Information Commissioner's Office

Upholding information rights

3rd Floor, 14 Cromac Place, Belfast, BT7 2JB
Tel. 0303 123 1114
www.ico.org.uk

Dr E.G.J. O'Neill
Consultant Medical Adviser
Health & Social Care Board
12-22 Linenhall St
Belfast
BT2 8BS

31 July 2020

By email

Dear Eddie,

Data Protection Impact Assessment (DPIA) – STOPCOVID App

Thank you for sharing with us the final version of your DPIA for the STOPCOVID App (the App) prior to its launch later today.

I would like to begin this letter by expressing our gratitude to you and your colleagues for your early engagement with our office on the App, and specifically in developing your responses to our previous advice of 3 July.

As your assessment did not conclude that residual high risk is present, you have not engaged the requirement to consult with the Commissioner as provided by Article 36 of the GDPR. It should therefore be noted that our views and advice in this letter do not constitute 'Prior Consultation'.

This letter will address your response to each of the issues and recommendations highlighted in our letter of 3 July. It should be noted that the Commissioner has no statutory role to endorse an assessment, and the Department of Health (DoH) as controller for the data processed, remain responsible for ensuring the App's compliance with data protection law.

We anticipate further engagement with you on the App, in particular in relation to ongoing discussions regarding interoperability, alongside our colleagues at the Data Protection Commission (DPC).

It should be noted that our views and advice given below are based on the information you have provided to date and are without prejudice to any future intervention by the Commissioner in accordance with her tasks and powers.

Issue 1 – Compliance with Article 22

We note that information about the existence of automated decisions (exposure notifications) is prominent during the onboarding process within the App and is referenced in your privacy information as provided to us.

You have also implemented measures to safeguard individual rights through the facility to discuss the decision with a human and for people to provide their point of view in the event that they disagree with that decision.

We appreciate how privacy-preserving design decisions you have made (specifically the implementation of the Google-Apple Exposure Notification Service – ENS) mean that you will not have access to the data processed in making the original decision in order to review it. However, we are satisfied that in the circumstances, the ability to contest any decision made, and receive advice on an individual's specific situation, has been provided for.

Issue 2 – Validity of lawful basis (consent)

You have taken the view that diagnosis keys constitute special category personal data at the point of upload from user devices to the App's backend architecture. Your rationale for this is that any upload of keys will include a user's IP address as part of the upload packet. You consider this IP address to be additional information which could potentially assist in the identification of the user that those diagnosis keys relate to.

At the point of receipt this IP address is stripped from the keys, which are then made available to other instances of the app (published) for a period of 14 days. In this form, it is your view that this data has been rendered anonymous on the basis that it is no longer possible to identify specific app users (directly or indirectly) from this data alone, and there is no other data that may enable such identification.

We would remind you that it is your responsibility to assess and determine that the information in question is effectively anonymised in the circumstances, and to be able to demonstrate this. Any assessment should ensure that no reasonable likelihood of re-identification remains, taking account of all objective factors including the possibility of singling out, linkability and inferences.

In order to ensure an effective notification service to app users, you also intend to enter a reciprocal agreement with the Department of Health Ireland, for the

sharing of anonymous 'diagnosis keys' generated by each jurisdiction's COVID-19 proximity app.

You should be satisfied that this arrangement will not result in the provision of information that may identify an individual (directly or indirectly) to the Department of Health Ireland. We would also recommend that you publish your assessment of anonymity and re-identification risk, and that app users are clearly informed that their data will be rendered anonymous before being transferred for this purpose.

We appreciate that, at the time of writing, interoperability discussions remain ongoing, and we anticipate further engagement with you as this issue progresses.

Recommendation 1: Metrics data, security tokens and identifiability

We note that your revised DPIA has provided further detail in response to our recommendation and has further considered the reidentification risk to individuals from these data. In relation to your proposal to share anonymised metrics data with the Health and Social Care Board (HSCB), we refer you to our previous comments on anonymised data.

We have no further recommendations to make on this subject at this time.

Recommendation 2: Data subject rights

We appreciate that the single purpose of your app, and the decision to implement the ENS limits the amount of personal data you will process and retain. Your description of how data subject rights will be responded to now reflects this position.

Recommendation 3: Assessment of application of the Privacy and Electronic Communications Regulations 2003 (as amended) ('PECR')

We note you have considered the application of PECR in the DPIA, and conclude that the exemption provided at Regulation 6(4)(b) is engaged as the storage of information, or access to information stored, by the app is deemed strictly necessary in order to provide a service requested by the subscriber or user.

In line with the ICO's contact tracing expectations document, the application of this exemption can apply where storage of information, or access to information

stored, on user devices is strictly necessary for the provision of a contact tracing service the user requests. However, it remains incumbent upon the controller to ensure that in cases where the exemption does not apply, valid consent is obtained. Consideration of this requirement must take place on a case-by-case basis.

Recommendation 4: Risk Assessment

We note your assessment of risk and application of safeguards, and that the level of residual risk identified has been considered acceptable. It remains your responsibility to ensure the security and integrity of personal data processed through the app under your control. We would recommend that the efficacy of the organisational and technical measures you have chosen should be subject to ongoing review.

In closing, I would like to thank you once again for your transparency and engagement with us throughout this process.

Yours sincerely,

Caroline Mooney
Regional Manager
Information Commissioner's Office, Northern Ireland