simonsen vogtwiig

The Norwegian Consumer Council
Fred Olsens gate 1,
0152 Oslo

Attn.: Inger Lise Blyverket

Lawyer in charge:	Our ref.:	Your ref.:	Oslo
Espen Tøndel	63617 501 ETO/MST	20/6987 - 8	15 May 2020

Concerning fluxLoops allegedly collection of personal data through the app Perfect365

Reference is made to the letter from the Norwegian Consumer Council (the "NCC") dated 12 May 2020 concerning fluxLoops alleged collection of personal data through the app Perfect365 and our preliminary response as of 13 May this year.

In general, cases brought up by the NCC gets considerable attention in media and from the market players. This fact calls for a high standard when it comes to credibility, thoroughness and safeguarding of the adversarial principle (hearing both sides of a case), to avoid that private actors as fluxLoop suffer as a consequence of being exposed in media according to unilateral, groundless allegations. All these principles for good administrative procedures were set aside in this case, to promote the NCC's own agenda.

1 fluxLoop has never received personal data from Perfect365

As described in the technical report from Mnemonic AS to the NCC[1] (which forms the basis for the report Out of Control[2]) section 3.3.5 fluxLoop did not process any personal data from the app Perfect365. fluxLoop did only deliver a configuration server to Unacast. fluxLoop received in that context two sorts of data from the app Perfect365: name of the app ("perfect365") and mobile phone model (e.g. iPhone 8). The following is a citation from the report:

> *"The parameters to this request contain information including **the mobile app**, and **the phone model**."*

This is evidently not personal data as defined in data protection law. fluxLoop was not authorized to and had no interest in using these data for other purposes than to deliver the agreed services to Unacast, nor was that done. fluxLoop had no contractual relationship with Perfect365.

[1] The report is accessible from the following URL: https://fil.forbrukerradet.no/wp-content/uploads/2020/01/mnemonic-security-test-report-v1.0.pdf

[2] The report is accessible from the following URL: https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf

If it is anything in this that the NCC does not understand, we suggest that the NCC contacts Mnemonic to have them explain this to the NCC.

2 About fluxLoop's services

In the letter, fluxLoop's deliverables to Unacast is mixed with what the NCC based on failing assumptions believes is fluxLoop's business model. The NCC makes a number of assumptions regarding fluxLoop's handling of personal data from apps, without learning about how this really works.

If the NCC in line with appropriate adversarial principles had taken the time to contact fluxLoop before it completely groundless alleges that fluxLoop operates illegally, fluxLoop would have provided the NCC with information about the services fluxLoop offers in the market and information on how fluxLoop has configured it services to ensure the privacy of end users in a manner that meets the requirements under the GDPR.

2.1 About the Pinch-technology

fluxLoop has developed a technology which makes it possible for enterprises within different industries to better understand their customers. The technology is based on the collection of location data which is combined with other data relevant in order to gain insight about the behaviour of the relevant customer segment.

fluxLoop's services are as per today especially relevant to the mobility sector, retail business and "smart cities". The technology is also of great immediate interest to municipalities and other public actors, which want to gain a deeper insight to the needs of the inhabitants.

The technology developed by fluxLoop is named "Pinch", and consists of among other elements a SDK (Software Development Kit), which may be incorporated into apps. The SDK collects information about the movements of end users in the physical sphere.

According to a data processing agreement with app owners, the SDK sends a de-identified data set[3] (personal data according to applicable data protection law) to a database controlled by fluxLoop, where location data is the most relevant and valuable parameter. fluxLoop processes these de-identified data sets confidentially in a defined time period agreed upon with the app owner, usually 65 days.

According to the data processing agreement with app owner, fluxLoop thereafter anonymizes the de-identified data sets (technically this is done by anonymizing data from day 1 on a daily basis) and puts them into a *trend database*. The anonymization process involves removement of all data which may link the data set to a natural person, in combination with an aggregation to avoid too detailed data sets (which may involve a risk for re-identification).

The anonymization process is as per today as follows:

- Installation ID is removed
- birth year is replaced by age group (e.g. 30-35 years)
- time stamps are replaced by time intervals (e.g. 14-15)
- coordinates are replaced by reference to basic statistical units (e.g. "Lille Tøyen")
- sensitive areas such as hospitals, institutions etc. may be restricted

[3] The data set contains no data that can be directly linked to a natural person, as for example name or phone number. However, the data set contains a unique identifier which may not immediately be linked to a natural person. This identifier is an ID that is generated upon installation of the app and which exists until the app is uninstalled (installation ID)

This aggregation in combination with the deletion of the installation ID of the App, render the data that fluxLoop continue to process anonymous, meaning that they cannot any longer be linked to a natural person. In this way data from app users turn into valuable statistics that customers of fluxLoop might exploit. Customers of fluxLoop get access to a dashboard where they can see illustrations showing how people have moved from one basic statistical unit to another within a given time interval.

fluxLoop has assessed that there is no practical possibility that customers may be able to identify a natural person based on the data presented to them. An important contributing factor to this conclusion is that far from everyone has an app using Pinch. In other words, the number of hits are not equivalent with the actual number meeting the criteria chosen.

2.2 Digital marketing and retargeting of app users is not part of fluxLoop's business model

It is reiterated and emphasized that Pinch does not collect IDs such as IDFA or AdID, which make it possible to target digital advertisements to app users. In other words, fluxLoop does not sell data for marketing purposes, as erroneously assumed by the NCC in the letter. NCC's assumptions is apparently based on an outdated privacy policy that unfortunately is still available from fluxLoop's homepage. Through a direct dialogue, fluxLoop could have explained the situation and avoided the misunderstanding.

fluxLoop operates solely as a data processor towards the app owner. The app owner is controller for all processing of personal data in the app and by fluxLoop by use of the Pinch technology. This means that fluxLoop does not have any independent obligation to inform end users of the app about the processing. However, due to fluxLoop's independent role in relation to the data processing in the context of the Pinch technology, especially with a view to the anonymization process taking place previous to further use of the data, fluxLoop has taken on responsibilities beyond what is strictly spoken required under applicable law and according to the definitions of roles, in order to ensure the end user appropriate information about the processing taking place.

fluxLoop acknowledges that a privacy policy on fluxLoop's homepage achieves very little when it comes to ensuring end users appropriate information about the processing activities carried out by fluxLoop. Thus, lately fluxLoop has instead focused on developing functionality in the SDK such as privacy dashboards. More information about this is provided below.

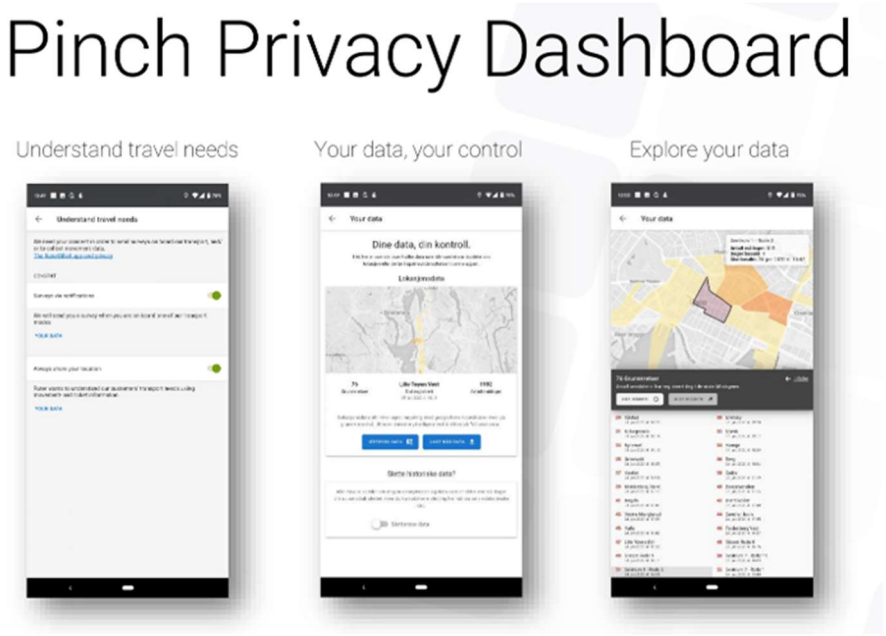
For the sake of good order, it is mentioned that fluxLoop has never sold location data as described in the articles written by NRK. fluxLoop sells insight in the form of visualized, statistical data which is used by fluxLoop's customers to optimilize their services.

2.3 Privacy in fluxLoop

fluxLoop has since the company was established, emphasized the aspect of developing services that protects privacy interests. This has not been a one-time effort, but is something that the company has worked on continuously and which fluxLoop will continue to focus on in the future.

Pinch is developed in accordance with principles of data protection by design and by default (cf. the GDPR article 25). As mentioned, fluxLoop makes sure unique data are removed from the data sets processed (such as advertising IDs, IP addresses, installation IDs etc.) and otherwise aggregate collected data as to exclude the possibility of tracking individuals.

fluxLoop has also developed functionality (part of the SDK) which gives the end users access to all data collected by fluxLoop and the opportunity to at any time delete and/or download the data (data portability), see illustration below. Such functionality contributes to the protection of end user rights in an effective and user-friendly manner. No other than the end user can access this dashboard. The dashboard is illustrated by the figure below and may be accessed here.



3 The NCC's behaviour is blameworthy

fluxLoop is shocked by the NCCs behaviour in this case. If this case was about minor factual misunderstandings or the similar, which had a natural explanation, fluxLoop could have shown understanding. However, it is fluxLoop's comprehension that the NCC has not shown any interest in trying to understand the services provided by fluxLoop, neither shown any interest in the comprehensive work done by fluxLoop in order to deliver services that comply with the strict requirements following applicable data protection law. Neither has the NCC bothered to contact fluxLoop.

Instead, the NCC has chosen to follow a modus operandi which serves the NCCs own agenda only, without taking into consideration the damage such behaviour causes a serious Norwegian start-up company. We also question the role taken by the NCC in the field of data protection law; analysing and concluding in complex questions regarding compliance with data protection law. The Data Protection Inspectorate – with good traditions of contradiction and a deeper understanding of both facts and law – is the relevant authority, which supervises this field.

The NCC has approached the media with the same allegations as presented in the letter; that fluxLoop operates in defiance with applicable data protection law, i.e. illegally. The way media was approached were utterly tactless. fluxLoop received a message from NRK that fluxLoop was about to receive a letter from the NCC. In other words, this letter was sent NRK before it was sent to fluxLopp and only minutes before Inger Lise Blyverket from the NCC and fluxLoop's Ulrik Prøitz should meet live at "Dagsnytt18".[4]

The agenda for the debate program was officially a more general approach to processing of personal data in apps (with Prøitz as an expert in this field), but was then adjusted by the NCC as to put fluxLoop in the stocks based on totally groundless allegations. This indicates a very poor judgement and lack of understanding for the damaging effects such approach to administrative procedures may have on the affected parties. The timing of the letter is also conspicuous. The report was published already in Januar, while the letter is not sent until three months later.

[4] Dagsnytt18 is a debate program sent by the Norwegian TV channel NRK.

The paradox in all this is that the NCC ends its letter with the following sentence: "*Please do not hesitate to get back to us if we have misunderstood anything about the practices of FluxLoop.*", which may indicate a trace of understanding that the facts may be different, but which is meaningless when the NCC first chooses to approach NRK (the TV channel) with the letter.

NCC's behaviour has caused fluxLoop an economic loss by scaring away existing and potential customers and due to the time spent to handle this case. fluxLoop asks the NCC to admit the mistakes committed and to make such apology accessible to the public.

Yours sincerely,
Simonsen Vogt Wiig

Marit Stubø Jorde
Associate
mst@svw.no