FORBRUKERRÅDET

Date: 12.05.2020

FluxLoop AS
Akersgata 41
0185 Oslo

Concerning FluxLoop collection of personal data through the app Perfect365

Dear madam/sir,

We would like to address a number of issues related to FluxLoop collecting personal data through the app Perfect365, as detailed in our report "Out of Control".[1] We find the data collection that we observed FluxLoop engaging in to be alarming from a data protection and consumer rights perspective.

As far as we are aware, FluxLoop has not responded to the findings of the report. Therefore, we want to take this opportunity to outline several problematic practices that we have observed through our work.

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. As described in chapter 6.1 of our report, location data can be used to identify individuals, and is therefore considered personal data.

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 collection we observed from FluxLoop. However, as far as we

[1] "Out of Control" https://www.forbrukerradet.no/out-of-control/

understand, the data collection that we observed FluxLoop engaging in lacks a valid legal basis for processing, and consequently does not comply with the GDPR.

On the same day, the Norwegian Consumer Council and other consumer organisations asked data protection authorities to take action regarding all processing activities and sharing of personal data described in the report.[2] Additionally, on March 4th 2020, eleven digital and human rights organizations sent letters to their national data protection authorities, voicing concern about the data collection practices from a human rights perspective.[3] This call for investigation includes our findings regarding FluxLoop.

As described in chapter 6.1.3 of 'Out of Control', during our testing of the app Perfect365, we observed transmissions of personal data such as the Android Advertising ID and GPS coordinates to a server that appears to be at least partially controlled by FluxLoop.

We acknowledge that third party service providers may need to collect some data in order to provide various in-app functionalities. However, as far as we can understand, FluxLoop reserves the right to use the data collected from Perfect365 for a variety of purposes, including combining it with other information to provide advertising.

> *If you have several applications which uses Pinch™, fluxLoop may compile personal data collected from all those apps to make information, services and advertisement even more relevant to you. The Pinch™ technology provides for an opt out opportunity with respect to such compilation. Note that fluxLoop will not share the compiled data sets with anyone.*[4]

The consumer is not in a position to know how this information may be used and how to meaningfully be in control. As described in the report, consumers

[2] "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
[3] "Rights Organizations Warn about Unlawful Data Exploitation in Popular Apps" https://www.liberties.eu/en/news/7-eu-countries-warn-about-unlawful-data-exploitation-of-popular-apps/18864
[4] FluxLoop privacy policy [accessed 05.05.2020] https://fluxloop.com/privacy-policy

have no way to understand how their personal data is shared with third parties. In short, consumers expect that personal data stays between them and the apps that they use.

According to the FluxLoop privacy policy, consumers may opt out of some processing purposes "by disabling Bluetooth, disabling location based services in the operating system (iOS), disabling Pinch™ in the application settings or by uninstalling the application."[5] However, this would entail both that the consumer is aware that FluxLoop is collecting and using personal data, and that the consumer significantly restricts the functionality of their phones.

Under the GDPR, the processing of personal data requires a valid legal basis. As described in the legal analysis in chapter 8 of 'Out of Control', the collection, compilation and use of personal data for advertising and other commercial purposes is often impossible for consumers to understand, and therefore data controllers such as FluxLoop cannot rely on consent for this processing. Additionally, under the GDPR, consent must be given by a clear affirmative act from the data subject,[6] and thus cannot be based on the user not opting out.

Furthermore, the extent of tracking that we observed constitutes a major breach of the rights and freedoms of the individual data subject, which outweighs any legitimate interest FluxLoop may claim to have to "to provide valuable marketing services to market players who want to target their communications".

Therefore, we cannot see that FluxLoop fulfils any of the relevant legal bases for the processing of personal data that we observed. We expect that FluxLoop changes its practices to bring it into compliance with the GDPR, and delete any data that has been collected without a valid legal basis.

Please do not hesitate to get back to us if we have misunderstood anything about the practices of FluxLoop.

[5] Ibid.
[6] GDPR Recital 32

This letter will also be forwarded to Datatilsynet, which is the relevant data protection authority investigating the issues highlighted in our report.

Regards,

Inger Lise Blyverket
Director General
Norwegian Consumer Council

Gro Mette Moen
Acting Director of Digital Services
Norwegian Consumer Council

CC: Datatilsynet
Att: Tobias Judin
Tobias.Judin@Datatilsynet.no