindr's responsibility to exercise processing with conscience and due knowledge of the requirements for the application of the legal basis on which it relies upon."*[5]

---

[4] Herbst in Kühling / Buchner, *'Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG'*, 2nd edition 2018, 80, p. 232.

[5] Advance notification of an administrative fine, 24.01.2021, p. 26.

We believe it is important to further consider whether participants in the ad-tech environment, such as Grindr, are able to comply with their obligations even in principle.

We believe this is not the case, considering how personal data is shared in a limitless cascade from one company to another.

Finally, it does not seem that Grindr is willing to comply and demonstrate such compliance to take control of what happens with users' data when they 'opt-out' from the personalised ads.

In the response to an order to provide information,[6] Grindr still states:

> *"[I]f interest based advertising is disabled on their device, advertising partners may still serve advertisements to the user on Grindr. However, advertising partners would be instructed (through transmission of the device opt-out signal) not to make those advertisements "interest-based."*[7]

The mere "instruction" is not sufficient and Grindr failed to demonstrate how it ensures compliance with the data subjects' refusal to consent.

Therefore, we submit that the final decision should confirm that Grindr also violated Articles 24 and 25 GDPR – and therefore Article 5(2) GDPR as mentioned – by failing to implement and to demonstrate the implementation of appropriate technical and organisational measures to ensure the sharing of the users' data with the actors of the adtech environment is performed in compliance with the GDPR.

Consequently, we submit that the NO DPA should take into account the violation of Articles 5(2), 24 and 25 along with the violation of Articles 6(1)(a) and Article 9 GDPR already mentioned in the advance notification when calculating the final amount of the fine.

[6] Attachment 1, Grindr's response to Order to provide information: Ref: 20/ 00100-3/ JDY, 22 May 2020. Accessed on basis of the Norwegian Act of Freedom of Information, p. 16.
[7] *Ibidem*.

3. Free, specific, and informed consent requires naming of all the recipients

As the NO DPA has already confirmed in its draft decision Grindr "*disclosed personal data to third party advertisers without a legal basis*".[8] We welcome the NO DPA's assessment[9] of the (in)validity of the consent Grindr relies on and would like to reiterate selected elements of the requirements for valid consent as defined in Article 4(11) GDPR that may be relevant for the NO DPA in making this conclusion:

Need to comply with all cumulative elements

First up, we would like to highlight that Grindr has to comply with all cumulative elements under Article 4(11), 6(1)(a) and 7 GDPR to have a legal basis for the processing operations. The NO DPA has rightfully found that Grindr fails that test on multiple levels, even though just failing one element is sufficient to make the relevant processing unlawful.

3.1. Freely given

As the NO DPA rightly noted, in order for the consent to be 'freely given', it shall be *granular*, ie it should allow for separate consents to be given to different personal data processing operations.[10] This is one of the requirements for a valid consent set forth by the GDPR and formulated in Recital 43 which further clarifies that consent cannot be presumed 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".*

The NO DPA decided that Grindr's consent requests were bundled with other processing operations and other purposes and therefore those consents were not given "freely". 'Granularity' as a requirement for consent to be free was also acknowledged by other Data Protection Authorities (DPAs), for example, the Danish DPA in its decision from 2020[11]:

[8] *Ibidem*, pp.1-2.
[9] *Ibidem*, pp.8-16.
[10] *Ibidem*, p. 9.
[11] Datatilsynet - 2018-32-0357.

> *"An important element in assessing whether consent is freely-given is therefore also the principle of "granularity". The principle means that in the case of processing that serve several purposes, separate consent must be obtained for each purpose. Thus, in data protection law context, the division (granulation) of purposes is essential to ensure the registered control over its information and transparency in relation to which processing operations take place. (...) Thus, it is Datatilsynet's assessment that the collection of personal data for different purposes on the basis of a single consent does not give the visitors a sufficient free choice in relation to being able to identify and opt out or opt out of the purposes for which the visitor really wants to give his consent."*[12] *(emphasis added)*

Another example is provided in the Belgian DPA's recent decision which analysed the element of granularity of consent:

> *"Furthermore, there is no granular nature of the consent. All purposes are becoming aggregated in the communication by the defendant. This limits the control of data subjects about their personal data. Likewise, the categories of the recipients of the personal data not sufficiently clearly defined. Data subjects cannot estimate the impact or nature of passing on their data thus compromising their free choice."*[13]

Granularity is not a new concept: this requirement was already developed by the Article 29 Working Party in 2011.[14] According to the Working Party:

> "*There is a requirement of granularity of the consent with regard to the different elements that constitute the data processing"*[15] and *"a separate and additional consent should be requested to allow for the sending of the individual's data to third parties"*.[16]

[12] Datatilsynet - 2018-32-0357 (automated translation).
[13] APD/GBA - 04/2021, 20.01.2021 (automated translation).
[14] See WP29 Opinion 5/2011 on the definition of consent, WP187.
[15] See Opinion 5/2011, p. 18.
[16] See Opinion 5/2011, p. 19.

It is therefore incontestable that the consent which Grindr attempted to rely on within its former system was bluntly violating the requirement of 'granularity'.

3.1.1. Conditionality

We support the conclusion of the advance notice that the provision of a service should not be made conditional to the processing of their personal data (*ie* the sharing of their data with third party advertisers) when such processing is not strictly necessary for the performance of the contract.

The aim of article 7 GDPR is precisely to prohibit the bundling of agreements where users would have to give their consent to the processing of their data when such processing is not necessary for the performance of the service. The EDPB confirms that *"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"* (see EDPB Guidelines 5/2020, §3.1.2).

Therefore, the mere fact that the Privacy Policy is separate is not a justification for Grindr to avoid the clear terms of this provision: as confirmed by the NO DPA in its advance notification, *"the way Grindr bundled consent with the whole privacy policy does not differ significantly from bundling consent with terms of use".*[17]

This is a shared opinion also amongst the legal commentaries on the GDPR:

> *"The bundling of a service (…) with consent to the use of data, which is not mandatory for the use of this service, also lacks voluntariness. This also results as a legal presumption from Art. 7(4). If consent is required for a contract for a service which is not necessary for the performance of the contract, then in case of doubt it is not voluntary (Art. 7(4)). This is likely to apply in particular to a majority of those online services which, notwithstanding the previous legal situation under the GDPR, have built their business model on the principle of "service for data" and turn the user's data into money by means of targeted advertising offers or the passing on of information. Thus, the reference to a 'free*

[17] See advance notification, p. 10.

offer' is also non-transparent if it actually concerns a 'consideration in data'.

Voluntariness can only be spoken of if the user in such cases can really choose which settings he makes with regard to the disclosure of his personal data. This is not the case if a change is possible but the disclosure of the data is already preset (see recital 32). This applies not only, but especially, if the user finds out about these default settings only with difficulty and changing them is cumbersome. The requirements of Art. 7 will not be met if the data subject is simply asked to "read our data protection provisions". Rather, what is required is an unambiguous notice "We insist on your consent to our use of your data beyond what is required by law" together with transparent information about the scope of this desired use of data."[18]

We would like to add the following points to the ones already raised in the advance notification:

3.1.1.1. The users do not have any other alternative than accepting the Privacy Policy

The advance decision makes clear that the only option for the users to access the app was to accept the privacy policy, since the only other option that had is to press "Cancel". Therefore, access to the Grindr app can only be done by accepting the Terms and Conditions AND the Privacy Policy in the first place. At the time of the registration, there is no other alternative for the users: they have to accept the Privacy Policy, even if they decide to use the paid version later. The consent of the user is therefore not free and conditional to the registration as a user.

3.1.1.2. The users are not offered the possibility to choose between a paid and a free version at the time of registration

At the time of the registration, the users are not given the possibility to opt for a paid version: as said above, the users have to accept the privacy policy to access the app. It is only after being registered that users can decide to

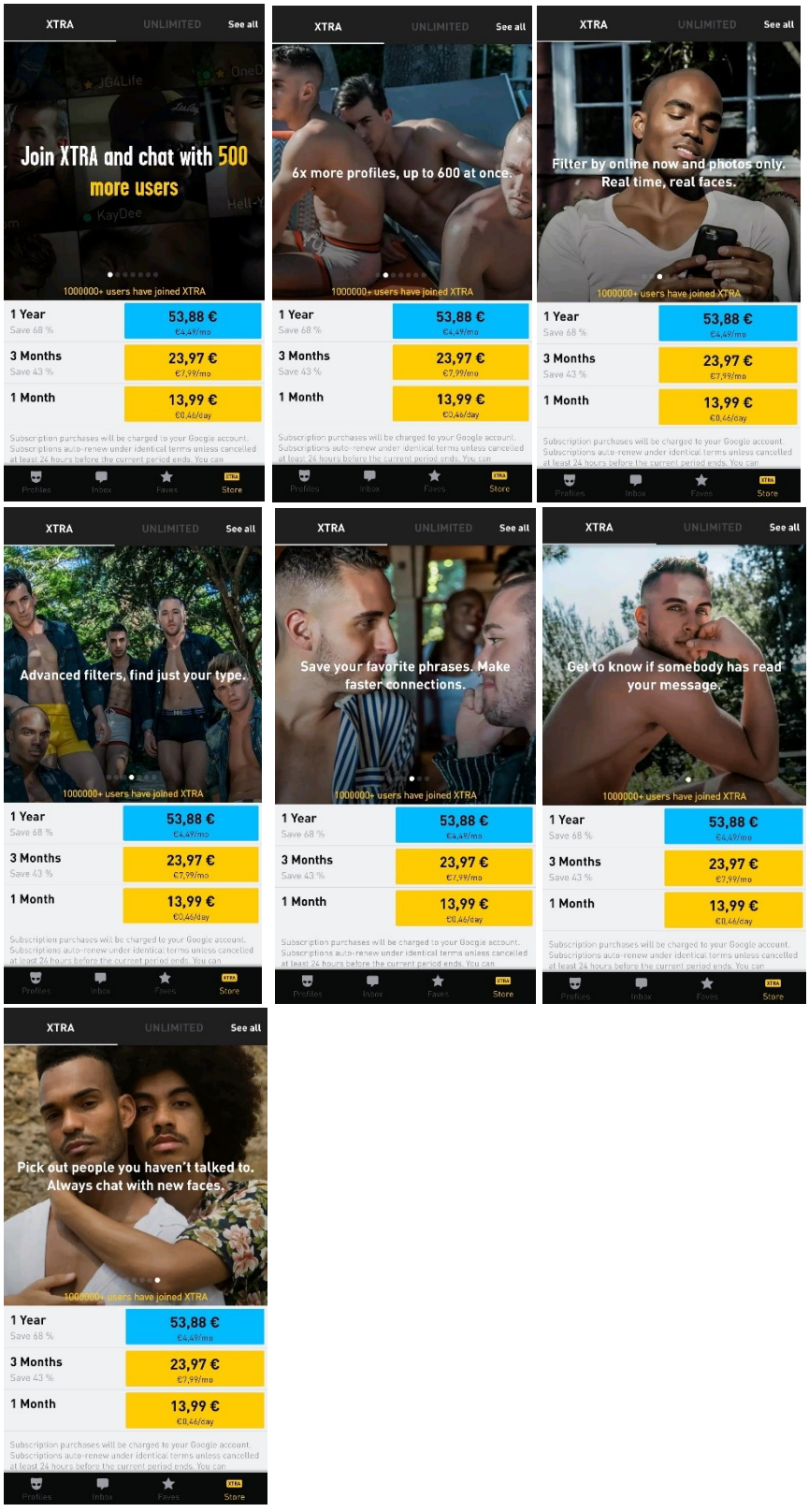
[18] *Ernst* in: Paal/Pauly, DS-GVO BDSG, 3rd ed. 2021, Article 4 para. 73, 74, itself also referencing *Buchner/Kühling* in Kühling/Buchner, DS-GVO, 3rd ed. 2021, Art. 7 para. 50. Automated translation.

upgrade to a paid version of the app. Therefore, we do not see how the existence of a paid version of the app (where personal data is not shared with third parties) would lead to the conclusion that users would have a free and informed choice when accepting the Privacy Policy. Their consent was a forced consent.

3.1.1.3. The paid versions are not advertised as versions "without data sharing": users do not have a "genuine choice"

It appears that Grindr considers that the users are offered a genuine choice, with the reasoning that Grindr offers an upgrade to the paid version which would not share their data by default. However, one should note that the way Grindr advertises its paid versions (Grindr Xtra and Grindr Unlimited) does not put any emphasis of the differences to the free version in terms of data sharing.

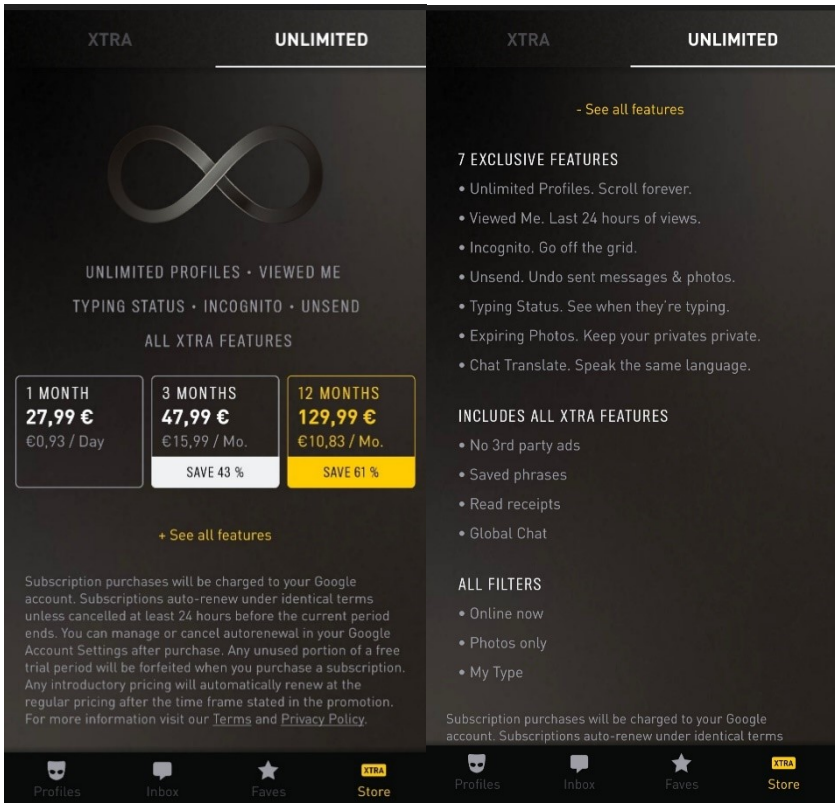
Instead, within the app, Grindr only refers to the following features when advertising the paid version Grindr Xtra, without any mention whatsoever of the absence of data sharing:



Forbrukerrådet

Postboks 463 Sentrum, 0105 Oslo, Org.nr 871 033 382
Telefon 23 400 500, post@forbrukerradet.no

The screens advertising the Unlimited version put emphasis on many extras features, including the asbence of third party ads, but also does not mention that the data of the users would not be shared:



Moreover, in the explanation available on its website, Grindr again only refers – among many other features – to the fact that users would not see third-party ads, but does not make any reference to the sharing of personal data:

What is Grindr XTRA?

Grindr XTRA is a paid version of the Grindr app. XTRA subscribers can enjoy the following additional features:

- No more third-party ads
- View up to 600 profiles in the cascade
- Explore mode / Global Chat
- Premium Filters
    - Online now
    - Photos only
    - Haven't chatted today
    - Height, Weight, Body type
    - Position, Relationship status
    - Meet at
    - Accepts NSFW
- Saved phrases
- Read receipts
- See who chatted with you

What is Grindr Unlimited?

Unlimited is the highest tier Grindr subscription.

Unlimited subscribers get all the In addition to the premium features that come with Grindr XTRA

- No more third-party ads
- View up to 600 profiles in the grid
- Explore mode / Global Chat
- Premium Filters
  - Online now
  - Photos only
  - Haven't chatted today
  - Height, Weight, Body type
  - Position, Relationship status
  - Meet at
  - Accepts NSFW
- Saved phrases
- Read receipts
- See who chatted with you

Plus, Unlimited subscribers have exclusive access to the following features:

- **Unlimited Profiles**—Never run out of people to browse and chat.
- **Viewed Me**—See who's viewed your profile.
- **Incognito**—Browse without being seen.
- **Typing Status**—Know when someone's messaging you.
- **Unsend**—Undo sent messages and photos.
- **Expiring Photos**—Send an unlimited number of photos that can be seen only once for 10 seconds.
- **Chat Translate**—Detects other users' language and translates it for you.

To learn more about Unlimited, Click Here.

Users are led to believe and understand that the paid versions of Grindr will give them the possibility to see more profiles, translate their chats, and send more pictures. Grindr does not inform users that the paid version will stop sharing personal data by default. Grindr does not present the paid version as an alternative for users who prefer that personal data is not shared by default. For these reasons, we support the view of the NO DPA that the consent required by Grindr to access the app must be considered as conditional.

3.1.2. Refusal or withdrawal of consent without detriment

3.1.2.1. The refusal to consent is not without detriment for the users

The advance notice refers to an average price of 360 USD per year to use the paid version of the Grindr app.[19] Considering that the average user may have 20 apps installed (which is a conservative number) and all apps would implement a "pay or okay" approach, this would mean that data subjects would have to spend about 4300 USD (36 190 NOK) per year for the use of all apps installed on their phone, if they do not want to consent to data sharing.

The fact that Grindr users would therefore pay a price (which is not a low price) if they want to choose one of the paid versions precludes any conclusion that the choice of the users would be free and without detriment. It is obvious that consent under such a regime cannot be considered a "freely given", since the price is significant enough to constitute a detriment in the sense of the GDPR.

3.1.2.2. The refusal and withdrawal of consent is in any case detrimental to the user

The Privacy Policy applicable at the time of the complaint[20] referred to the following wording:

> *"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".*

We can therefore not follow Grindr when it states that the users could withdraw their consent without detriment, since the Privacy Policy of Grindr itself confirmed that the users could no longer use the services if they withdrew their consent for the sharing of their personal data with third party advertisers.

Moreover, in the case one would accept that the withdrawal of consent would not be detrimental for the users (which we contest, in line with the arguments

[19] See page 12 of the advance notification.
[20] See Attachment 2 to the complaint.

of the NO DPA), it is obvious that if they do not want to consent to the processing of their data by accepting the Privacy Policy, the user had no other choice than pressing the "Cancel" button on the app.

The fact that the user cannot access the app without accepting the Privacy Policy is beyond any doubt detrimental to the users, since they cannot even access the app and the service.

Therefore, both the withdrawal and the refusal of consent by the users were detrimental to them, since they could not access or continue using the app without giving upholding such consent.

3.1.3. Personal data at stake of the complaint cannot be used as a payment and are not necessary for the performance of the contract

Consent of users to process their data in the context of a free app does not allow the app provider to use the data without meeting the requirements of the GDPR. In this case, the NO DPA made it clear that processing of data for online marketing/ behavioral marketing purposes cannot be considered as necessary for the performance of the contract.[21]

Even if several statements and business models rely on the use of data to monetize their use, that does not mean that the users are left without protection. The GDPR remains applicable to every processing of data, even in a contractual context.

For example, in the case of the Directive "on the provision of digital services"[22], it is made clear that *"this Directive shall be without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC. In the event of conflict between the provisions of this Directive and Union law on the protection of personal data, the latter prevails".*[23]

[21] See page 10 of advance notification.
[22] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services.
[23] See Article 3, 8, §2.

The concept of paying with data has also been strongly criticized by the EDPS.[24] In its Opinion, the EDPS does not deny that some data can be used to create value, but refuses to consider and assimilate this as a payment that would be similar to a traditional payment in currency, using the following terms:

> *"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".*[25]

Therefore, even if data can be used by some organization to create value and even monetized, that does not prevent the GDPR from remaining applicable in all cases. In the case at stake, the respect of the conditions of Article 7 is of the essence in this case since it concerns the specific issue of the processing of data in connection with a contract and aims at prohibiting abuses in this context.

For these reasons, we support the conclusion of the NO DPA according to which the paid version of the app is not a valid and equivalent alternative for users of the free version that refuse to give their consent to the sharing of personal data.

3.2. Specific

The NO DPA concluded that in order for a consent to be specific, the controller must collect a separate 'opt-in' consent for each specific purpose. The NO DPA further concludes that Grindr did not provide separate 'opt-in' for each purpose and had therefore failed to comply with the principle of purpose limitation in Article 5(1)(b) and the requirement of 'specific' consents in Article 4(11).

The requirement that consent must be specific was also spelled out by the CJEU in the *Planet 49* case:

> *"It should be added that the indication of the data subject's wishes (…) must, inter alia, be 'specific' in the sense that it must relate specifically to*

[24] Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, https://edps.europa.eu/sites/default/files/publication/17-03-14_opinion_digital_content_en_1.pdf

[25] See EDPS Opinion 4/2017, §17.

the processing of the data in question and cannot be inferred from an indication of the data subject's wishes for other purposes."[26] *(emphasis added)*

This requirement was recently reiterated by the CJEU in the case *Orange Romania SA*:

> *"Furthermore, Article 2(h) of Directive 95/46 and Article 4(11) of Regulation 2016/679 require a 'specific' indication of the data subject's wishes 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."*[27]

3.3. Informed

The NO DPA concluded that *"the data subjects were not equipped to make informed decisions and understand what they were agreeing to"* because the information about the further processing by the third parties who receive the data from Grindr was not easily accessible.[28]

We agree with the NO DPA that *"The fact that third parties may process personal data further and that this will happen outside of Grindr's control is [in our view] crucial information to the data subject for it to make informed decisions and understand what it is agreeing to"*[29].

The CJEU confirms in the case *Orange Romania SA* that in order for the data subject to make an "informed" choice and understand the consequences of the consent they might give:

> *"(…) the controller is to provide the data subject with information relating to all the circumstances surrounding the data processing, (…), 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. Such information must enable the data subject to be able to determine*

[26] CJEU, C-673/17, EU:C:2019:801, 1 October 2019, paras. 58, 60.
[27] CJEU, C-61/19, ECLI:EU:C:2020:901, 11 November 2020, para. 38.
[28] Advance notification of an administrative fine, 24.01.2021, p. 14.
[29] *Ibidem.*

easily the consequences of any consent he or she might give and ensure that the consent given is well informed."[30]

As was already mentioned in point 1 of this submission, the Complainant could not have possibly known or been able to determine the consequences of Grindr's data sharing with the advertising partners from the 'consent collection method' of Grindr. As the NO DPA mentioned, the possible consequences of this sharing could be *"that over 160 partners could access personal data from Grindr without a legal basis".*[31]

Nothing in the GDPR says that only first layer recipients must be named to have "informed and specific" consent. Article 4(9) GDPR clearly has a global definition of "recipient" that does not differentiate between first, second or third layer recipients. Otherwise it would be easy to add a "proxy" to a data flow in order to camouflage all actual recipients from the data subject.

In fact, Article 28(2) GDPR indicates that with regards to processors and sub-processors, the controller must be aware of each layer in order to be able to exercise its right (and in certain cases duty) to object to their appointment. The GDPR places obligations on the controller and processor in order to protect and empower the data subject. It follows that if the controller is obligated to know about each layer of sub-processors, the data subject must also know about each layer ('information parity').

Regardless of whether the recipients are separate or joint controllers, processors or sub-processors, their involvement not only means that the data subject's personal data are further spread with the subsequent and automatic increase in risk to the personal data. The involvement of certain recipients by itself might also be a reason for the data subject to decide against using certain services – all the more so when the processing itself involves special categories of personal data, the processing of which present a higher risk to the data subject's rights and freedoms.

Also national courts agree with such an approach, for example, the Austrian Supreme Court (*OGH*) already held in 1999 (case no. 7 Ob 170/98 w)[32] that, where consent is sought for a data sharing, all individual recipients must be

[30] CJEU, C-61/19, ECLI:EU:C:2020:901, 11 November 2020, para. 40.
[31] Advance notification of an administrative fine, 24.01.2021, p. 21-22.
[32] https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJT_19990127_OGH0002_0070OB00170_98W0000_000, automated translation.

named in order to meet the requirements of valid consent. Simply stating that personal data may be shared with other "group companies" does not meet the required level of transparency to be "informed". The constituent companies of an internationally active group may change and any changes in the group structure are "completely intransparent" to the data subject. It follows that if the recipients within a group of companies, which theoretically can be a "closed" group, need to be individually mentioned for consent to be valid, then the recipients that constitute a practically 'open' group of 'advertising partners' must all the more so be individually named. The rationale is even more relevant when not a group of companies, but a potentially unlimited number of recipients receives personal data.

The holding of the Austrian Supreme Court is mirrored by the legal literature on the GDPR.

For example, Buchner/Kühling in Kühling/Buchner, DSGVO, Art. 13, para 63 *et seqq*, state that consent being "specific" is an essential part of consent being "informed". Consent that is not specific enough does not permit the data subject to evaluate the consequences of their consent, for example who may all receive the personal data.

Following the CJEU's preliminary ruling in the Planet 49 case, the German Federal Court of Justice (*BGH*) decided on the requirements for a valid consent to telephone advertising and the storage of cookies on the user's terminal device. The *BGH* ruled that the consent does not exist where consumers do not receive full information about the companies which process their data*:*

> *"If the consumer, in the absence of knowledge of the content of the list and without exercising the right of choice, does not know which products or services of which traders the consent covers, there is no consent for the specific case."*[33]

There is also a wide array of decisions available on the matter of consent by the Data Protection Authorities (DPAs) across the EU/EEA[34]. Clearly, there is an agreement across the DPAs that the consent cannot be "informed" if individuals do not understand what they are consenting to or if the consent is hidden in the privacy policy. The ICO has for example confirmed that:

[33] BGH - I ZR 7/16, automated translation.
[34] See for example, Datatilsynet - 2019-431-0018; Datatilsynet - 2018-32-0357; APD/GBA - 04/2021; AEPD - PS/00234/2020 and other.

> *"consent will not be valid if individuals are asked to agree to receive marketing from "similar organisations", "partners", "selected third parties" or other similar generic description."*[35](emphasis added)

As a conclusion, we submit that the final decision should mention that Grindr's consent collection method did not comply with the requirements of "freely given", "specific", and "informed" because Grindr failed to inform the Complainant about and collect a granular, non-conditional, and separate consent to the sharing with each specific recipient of the Complainant's personal data.

We would therefore like to request the NO DPA to include an additional requirement that apart from different processing operations and purposes, the consent that Grindr collected was unlawful because it did not disclose each of the recipients of personal data.

4. On special category data

Grindr has not challenged the fact that its ad calls include information that the Complainant uses Grindr. We refer to our complaint regarding the fact that Grindr described itself as "Grindr - Gay Chat" until today on the Google Play store. It is further uncontested that the use of this app is being broadcasted (together with other information) to potentially hundreds of recipients.

From a legal perspective it should be highlighted that while Article 9(1) GDPR requires data "revealing" certain other characteristics in the first sentence, it only requires data "*concerning a natural persons's sex life or sexual orientation*" in the second sentence. Even when in some of the cases that Grindr tries to bring into play, the use of Grindr may not "reveal" the orientation of a person (for example, when a person may not even know his/her orientation), such data is clearly "concerning" sex life and sexual orientation (e.g. when a straight person is only "curious" about a "Gay Chat").

Just like when a health test produced a false result, the personal data still "concerns" sex life and sexual orientation. Equally, already the "disclosure" of such personal data is considered "processing" under Article 4(2) GDPR and therefore requires a legal basis under Article 9 GDPR.

[35] ICO, 'Monetary Penalty against Decision Technologies Limited', 01.07.2020, para. 38.

Given the facts and the broad wording of the GDPR when it comes to the processing of personal data concerning sexual orientation, the personal data that Grindr shared with third parties in our opinion clearly does fall under Article 9(1) GDPR. Nevertheless, we would like to highlight that the violation of Article 9(1) GDPR constitutes only an additional violation and the processing already lacks a legal basis under Article 6(1) GDPR.

5. Recipients of Complainant's personal data must be provided

The lack of information about the parties with whom the personal data was shared by Grindr constitutes the core of the complaints. This data sharing was described in our report "Out of Control", which formed the basis for the complaints.

However, the advance notification does not mention any order aiming at obtaining information about the recipients of personal data from Grindr.

As was confirmed by the NO DPA in the advance notification, Grindr provided some information on sharing personal data with advertising partners, but it was *"bundled with all other information regarding other processing operations for different purposes.(…) The fact that third parties may process personal data further and that this will happen outside of Grindr's control is in our view crucial information to the data subject for it to make informed decisions and understand what it is agreeing to."* [36]

When explaining the scope of the data sharing with the third parties, Grindr repeatedly evokes *"the privacy policies of these third party companies"*.[37] Grindr relies on the data subjects to check all the privacy policies themselves and find information about further recipients of their data in the said privacy policies.

Clearly, it is unreasonable to expect a data subject to read and check every privacy policy. Even after taking this excessive effort, there is no guarantee that a data subject will get information about further recipients of their

[36] See 5.1.3. of the Advance notification of an administrative fine, 24.01.2021, pp. 13-14.
[37] Attachment 1, Grindr's response to Order to provide information: Ref: 20/ 00100-3/ JDY, 22 May 2020, p. 42. Accessed on basis of the Norwegian Act of Freedom of Information.

personal data as not all of the privacy policies provide an exhaustive list of such recipients.

Grindr claims to disclose more information on the 'Third Party Disclosure' website with *"highly detailed information regarding how user personal data is collected, used, disclosed, and retained"*, including *"the specific entities with whom Grindr shares that personal data"*,[38] but the link provided in the document does not lead to such a page. The main page which automatically opens in the browser does not contain any information about processing by third parties (see Attachment 2).[39] Moreover, the subpage 'Third Parties' of Grindr's latest privacy policy of 8 December 2020, does not provide any more details with regard to the advertising partners than just a list with hyperlinks to those parties' privacy policies.[40]

In any case, under Articles 13 and 14 GDPR, the Complainant should be informed of the actual recipients to whom his data is disclosed. Moreover, Article 19 GDPR ensures that the Complainant gets exactly that specific information ("*The controller shall inform the data subject about those recipients"*) to e.g. review the controller's compliance with the rights of the Complainant.

We therefore request the NO DPA to exercise its powers under Article 58(2)(g) GDPR and order Grindr to inform the Complainant about each of the advertising partners receiving his personal data to fully enforce the Complainant's rights under Articles 13, 14, and 19 GDPR.

6. The fine

Finally, we would like to add, that Grindr does not seem to have ensured that the Complainant's personal data (or indeed any other data subject's personal data) was actually erased internally or at any of the recipients until today, but instead Grindr continues to deny any wrongdoing. This is another aggravating factor under Article 83(2)(c) and (f) GDPR and should be taken into account when calculating the fine.

[38] Attachment 1. Grindr's response to Order to provide information: Ref: 20/ 00100-3/ JDY, 22 May 2020. Accessed on basis of the Norwegian Act of Freedom of Information, p. 13.
[39] www.grindr.com/third-party-disclosure/. See also Attachment 2.
[40] Attachment 3 Grindr's 'Third Parties' section in the privacy policy of 08.12.2020.

The Norwegian Consumer Council remains available to assist with any further factual or legal details the NO DPA may require. We can be contacted at finn.myrstad@forbrukerradet.no

Regards

The Norwegian Consumer Council

Finn Lützow-Holm Myrstad

Director,
Team leader digital policy