FORBRUKERRÅDET

COMPLAINT UNDER ARTICLE 77(1) GDPR

1. PARTIES

1.1. Controllers / Respondents

This Complaint is filed against **Grindr LLC**, PO Box 69176, West Hollywood, CA 90069 – the largest dating app for gay, bi, trans, and queer people (hereinafter "Grindr"). According to their privacy policy, their Article 27 GDPR representative is the DPR Group, The Cube, Monahan Road, Cork, T12H1XY, Republic of Ireland (Attachment 1: "Updated Grindr Privacy and Cookie Policy", 31 December 2019) and (Attachment 2: "Grindr Privacy and Cookie Policy", 3 December 2018)

and

Smaato, Inc., Valentinskamp 70, Emporio, 19th Floor, 20355 Hamburg, Germany, a mobile advertising technology service provider (hereinafter "Smaato"), (Attachment 3: "Smaato Privacy Policy", 16 April 2019).

Note that the complaint relies on the privacy policies that were effective at the time of the alleged infringement, so the period from approximately 1 July to 15 December 2019.

Subject to further submissions by these entities, we assume for this complaint that these companies act as individual controllers.

1.2. Data subject / Complainant

The Complainant and the Data Subject is [redacted], born on [redacted], and residing in [redacted], Norway. The Complainant is a user of the Grindr mobile application with a private account registered under the following e-mail address: [redacted].

The Complainant has mandated us, the Norwegian Consumer Council (further "NCC"; *Forbrukerrådet*), to represent him pursuant to Article 80(1) GDPR (Attachment: "Representation Agreement").

2. FACTS

This complaint is based on the information obtained from the technical testing which was performed by mnemonic on a device running in the technical test environment as explained by us in the attached report (Attachment 5: "Out of Control", section 4) as well as the information derived by the Complainant through a subject access request to Grindr and on the

overview of privacy policies published by Grindr and Smaato on their respective websites. The details of the technical testing, including excerpts of the data, can be found in the attached technical report (Attachment 6: "mnemonic Technical Report").

2.1. Overview

As a part of its free application service, Grindr displays advertising banners in its mobile application ("app"). Grindr also lets third party advertisers collect information about its users, as part of this process. The Grindr app includes SDKs (software development kit – a piece of software that can be incorporated into another software for functional or advertising purposes) from some companies, one of which is **Smaato**.

Since March 2014, Grindr has been using Smaato's mobile RTB ad exchange (real-time bidding – a mechanism whereby advertisers bid to place their ads in a certain online environment, such as an app or a website) and its ad network mediation platform (platform that is directly integrated into apps through a software development kit and which manages ad requests between apps and advertisers) for monetising advertisements (Attachment 7: "Grindr Case Study"). As mentioned above, Smaato was directly integrated into the Grindr app through Smaato's own SDK.

On its website, Smaato describes how a partnership with Grindr provided Grindr with access to more than 337 ad networks and DSPs (demand-side platforms allow buyers of digital ad inventory to manage multiple ad exchanges via one interface. These buyers commonly include trading desks, agencies, or advertisers directly) (Smaato: *'What's the Difference Between an SSP and a DSP?'* [accessed December 18, 2019], https://www.smaato.com/blog/whats-the-difference-between-an-ssp-and-a-dsp/).

The technical testing showed that Smaato was collecting an order of magnitude more requests from the Grindr app than any other third party (Attachment 6: "mnemonic Technical Report", page 30). These transmissions are reflected in Figure 1 (below).

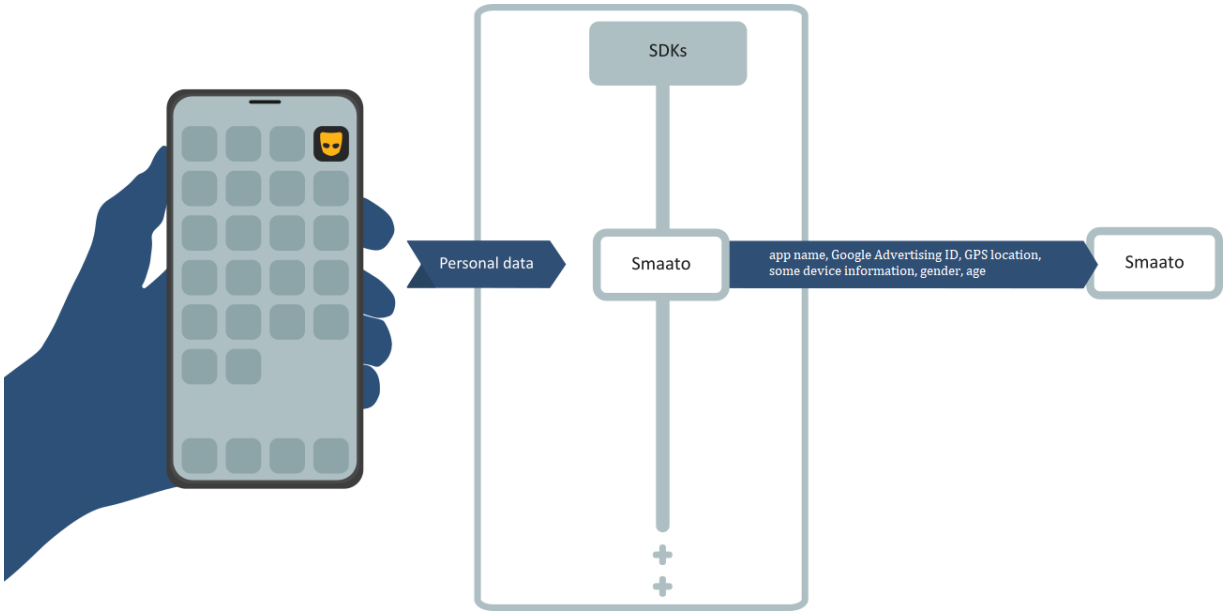

Figure 1 (Illustration of the dataflow from Grindr to Smaato).

2.2. Technical testing by mnemonic

From July–September 2019, we commissioned a technical test of ten mobile apps on Android from the security company mnemonic. The technical tests were performed in Norway to reveal and document data transmissions from the apps to other entities. Additional tests on the Grindr app were performed in mid-September, November and December 2019. All the complexities of the adtech ecosystem for Grindr are presented in the NCC report (Attachment 7: "Out of Control", section 7.1).

The testing showed that the "gay/bi app" Grindr shares user data such as Google Advertising ID, GPS location, gender, age and device information with 3rd party analytics and advertising companies. Grindr therefore monetises personal data by displaying in-app advertising banners in the free version of the app.

Paid versions of the app are supposed not to display advertising (according to Grindr, "*Subscribing users [of Grindr XTRA] can enjoy (...) no banner ads, no interstitial ads*" as per https://help.grindr.com/hc/en-us/articles/115008879108-What-is-Grindr-XTRA). The paid version of the Grindr app is therefore not within the scope of this complaint.

2.3. Personal data processed by Grindr including sharing with Smaato

According to Grindr's privacy policy, the personal data shared with third party advertising companies includes:

> "*your hashed Device ID, your device's advertising identifier, a portion of your Profile Information, Distance Information, and some of your demographic information*" (Attachment 2: "Grindr Privacy and Cookie Policy", 3 December 2018, page 4).

On 21 November 2019, the Complainant submitted an access request ("SAR") to Grindr by e-mail (Attachment 8: "Access Request to Grindr").

Grindr answered the access request by e-mail (Attachment 9: "Grindr Response to the Access Request"). In addition to the e-mail, Grindr attached a copy of some personal data; however, for the purposes of this complaint only the relevant part of this response will be considered and included in the attachments (Attachment 9: "Grindr Response to the Access Request"). Should the authorities require any further parts of the SAR, we are happy to provide them at any time.

In response to the SAR, Grindr stated they process the following categories of personal data: chat message text, chat message images, e-mail address, display name, "About Me", age, height, weight, body type, position, ethnicity, relationship status, "My Tribes", "I'm Looking For", gender, pronouns, HIV status, last tested date, profile picture, linked Facebook data, linked Twitter data, linked Instagram data, location data, IP address, and device ID, such as Google Advertising ID (Attachment 9: "Grindr Response to the Access Request").

Grindr stated it **shares** personal data such as: device identifier (ie Google Advertising ID) ("if allowed by user"), age, gender, and location data with **Smaato**.

The testing showed, that in addition to what Grindr stated they share with Smaato, the Grindr app also sent device information and **app name** to Smaato.

The testing also revealed that the Grindr app passes a 'gdpr_consent' string (the data in the consent string answers the question: 'Which vendors and purposes did the user give consent for?') for processing of this personal data to Smaato. The contents of the decoded consent string indicate that the user (allegedly) consented to the following purposes: (1) information storage and access (2) personalisation; (3) ad selection, delivery, reporting; (4) content selection, delivery, reporting; and (5) measurement. The admissible vendors are: Oath (EMEA), OpenX, Smaato, Inc., and Mobfox US LLC. Mnemonic did

not look any further into any collaboration between these parties (Attachment 6: "mnemonic Technical Report", page 32).

2.4. Personal data processed by Smaato

In the privacy policy, Smaato explains that it processes two types of information. One is the information Smaato receives about end users of third-party mobile applications that use Smaato's SDK, other collection interfaces (collectively, "APIs"), the Smaato Demand Platform ("SDX"), or the Smaato Publisher Platform ("SPX") (collectively, the "Smaato Ad Services"). The second type is the information Smaato receives through their corporate website at www.smaato.com (Attachment 3: "Smaato Privacy Policy", page 1).

This complaint focuses on the processing of the first type of information – personal data received through the Smaato Ad Services. Smaato acknowledges that the data mentioned above are "personal data" in their privacy policy (Attachment 3: "Smaato Privacy Policy", pages 9-10).

As mentioned in subsection 2.3, through their integration in the Grindr app, Smaato receives the **app name**, Google Advertising ID, GPS position (location data), gender, age, device information and a "gdpr_consent" (Attachment 6, "mnemonic Technical Report", page 31).

3. LEGAL ANALYSIS

The subject matter of the complaint is unlawful sharing of user's personal data between the Grindr app and Smaato. Grindr and Smaato process personal data without a valid legal basis under Article 6 and Article 9 GDPR.

Introduction

Consent plays a central role in informational self-determination, as it allows data subjects control over whether or not personal data concerning them will be processed.

Indeed, for the processing of personal data for advertisement purposes in the adtech ecosystem, consent is the *only* possible legal basis (as also supported by ICO, "*Update report into adtech and real time bidding*, 20 June 2019", page 18).

One of the main objectives of the GDPR is to stop the frivolous gathering of alleged consent in all shapes and forms by controllers – such as the current practice by Grindr, which will be analysed in this complaint.

Consequently, this complaint focuses on consent, which, in the present case, does not exist - and even if it is assumed otherwise - does not satisfy any of the GDPR criteria.

3.1. Source “Grindr” makes all personal data fall under Article 9

The fact that the data is collected from Grindr and linked with the source **app's name** is a clear indication of the user’s sexual orientation.

The Grindr app is a known online dating app geared **exclusively** towards gay, bi and trans people, as admitted by Grindr in its own statements (Figure 2). As such, any personal data that can be traced back to Grindr concerns the user’s sexual orientation and thus falls under “special categories” of data under Article 9 GDPR.

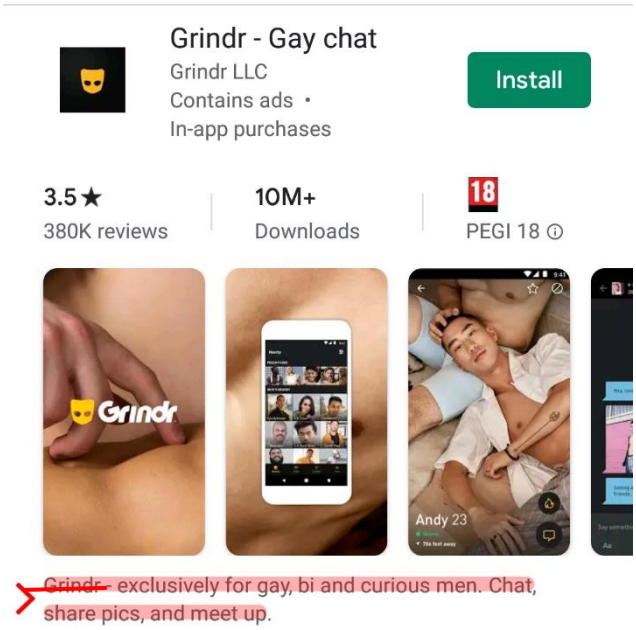

Figure 2 (Grindr app in Google Play - highlighting added).

The processing of such data is clearly prohibited under Article 9(1) unless one of the exceptions exhaustively listed in Article 9(2) is met. In the case of the Respondents, the explicit consent to process the special categories of data remains the only realistically possible lawful exception to process such data.

3.2. Burden of proof

Article 6(1) GDPR imposes a general prohibition of any processing operation unless the controller can demonstrate that it complied with one of its requirements. Article 7(1) GDPR further highlights the specific obligation on the controller to demonstrate valid consent.

The burden of proof to demonstrate that the processing operation is lawful and that valid consent was obtained is hence placed on the controller, not the Supervisory Authority or the data subject.

3.3. Analysis of legal bases

As a matter of procedural precaution, we start this analysis with a brief explanation why other legal bases which Smaato randomly refers to in their privacy policy cannot be relied upon for the named processing operations. Their privacy policy states that it relies on legitimate interest, performance of a contract, legal obligations, and consent (Attachment 3: "Smaato Privacy Policy", page 10).

For legitimate interest, Smaato states:

1. *"**In some cases**, we rely on legitimate interest as a legal basis for processing Personal Data, in order to provide our and/or other data controllers' services. Such processing goes beyond the original collection of Mobile IDs. A legitimate interest we rely on, **for instance**, is the tailoring of promotional communications within mobile apps and services, which is beneficial to End Users and is an integral part of the ecosystem by which freely available content is funded through advertising revenue. This also **may include** providing analysis of and reporting about ad campaigns. We also rely on legitimate interest when we use Personal Data to maintain the security of our services, **such as** to detect fraud or to ensure that bugs are detected and fixed;"* (Attachment 3: "Smaato Privacy Policy", page 10. Emphasis added.)

The analysis of this legal basis is performed in section 3.3.1.

For performance of a contract, Smaato states:

2. *"**Sometimes**, we process certain data as necessary under a contractual relationship we have (**such as** our customer records and contact information);"* (Attachment 3: "Smaato Privacy Policy", page 10. Emphasis added.)

The analysis of this legal basis is performed in section 3.3.2.

Regarding processing because of legal obligations, Smaato states:

3. *"**some processing** of data **may be** necessary for us to comply with our legal or regulatory obligations."* (Attachment 3: "Smaato Privacy Policy", page 10. Emphasis added.)

We do not analyse this legal ground; it is clear that Smaato cannot rely on it for the sharing of data for advertising purposes. There is no such legal obligation in any jurisdiction we are aware of.

For consent, Smaato states in its privacy policy that they

> *"rely on mobile app developers and oblige them contractually to pass on only legally obtained data."* (Attachment 3: "Smaato Privacy Policy", page 10)

The analysis of this legal basis is performed in section 3.3.3.

3.3.1. Lack of any overriding legitimate interests

Smaato claims to have a legitimate interest under Article 6(1)(f) GDPR to process special categories of personal data stemming from Grindr. Smaato states that *"in some cases"* they rely on the legitimate interests for instance to "*[tailor] promotional communications within mobile apps and services*" (Attachment 3: "Smaato Privacy Policy", page 10). However, the precise extent of the processing based on legitimate interests by Smaato is unclear.

Processing of personal data may be based on the controller's "legitimate interest" under Article 6(1)(f) GDPR, provided that the personal data does not concern any of the categories listed in Article 9.

The personal data being processed concerns the user's sexual orientation. It must therefore fulfil the obligations required under Article 9 for the processing operation to be legal.

Under Article 9, the only available legal ground to process the data is on the basis of explicit consent. Processing the personal data on the basis of legitimate interest does not satisfy the requirements that follows from Article 9.

As such, processing the special categories of personal data on the basis of legitimate interest is illegal under the GDPR.

***In the alternative*: Online Tracking is not a "legitimate interest"**

If the supervisory authority should find that the personal data is not covered by the special protections afforded by Article 9, we maintain that the processing cannot be based on the controller's legitimate interest under Article 6(1)(f).

Some controllers rely on the false assumption that any processing for advertisement constitutes "direct marketing", and as this is mentioned in the non-binding Recital 47 as a situation that "*may*" be regarded as a legitimate interest, that any advertisement is allowed under Article 6(1)(f):

> "*[t]he processing of personal data for direct marketing purposes* ***may*** *be regarded as carried out for a legitimate interest*" (emphasis added)

The qualification of "*may*" to the processing of personal data for the purpose of "direct marketing" reflects that direct marketing was seen as an "edge" case by the legislator where the interest of the data subject or controller *may* or *may not* prevail. Data sharing for targeted online advertisement can however never fall under Article 6(1)(f) GDPR for at least the following reasons:

First, targeted online advertisement cannot at all be compared to "*direct marketing*".

Article 13(2) of the e-Privacy Directive 2009/136/EC allows direct marketing under the conditions that:

(1) the data was obtained from an existing customer by a single company,
(2) in the context of a previous sale and
(3) in line with Directive 95/46 (now GDPR).

If these conditions are met, Article 13 only allows:

(1) the use of electronic contact details (like an email address) to,
(2) promote similar products and services,
(3) if the data subject can opt-out at any time.

This is wholly different form a *targeted online advertisement and tracking* ecosystem,

(1) where one company forwards data to third parties, that in turn forward that data to hundreds of further advertisement firms with no existing relationship,
(2) where the companies gather hundreds of personal details (like personal preferences or tracking IDs) and not just contact details (like an email address) and
(3) where this personal data is used to promote any product or service of any unrelated company in the world.

In summary, the targeted online advertisement and tracking ecosystem could not be further away from "direct marketing" as traditionally understood. Nothing of this vast system of user tracking and data flows

among hundreds of companies can be compared to a simple postal mailing or email newsletter in an existing relationship between a customer and a business.

As the legislature was already not decisive if the traditional form of direct marketing (as defined in Article 13 e-Privacy Directive) can be seen as a legitimate interest ("*may be regarded*" in Recital 47), it is beyond a doubt that this highly intrusive form of an unregulated "online tracking and advertisement data market" with potentially data sets on millions of people and thousands of recipients globally can (in any way shape or form) constitute a "legitimate interest" that would override the fundamental right to data protection of the data subject.

Second, even if this online tracking and advertisement data market would constitute "direct marketing", all the other elements in Recital 47 would not be fulfilled: Smaato has neither an existing relationship with the data subject, nor has the data subject any reasonable expectation when he creates an account on the Grindr app that a company he has never heard of will get personal data from his Grindr use.

Third, when balancing the interests, the interest of Smaato in slightly increasing the click rate on online advertisements in comparison with non-targeted or contextual ads has to be considered a rather minimal interest in additional profit. According to the latest studies from the US, personalized advertisements leads to only about 4% more revenue for publishers (https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf). After all Grindr may simply have a slightly smaller profit when advertisements are served without the use of personal data (but instead based on language, time, rough location, context of the app and alike). Grindr mainly generates revenue from the paid "Grindr xtra" and "Grindr Unlimited" (€42,99 per month) version of the app, while the free Grindr version serves as a "Freemium" preview of the actual paid product. In the overall business model of Grindr, the additional profits from personalized advertisements are clearly trivial.

At the same time the personal data gathered by Grindr and transferred to Smaato is highly sensitive and concerns one of the most intimate aspects of human activity, something few users would expect to be harnessed for the aim of serving them advertisement. In an overall balancing of interests (in light of the principle of proportionality in Article 52(1) of the Charter of Fundamental Rights), it is impossible that the interest of Grindr or Smaato would therefore override the fundamental right to data protection of the complainant.

The GDPR would not be worth the paper it is written on, if the aim of a controller to merely increase profits through the use and trading of personal data would override the interests of data subjects.

Fourth, the same result can be derived, when this case is compared to the other legitimate interest named in Recital 47 or 49, like the use for data security or for combating fraud or to the CJEU case law on overriding interest: if e.g. Member States' interests in combating terrorists was not overriding the interests in telephone metadata (see C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger*) it is hard to conceive that a private entity like Smaato would have an overriding legitimate interest in tracking similar communication data merely for better targeting advertisements.

Fifth, the Article 29 WP emphasize in their *Opinion 06/2014* (WP217) on legitimate interests that the business model of adtech cannot rely on "legitimate interests":

> *"to unduly monitor the on-line or off-line activities of their customers, combine vast amounts of data about them from different sources that were initially collected in other contexts and for different purposes and create – and for example, with the intermediary of data brokers, also trade in – complex profiles of the customers' personalities and preferences without their knowledge, a workable mechanism to object, let alone informed consent. Such a profiling activity* ***is likely to present a significant intrusion into the privacy of the customer****, and when this is so, the* ***controller's interest would be overridden by the interests and rights of the data subject***" (page 26, emphasis added)

This view is endorsed by the EDPB in *Opinion 5/2019* on the interplay between the ePrivacy Directive and the GDPR, which reference the Article 29 WP and state that:

> "*Instead of merely offering the possibility to opt out of this type of profiling and targeted advertisement,* ***an informed consent would be necessary****, pursuant to Article 7(a) but also under Article 5(3) of the ePrivacy Directive.* ***As a consequence, Article 7(f)*** **[now Article 6(1)(f) GDRP]** ***should not be relied on as a legal ground for the processing***" (page 22, emphasis added).

The information Commissioner's Office (ICO) similarly endorse the view of EDPB and the Article 29 WP in their *Update report into adtech and real time bidding,* 20 June 2019 stating:

> "*Overall, we do not believe there is a full understanding of what legitimate interests requires. In our view, the only lawful basis for 'business as usual' RTB* [Real-time bidding] *processing of personal data is* ***consen****t.*" (page 18, emphasis added) and "*Our work has established that, at present, some parts of the adtech industry are unaware of this advice.*" (page 19).

The Dutch data protection authority, *Autoriteit Persoonsgegevens*, recently stated that legitimate interests cannot be relied on when the processing operation pursues purely commercial interests; profit-maximisation and tracking (potential) customers (as seen on https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/mag-u-persoonsgegevens-verwerken#hoe-toetst-u-of-u-zich-mag-baseren-op-de-grondslag-gerechtvaardigd-belang-7531).
Smaato's business model is based on the mass sharing of personal data to serve advertising. This does not mean that legitimate interests can be relied on as a legal basis for the vast processing of personal data that underpin their business model.

In conclusion, Smaato cannot rely on legitimate interests as a legal basis for processing personal data.

3.3.2. No contract over advertisements

Smaato bears the burden of proving the existence of a "contract" as defined in Article 6(1)(b) GDPR and in the applicable civil law and in any case, the complainant has never concluded any contract with Smaato.

The only possible party with which the complainant could have a relevant contract is with Grindr, but the terms of service of Grindr do not mention any duty of Grindr to serve ads or a right of the user to receive these ads (Attachment 10: "Grindr Terms of Service"). The placement of advertisement is therefore a merely factual act by Grindr, as the owner of the app (just like the placement of an advertisement on a house, with the agreement of the owner) not a contract under Article 6(1)(b) GDPR.

3.3.3. Lack of a valid consent

When consent is relied on, both Grindr and Smaato rely on the consent collected in the Grindr app. The Grindr app seems to transmit or "pass" the collected 'gdpr_consent' to Smaato together with other personal data (see section 2.3). In order to analyse the lawfulness of the processing based on such consent, we analyse how Grindr collects consent from users.

3.3.3.1. Grindr confuses consent under Article 6(1)(a) with information under Article 13

Grindr believes that by agreeing to the privacy policy they are soliciting valid consent ("*By agreeing to our privacy policy, you consent to the collection of the information indicated below*" (Attachment 2: "Grindr Privacy and Cookie Policy", page 1)). However, a privacy policy is not intended to solicit consent, but to provide information required under Article 13 GDPR.

When opening the app for the first time, users are asked to accept an approximately 3,793 words long Privacy and Cookie Policy document that takes about 37 minutes to read on a small cell phone screen. Upon consenting to the Privacy and Cookie Policy, users are asked to accept another lengthy document, the Terms and Conditions of Service, which is approximately 28 A4 pages-long (11,315 words) and takes an additional about 1h50min to read on a small screen. As a dating app for *"millions of daily users"* who install it to satisfy their urgent need for socialising, it is unrealistic to assume that a user will spend over 2h on reading the overwhelmingly lengthy conditions on a mobile phone.

Indeed, such a method to obtain consent is unlawful and does not satisfy the conditions for valid consent. For one, Article 7(2) GDPR requires that consent must be clearly distinguishable from other written information (such as privacy policies under Article 13); any "bundled" consent given as part of such a broader written declaration as a general privacy policy is not binding.

3.3.3.2. Consent is not freely given

As the screenshot below demonstrates, Grindr uses the wording "ACCEPT" or "CANCEL" as the only two possible options within its app. The data subjects therefore have no real choice but to consent to the privacy and cookie policy and to the terms and conditions of service. In particular, when they click "CANCEL", further registration is impossible. If a user wants to have access to the service, they have to consent to the conditions described in the Privacy and Cookie Policy in their entirety ("*take it or leave it*"). Grindr therefore makes the provision of its service dependent on the consent and the user is deprived of a genuine and realistic choice to accept or decline the terms of a service without detriment.

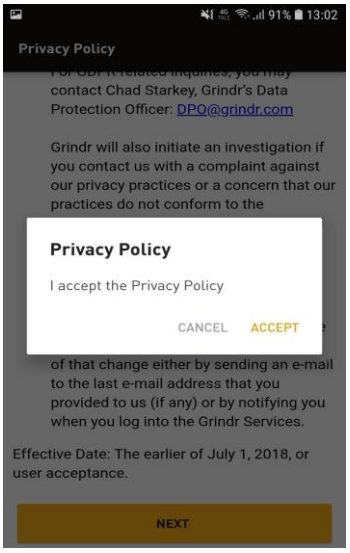

Figure 3 (Privacy and Cookie Policy).

The 'core' element of consent is the fact that it must be freely given, as clarified in Article 4(11) GDPR and further specified in Article 7(4) GDPR. Furthermore, Recital 43 GDPR provides 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, or 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."*

Furthermore, the Article 29 WP *Guidelines on consent under Regulation 2016/679* (WP259 rev.01) from 10 April 2018, endorsed by EDPB on 25 May provide:

> *"If a controller is able to show that a service includes the possibility to withdraw consent without any negative consequences e.g. without the performance of the service being downgraded to the detriment of the user, this may serve to show that the consent was given freely (...)."* (page 11)

In this case, not only is the provision of the service impossible without a consent, but in case of the withdrawal of the consent, Grindr informs users*:*

> *"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"* (Attachment 2: "Grindr Privacy and Cookie Policy" page 6).

This brief paragraph reveals a two-fold violation by Grindr. For one, Grindr does not permit an Article 7(3) GDPR withdrawal of consent because the provision of the services is conditional on the consent being granted, which, for another, is a violation of the provision Article 7(4) GDPR.

3.3.3.3. Dominant Market Position of Grindr

Recital 43 GDPR further clarifies:

> *"Consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller (…) and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation."*

Although the Recital mentions authorities as an example of where such an imbalance may be found, it does not exclude other situations where a similar imbalance of powers between the controller and the data subject might arise, including situations where controllers are private corporations (Article 29 WP *Guidelines on consent under Regulation 2016/679* (WP259 rev.01):

> *"Imbalances of power are not limited to public authorities and employers, they may also occur in other situations. As highlighted by WP29 in several Opinions, consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences (e.g. substantial extra costs) if he/she does not consent. Consent will not be free in cases where there is any element of compulsion, pressure or inability to exercise free will."* (page 7)

If a controller is in a dominant position that creates an imbalance of power between him and the data subject, then this is likely to affect the voluntariness of the latter's consent.

Grindr admits that their app is "the world's largest social networking app for gay, bi, trans, and queer people" (see Figure 4 below).

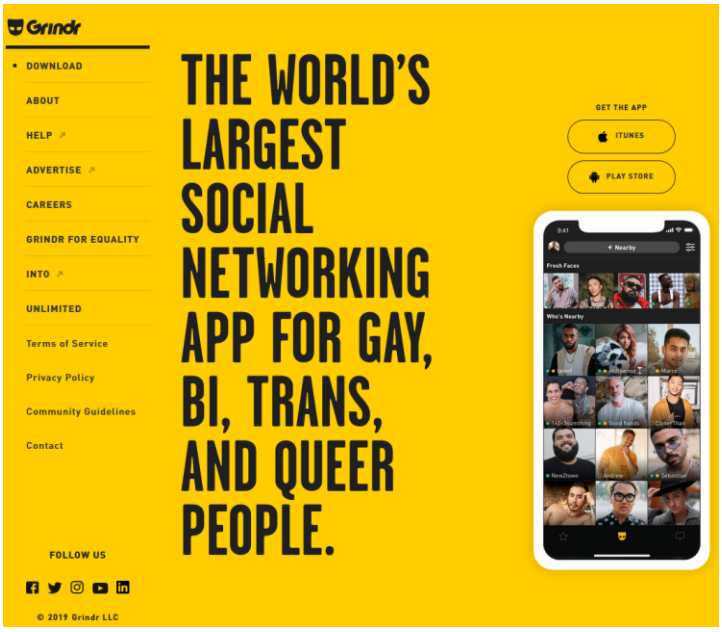

Figure 4 (Frontpage of grindr.com).

3.3.3.4. Lack of specific consent

Article 6(1)(a) GDPR provides that the consent of the data subject must be given in relation to *"one or more specific"* purposes and that a data subject has a choice in relation to each of them.

Grindr requires the user to consent to its privacy and cookie policy and the terms as a whole. This bundling of consent to the other provisions of the terms renders consent invalid because the consent is not in any way "specific". It is rather based on an "*all or nothing*" approach, which clearly does not comply with the GDPR. For example, Grindr makes the user consent to such varied processing purposes as *"provide products and services; improve the Grindr Services; partner promotions; marketing and advertising"*

etc. (Attachment 2: "Grindr Privacy and Cookie Policy" page 3). Moreover, in its response to the SAR, Grindr provides for only one overly broad purpose for the processing of all the personal data described in the SAR, namely "User Services" (Attachment 9: "Grindr Response to the Access Request").

Article 29 WP provides that *"consent must be specific to the purpose"* and in cases when a *"controller seeks consent for various different purposes [it] should provide a separate opt-in for each purpose, to allow users to give specific consent for specific purposes."* (Article 29 Working Party *Guidelines on consent under Regulation 2016/679*, (WP259 rev.01), page 12).

3.3.3.5. Lack of informed consent

Consent should also be "informed". This means that the information should be provided to the data subject before the collection of the consent, and that the information must be complete and understandable. As already explained in 3.4.3.1., the windows with Grindr's Privacy and Cookie Policy and the Terms and Conditions of Service pop up before consent is granted and contain a very long text that is difficult to read.

There are many ways to improve readability of complex documents. For example, Article 29 WP *Guidelines on transparency* (WP260 rev.01) states:

> *"The requirement for clear and plain language means that information should be provided in as simple a manner as possible, avoiding complex sentence and language structures. The information should be concrete and definitive; it should not be phrased in abstract or ambivalent terms or leave room for different interpretations. In particular the purposes of, and legal basis for, processing the personal data should be clear."* (pages 8-9).

The complainant was "factually uninformed" about the fact that his data will be processed for advertisement and disclose to third parties as described above. The lack of information makes any form of consent equally invalid.

3.3.3.6. Lack of unambiguous indication of wishes

GDPR consent requires a statement from the data subject or a clear affirmative act, which means that it must be given through an active motion or declaration. Article 29 WP *Guidelines on Consent* (WP259 rev.01) states:

> *"It must be obvious that the data subject has consented to the particular processing. (...) A "clear affirmative act" means that the data subject must have taken a deliberate action to consent to the particular processing. (...) A controller must also beware that consent cannot be obtained through the same motion as agreeing to a contract or accepting general terms and conditions of a service. Blanket acceptance of general terms and conditions cannot be seen as a clear affirmative action to consent to the use of personal data"* (, pages 15-16).

It is obvious that the way Grindr solicits consent in no way provides for a chance to distinguish between "consenting"/ "agreeing" to the terms and "consenting" to a (specific) processing of personal data (see Figure 3 on page 12).

3.3.3.7. Lack of explicit consent

The processing of any personal data received from Grindr reveals "special categories of data" under Article 9(1) GDPR. The indication of the source of the personal data (the app name) enriches any personal data transmitted with information about the data subject's sex life or sexual orientation. It is not necessary that Grindr directly discloses a user's sex life or sexual orientation. The origin of the personal data as coming from Grindr is sufficient to indicate that it concerns the data subject's sex life / sexual orientation.

Even if the Supervisory Authority would take the view that the consent would be "unambiguous" (as required under Article 6(1)(f) GDPR), it definitely does not fulfil the requirements of the "explicit" consent (as required under Article 9(2)(a) GDPR).

The requirement under Article 9(1) GDPR is merely that the processing of personal data should *"concern"* a natural person's sex life or sexual orientation. It is therefore not necessary that the data processed is directly in and of itself special.

According to Article 29 WP *Guidelines on Consent* (WP259 rev.01):

> *"The term explicit refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent"* (page 18).

The personal data that was observed in the transmissions does not as such constitute special categories of data, but it becomes one when it is combined with the app name or keywords describing the app and is disclosed to third parties. If those third parties rely on the consent from Grindr, that consent should fulfil all the criteria under Article 6(1)(a) and Article 9(2)(a) GDPR.

3.4. Conclusion

In conclusion, the consent collected by the Grindr app does not constitute a valid consent and as such infringes all the requirements set out in Article 4(11), Article 6(1)(a), Article 7 and Article 9(2)(a) of the GDPR, as well as all elements identified by the Article 29 Working Party Guidelines. The consequence is that the processing of the personal data on the basis of the

invalid consent by Grindr and Smaato is unlawful and breaches the rights of the data subject under the GDPR.

In addition to the lack of a valid consent, Smaato cannot rely on legitimate interests or performance of a contract for their processing operations. The scope of the unlawful processing could therefore cover all the personal data processed by third parties, as well as the processing operations by Grindr where they rely on consent as the legal basis.

4. APPLICATIONS

4.1. Request to investigate and to disclose information

The Complainant hereby requests that you fully investigate this complaint, in accordance with the powers vested in you, including by Article 58(1)(a), (e) and (f) GDPR, to determine:

i. which processing operations the controllers engage in, in relation to the personal data of the data subject, inter alia through the record of processing activities (RoPA) of all the controllers and their data protection representatives,
ii. for which purpose they are performed,
iii. which legal basis for each specific processing operation the controllers rely on.

Finally, the Complainant would like to request that any results of this investigation are made available to us in the course of this procedure, in accordance with Article 77(2) GDPR and the right to be heard under the applicable national procedural law.

4.2. Request to handle the complaint locally

The Complainant requests that the complaint is handled by the Supervisory Authority in Norway for Grindr and Smaato.

4.3. Request to compel the controller to erase all the personal data and stop the processing

The Complainant also requests that the Respondents are compelled to erase all unlawfully processed personal data without undue delay (Article 17(1)(d) GDPR) and to prohibit the relevant processing operations in accordance with the powers vested in you, including by Article 58(2)(d), (f), and (g) GDPR.

4.4. Request to impose an effective, proportionate and dissuasive fine

Finally, we request that you (or the relevant supervisory authority), by virtue of the powers provided by Article 58(2)(i) in combination with Article 83(5)(a) GDPR, impose an effective, proportionate and dissuasive fine against the controllers, taking into account that:

i. the gravity of the infringement, considering that the lawful processing is the cornerstone for the fundamental right to personal data protection (Article 83(2)(a) GDPR);
ii. the Respondents wilfully and intentionally violated the law, by founding its business models on abusing consumers' rights and on processing personal data without a legal basis (Article 83(2)(b) GDPR);
iii. the Controllers process highly sensitive data, including special categories of personal data (Article 83(2)(g) GDPR);
iv. a wilful, massive and profound violation by major players within the data industry must be adequately sanctioned to prevent similar violations of the GDPR in the future, and to ensure respect of the consumers' rights under the new data protection acquis.

We request the maximum possible fine under Article 83(5)(a) GDPR, that is the higher of 20 million euros or 4% of the worldwide annual turnover of **Grindr**. We were unable to calculate the fine based on the 4% because the company's turnover is not publicly available.

We request the maximum possible fine under Article 83(5)(a) GDPR, that is the higher of 20 million euros or 4% of the worldwide annual turnover of **Smaato**. We were unable to calculate the fine based on the 4% because the company's turnover is not publicly available.

5. OTHER

5.1. Contact details

We are happy to assist you with any further factual or legal details you may require to process this Complaint. Please contact us at gmm@forbrukerradet.no.