FORBRUKERRÅDET

Morgan Cauvin
Head of Government Relations & Communication
Match Group

Case officer:	Our date:	Our case:	Your date:	Your case:
Ailo Krogh Ravna E-mail: ailo.krogh.ravna@forbrukerradet.no	27.02.2020	19/3372 - 23		

Concerning the Match Group and use of third party tracking in dating apps

We would like to address a number of issues related to the Match Group Android applications OkCupid and Tinder, as detailed in our report "Out of Control".[1] We found the data sharing practices in Match Group apps Tinder and OkCupid to be alarming from a data protection and consumer rights perspective.

In a press release dated January 15th 2020, the Match Group seems to contest a number of our report findings.[2] With this letter, we would like to clarify some aspects and ask the Match Group several questions that we hope that you are able to address.

We would like to start by saying that throughout our report and this letter, we refer to "personal data" as set forth in GDPR Article 4(1). This includes any information relating to an identified or identifiable natural person, including identifiers such as Android Advertising IDs and IP addresses. We refer to "special categories of personal data" as set forth in GDPR Article 9, which includes data concerning a natural person's sex life and sexual orientation.

We would also like to emphasize that the Norwegian Consumer Council is not a regulatory body or supervisory authority. We are a governmentally funded interest organization working for consumer rights.

When the report was published on January 14th 2020, the Norwegian Consumer Council did not formally file complaints to data protection authorities against the data sharing we observed when testing OkCupid and Tinder due to lack of resources. However, on the same day the Norwegian Consumer Council and other consumer organisations asked data protection authorities to take action regarding all processing activities

[1] "Out of Control" https://www.forbrukerradet.no/out-of-control/
[2] "Privacy And Protection Of User Data Is A Top Concern For Match Group" https://newsroom.mtch.com/2020-01-15-Privacy-And-Protection-Of-User-Data-Is-A-Top-Concern-For-Match-Group

and sharing of personal data described in the report.[3] These include our findings on both applications and online advertising partners.

1. Selling or sharing user data

We welcome the Match Group's commitment not to sell user data. However, the findings of our investigation does not address the *sale* of user data, but concerns the *sharing* and *spread* of personal data to third parties.

As detailed in the report, personal data is often being shared with a wide variety of third parties, and consumers cannot know what data is shared, and how this data may be used now or in the future.

2. Sharing special category personal data with third parties

Information from dating apps, including the use of the apps, is often related to a person's sex life and/or sexual orientation. As described in chapter 6.2.4 and 6.3.1 of the report, the data flow analysis of Tinder showed the app sending special category personal data to the third party providers LeanPlum and AppsFlyer. OkCupid was observed sending sensitive personal data to Braze, as described in chapter 6.2.3 of the report.[4]

We acknowledge that the sharing of data with third party service providers may be necessary for various in-app functionalities. However, we question the necessity of Tinder and OkCupid sharing special category data such as sexual orientation and drug use with third party companies, regardless of the purposes of processing.

As discussed throughout the report, it is unclear why these categories of data need to be shared with third party companies. The data sharing is particularly concerning since the consumer is not in a position to know how this information may be used, with whom it may be shared and how to meaningfully be in control.

Sensitive data should not be processed without explicit consent, and consumers do generally not expect this kind of data sharing.

We have not been able to locate documentation that clarifies that third parties cannot use personal data obtained through Match Group properties for their own purposes.

[3] "Consumer organisations call to stop online advertising companies' massive surveillance practices infringing EU laws" https://www.beuc.eu/publications/beuc-x-2020-002_letter_to_executive_vice-president_vestager.pdf
[4] "Out of Control" https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/report-out-of-control/

Can you provide clarification that Braze, LeanPlum and AppsFlyer cannot use any personal data (including GPS coordinates, IP addresses, Advertising ID, etc) received from Match Group properties for their own or other partners or clients' purposes?

3. Use of personal data for advertising purposes

It is stated in the Match Group press release that Match Group does not use "sensitive personal information" for advertising purposes. However, this does not preclude other personal data being shared with third parties, and/or used for serving targeted advertising.

In addition to our observations about Match Group properties sharing personal data with third parties through integrated Software Development Kits, a recent report showed Match Group properties integrating a significant amount of advertising trackers on their websites. [5] The implication of this is that consumers are tracked by numerous commercial third parties when browsing Match Group's websites. We are also concerned about reports that Tinder's Noonlight service was found transmitting data to several adtech companies, including the data broker Kochava.[6]

As mentioned, our research has shown that personal data is transmitted from Tinder and OkCupid to a number of third party companies that are involved in advertising. From your press release and from the privacy policies of Tinder and OkCupid, it is not clear what personal data, if any, Match Group properties share with third parties for targeted advertising purposes, and it is similarly unclear what limitations the Match Group places on further sharing and use of the personal data. Furthermore, the privacy policies of Tinder and OkCupid are not clear about what legal basis applies to which processing operations.

In order for us to better understand how the Match Group protects consumers personal data, could you provide evidence about what categories of personal data (if any) that Match Group properties share or otherwise use for advertising purposes?

4. Sharing identifiers with other third parties

During our technical testing, Tinder was observed transmitting the Android Advertising ID to Salesforce/Krux. OkCupid was observed transmitting the Android Advertising ID to Kochava. Both Tinder and OkCupid were also transmitting the Android Advertising ID to Facebook, and interacting with Google DoubleClick.[7]

[5] "Your favorite dating site isn't as private as you think" https://www.vox.com/recode/2020/2/12/21133832/dating-site-apps-privacy-valentines-day
[6] "Tinder's New Panic Button Is Sharing Your Data With Ad-Tech Companies" https://gizmodo.com/tinders-new-panic-button-is-sharing-your-data-with-ad-t-1841184919
[7] "Out of Control – A review of data sharing by popular mobile apps" https://fil.forbrukerradet.no/wp-content/uploads/2020/01/mnemonic-security-test-report-v1.0.pdf

This identifier allows third parties to track consumers across services. Consumers were not made aware of this upon registering for the services, and were not asked separately to consent to this sharing, as described in chapter 5.14 of the report.

Although consumers can use system level Android settings to opt out of the Advertising ID being used for personalized ads, this does not necessarily stop apps and third parties from collecting and using the identifier.

Can you explain why, and on what legal basis, these Match Group apps are transmitting the Android Advertising ID to Salesforce, Kochava, and Facebook?

How do you ensure that the companies Salesforce, Kochava, Google and Facebook, who are known to monetize consumer data, do not use personal data collected from Match Group properties for their own purposes, or share this data onward with their customers and other partners?

Can you confirm whether Match Group apps and any integrated third parties actually comply with the Android system level opt out settings? Have you put any technical measures to ensure compliance?

5. Sharing of data between Match services

We appreciate Match Group's claim[8] that it does not share user data between its services for any commercial purposes. However, this statement seems to contradict OkCupid's and Tinder's own privacy policies, which were last updated May 25th 2018, and which both contain the following statements (with some minor formatting variations):

> We share your information with other Match Group companies to benefit you in two respects:
>
> for other Match Group companies to assist us in processing your information, as service providers, upon our instructions and on our behalf. Assistance provided by other Match Group companies may include technical processing operations, such as data hosting and maintenance, customer care, marketing and targeted advertising, finance and accounting assistance, better understanding how our service is used and users' behavior to improve our service, securing our data and systems and fighting against spam, abuse, fraud, infringement and other wrongdoings.[9]

As this appears to be self-contradictory, we are left confused about whether Match Group companies actually share personal data between each other for marketing and targeted advertising purposes. Can you clarify what the Match Group actually does?

[8] "Privacy And Protection Of User Data Is A Top Concern For Match Group" https://newsroom.mtch.com/2020-01-15-Privacy-And-Protection-Of-User-Data-Is-A-Top-Concern-For-Match-Group

[9] OkCupid Privacy Policy (accessed February 17th 2020) https://www.okcupid.com/legal/privacy
Tinder Privacy Policy (accessed February 17th 2020) https://www.gotinder.com/privacy

We welcome the Match Group supporting strong data protection regulation, and we hope that you will help set the standard for respecting the GDPR principles of lawfulness, transparency, data minimisation and purpose limitation for processing of personal data. These are fundamental principles that are key to earning the trust of consumers.

We look forward to receiving substantial responses to our questions, and hope that your response will serve to clear up any potential misunderstandings or confusion.

This letter will also be forwarded to the relevant data protection authorities that are investigating the issues highlighted in our report.

Best regards
The Norwegian Consumer Council

Gro Mette Moen
Acting Director of Digital Services

Ailo Krogh Ravna
Digital policy advisor

This document is digitally validated and therefore has no signature.

CC: Datatilsynet

Att: Tobias Judin

Tobias.Judin@Datatilsynet.no

CC: Data Protection Commission

Att: Laura P. Flannery

LPFlannery@dataprotection.ie