

Datatilsynet
Att. Atle Årnes
post@datatilsynet.no

Oslo, 3 April 2018

Complaint against Grindr for breaching data protection law

The Norwegian Consumer Council are filing a complaint against the mobile application Grindr, for breaching data protection law.

The Consumer Council has looked at the terms of service and the privacy policy for downloading and using the app. Furthermore, we have looked at how the application asks for consent to the processing of personal data when a user account is created in the app.

Documentation:

- The published report from the technical test by the Norwegian research institute SINTEF: "Privacy and Privacy leaks in Grindr" on GitHub, including raw data documentation¹.
- The privacy policy for the app dated August 9. 2017².

In general, the Consumer Council ask the enforcement authorities to look at the technical documentation and privacy policy, and consider whether there are issues within that constitute a breach of the personal data protection act.

In this complaint, we have pointed to some issues from the background material that we regard as particularly disconcerting, and we therefore ask that these issues are considered.

About the app Grindr and the investigations

Grindr is, according to themselves, «The world's largest social networking app for gay, bi, trans and queer people»³. The app is quite popular, having more than 10 million downloads in Google Play Store. According to the website

¹ <https://github.com/SINTEF-9012/grindr-privacy-leaks>

² <https://www.grindr.com/privacy-policy>

³ <https://www.grindr.com/>



Gaysir, Grindr had around 2 million daily users in 2016, and is also a popular app in Norway⁴.

The investigation of how Grindr gathers user consent was done by downloading the app from Google Play, on an Android-based mobile phone.

The terms of service and privacy policy was found through Google Play.

The technical analysis done by SINTEF was performed in Sweden on commission from the Swedish TV channel TV2.

How the app works

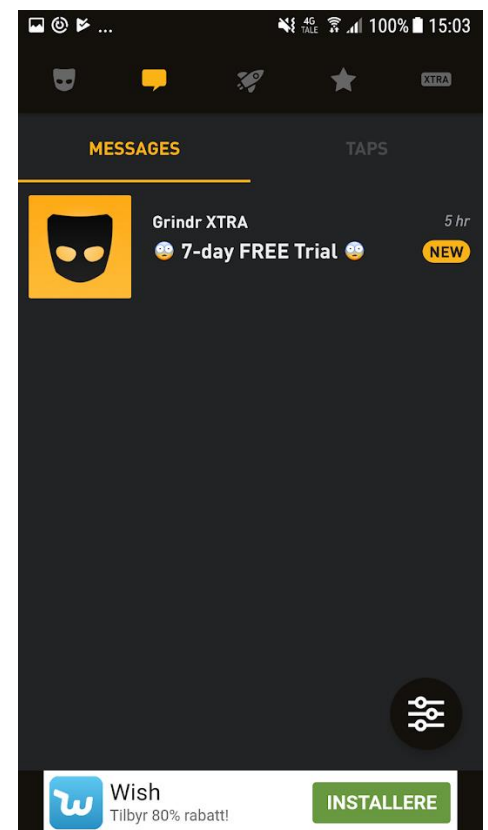
In order to use the app, one first has to register a user account.

When registering a user account on Grindr, the user can voluntarily choose to register information about themselves, for example a profile picture, username, sexual orientation, and HIV-status (defined by Grindr as «Profile Information»). In the privacy policy, Grindr states that “Profile Information” is shared with other users as a part of the core functionality of the app, similarly to how names and pictures are shared with other users in social media services such as Facebook. The user can also choose to register their “tribe” (group-affiliation, for example “trans”), and sexual preferences.

It is also possible to share your geolocation, which is then used to get in touch with other users of the app in your near vicinity. This option is turned on by default.

Grindr has an advertising-based business model, in addition to premium memberships, and displays advertisements in the app interface.

The attached screenshot from Grindr displays an advertisement banner for the online store Wish.



Grindr point of contact

The Consumer Council have not been able to find a European point of contact for Grindr.

⁴ <https://www.gaysir.no/artikkel.cshtml?cid=17218>



As far as the Consumer Council are able to see, Grindr only provides an electronic point of contact through an online form on their website.⁵

The address listed in the terms of service is:

Grindr LLC
PO Box 69176
West Hollywood, CA 90069

Points of complaint

Information about sexual orientation and health status are sensitive personal data according to European legislation. Grindr processes sensitive personal data, such as HIV-status, sexual orientation, and sexual preferences. This complaint concerns how Grindr shares and protects these sensitive personal data.

The points of complaint that the Consumer Council particularly asks the enforcement authority to look at are described below, and SINTEF's GitHub post and Grindr's privacy policy are referenced for further documentation.

Sharing sensitive personal data with third parties

In their privacy policy, Grindr opens for sharing personal data with third parties, and they waive responsibility for what kind of information third parties may collect. The technical analysis done by SINTEF confirms that sensitive personal data is shared with third parties.

According to the privacy policy, the company can share information with third parties:

«We may share your hashed Device ID, Profile Information, Distance Information, and demographic information with our advertising and analytics partners. These third parties may also collect information directly from you as described in this Privacy Policy.»

Grindr defines "profile information" as following:

"Profile Information. We may collect Personal Data from you. For example, in the Grindr App, we may collect your photo, display name, relationship status, ethnicity, age or date of birth, geo-location data, email address, password for the Grindr Services, height, weight, social network link, "Looking For," "About

⁵ <https://www.grindr.com/contact/>



Me,” “Favorites,” “Blocks,” “Tribes”⁶ and any other information that you voluntarily add to your profile on the Grindr App or that is generated through your use of the Grindr Services. You may also have the option to provide information concerning health characteristics, such as your HIV status or Last Tested Date.”

Simultaneously, the company waive responsibility for how third parties use tracking technologies in the Grindr service:

“Our advertisers and partners may also use their own cookies or other tracking technology which may collect information about you within the Grindr Services. We do not control use of these tracking technologies.” (Our underscoring)

The table presented by SINTEF on GitHub documents that sensitive data is extensively shared by third parties that according to SINTEF can be classified as tracking- and marketing companies.

Furthermore, SINTEF documents that HIV-status was shared with two third party actors, Localytics and Apptimize. Based on available information about these companies online, it seems like Apptimize deliver analytics services for digital services, typically used for optimizing functionalities.⁷ Localytics appears to offer services for analytics, and for targeting, for example for marketing purposes (“finding your target audience”).⁸ Information about HIV-status, which these services receive from Grindr, are sensitive personal data. According to an assessment done by SINTEF, it is not strictly necessary to transmit such data for analytics and functionality testing (A/B testing).

The Consumer Council find it disconcerting that users of the Grindr service are at risk of losing control over personal data regarding their sexual preferences and HIV-status.

Data transfers to the United States

Data protection legislation in the United States is significantly weaker than in Europe, and the individual is afforded a lower grade of protection for their own personal data. This is also mentioned in the Grindr privacy policy:

“Your Personal Data may be processed in the country in which it was collected and in other countries, including the United States, where laws regarding Personal Data may be less stringent than the laws in your country. Therefore, in

⁶ Examples of a «tribe» is «trans», «leather», and «bear»

⁷ <https://apptimize.com/product>

⁸ <https://www.localytics.com/features?page=engage>



some circumstances, you might be left without a legal remedy in the event of a privacy breach. By submitting your Personal Data, you agree to this transfer, storage and/or processing, including all associated risks.”

The Consumer Council regard this disclaimer as unfortunate, especially when Grindr is transferring sensitive personal data about European users. European users of the app have the right to have their personal data protected according to European law. The Consumer Council cannot see that Grindr is registered under the trans-Atlantic data transfer agreement Privacy Shield, which is meant to ensure that personal data that is transferred to the United States is protected in line with European data protection law.⁹ The Consumer Council see this as a cause for concern regarding whether the privacy rights of European Grindr users are sufficiently respected.

Insufficient consent

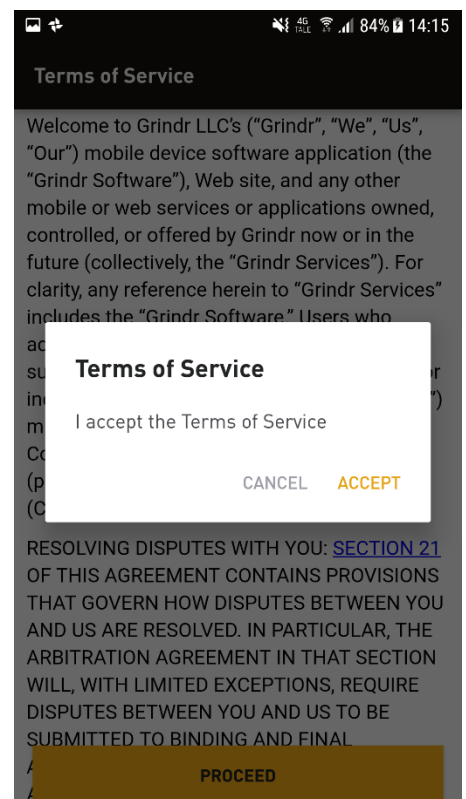
According to the SINTEF report, Grindr shares personal data with different of third parties.

When a user registers a user account in Grindr, the app asks for consent to the terms of service in whole, without individual elements being emphasized or singled out (see attached picture).

In the view of the Consumer Council, information about sensitive personal data being shared with third parties should not be hidden away in long terms of service and privacy policies. The Consumer Council cannot see that Grindr fulfill the conditions for gathering an informed and explicitly given consent.

During the process of registration and inside the app, there is no further description of how data may be shared, other than what is hidden away in the terms of service and privacy policy. There is also no separate consent for sharing sensitive personal data with third parties.

The app does not provide an opportunity to not share personal data with third parties.



⁹ <https://www.privacyshield.gov/list>



Lack of security

According to the technical documentation from SINTEF, Grindr shares sensitive personal data with third parties through unencrypted data flows.

If the user enters information about sexual orientation, sexual preferences, and «tribe» (for example «trans», «leather», and «bear»), this is shared in unencrypted form, according to SINTEF. In the view of the Consumer Council, this does not fulfill the conditions of sufficient information security.

In the cases where SINTEF observed information about HIV-status being shared with third parties/service providers, this data flow was encrypted.

Summary

Grindr is an app that is targeted to and used by sexual minorities, and on that basis there is reason to believe that information about the use of the service could be sufficient to draw conclusions about sexual orientation.

The Consumer Council is of the opinion that Grindr cannot waive their responsibility for how third parties collect data on the users of the service.

When Grindr transmits sensitive personal data to third parties, who could use this information for advertising purposes, this is outside of the scope of the original purpose of the data collection, which is to offer a social networking service. This is in breach of the principle of purpose limitation, and to our knowledge Grindr does not sufficiently ask for consent to this further purpose. In the view of the Consumer Council, this is in breach of Norwegian and European data protection law.

The Consumer Council welcomes the Data Protection Authority undertaking further research based on the findings outlined above.

Feel free to contact us if further clarification is needed.

Sincerely,

The Norwegian Consumer Council, Forbrukerrådet

Gro Mette Moen
Senior advisor digital services

Finn Lützow-Holm Myrstad
Director of digital services