Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

Scottish Government
St Andrews House
Regent Road
Edinburgh
EH1 3DG

NHS National Services Scotland
Gyle Square
1 South Gyle Crescent
Edinburgh
EH12 9EB

By email only.

24 February 2022

To whom it may concern

ICO investigation into the NHS Scotland Covid Status App – Reprimand for failure to comply with UKGDPR

I write to inform you that the ICO has now completed its investigation into the compliance of the NHS Scotland Covid Status App (the App) with UK data protection law.

Based on our assessment of the information provided, I have decided to issue the Scottish Government and NHS National Services Scotland (NHS NSS) with a reprimand in accordance with Article 58(2)(b) of the UK General Data Protection Regulation ('UKGDPR'). The specific terms of the reprimand can be found towards the end of this letter.

Factual Background

In summary, the ICO has engaged at a high level with the Scottish Government and NHS NSS on routes for COVID status certification since May 2021, with a primary focus on providing vaccine certificates for the purpose of international travel. As the likelihood of using certification domestically increased, the focus of these meetings moved to consider the implications of this policy and in particular, the App in development to facilitate it.

Despite a commitment to provide the ICO with a Data Protection Impact Assessment (DPIA) from the beginning of September 2021, the ICO was not provided with this document until the evening of the 27 September 2021. As the App launch was scheduled for 30 September, this meant that the full details of the intended processing were not known to the ICO until three days before the proposed app launch date.

Our review of the DPIA on 28 September 2021 revealed intended processing operations the ICO had not previously been aware of. Of significant concern was the intention to allow the App's third party ID verification provider to retain images provided by the user during the registration process to verify their identity for five days in order to train their proprietary facial recognition algorithms. This did not appear to be necessary for the App's functioning.

The ICO provided comprehensive feedback on the DPIA on 29 September 2021, and advised Scottish Government and NHS NSS to delay the app launch until our most serious concerns were addressed in full. This included revoking permission for the third party's retention and re-processing of data to train their algorithms.

It is important to note that the App would not have been the only way to obtain proof of COVID vaccination – other methods available at the time included downloading a copy from the NHS Inform website, or contacting the National Contact Centre for a paper copy sent via the post. Delaying the launch of the app would therefore not have prevented the implementation of the Scottish Government's policy on mandatory COVID certification.

At a meeting with John Swinney MSP, Deputy First Minister of Scotland, on 30 September I stressed the importance of the App's compliance with data protection law and reminded him that as the regulator we would consider taking action where appropriate.

The App was launched on the evening of the 30 September 2021. The planned sharing of data (including images) with the third party ID verification provider was suspended prior to launch, however some aspects of the App remained non-compliant with data protection law. As a result the former Information Commissioner, Elizabeth Denham, met with the Deputy First Minister to inform him that the ICO had launched a formal investigation into the App's compliance.

Our consideration of this case

The ICO has investigated whether the Scottish Government and NHS NSS have complied with the requirements of data protection legislation during the development and ongoing deployment of the App. This matter has been

considered under the UK General Data Protection Regulation (the UK GDPR) due to the nature of the processing involved.

During our investigation, we have considered the following:

- The ICO had been cognisant of the possibility of domestic COVID status certification being implemented across the UK since late 2020, and has worked to advise governments across the four UK nations of the data protection considerations. As part of this, the ICO published "COVID-status certification: data protection expectations" on 14 May 2021, making clear the primary data protection considerations and offering guidance on compliance. This document highlighted the importance of ensuring any certification scheme operates in a fair, transparent and lawful manner and that data is not used in ways people would not expect.

- Prior to the App's launch, Scottish Government and NHS NSS explained that they intended to rely on explicit consent for the processing of biometric data and for automated decision-making under Article 22 (despite the ICO's previously published expectations document stating that consent was unlikely to be appropriate in this context). Following separate verbal advice from us that Article 22 was not likely to apply to the processing, reliance on consent was reconsidered by the controllers prior to launch, with the conclusion that this was not necessary. Following the App's launch however, the ICO identified that it contained a misleading statement with respect to the basis for processing personal data. In particular, until 4 October the App contained a statement asking users to provide their consent to the processing of their data. However, processing of personal data within the App was not predicated on the user's consent given that the controllers were relying on public task as their lawful basis. This statement was therefore misleading and unfair, giving users the impression of greater control over their personal data than was the case.

- Article 5(1)(a) sets out the principle that personal data shall be processed in a lawful, fair and transparent manner. The ICO considers that the failure to remove the misleading consent statement from the App prior to launch breached this principle. Evidence provided by the controllers shows that between 554,504 and 615,639 people were affected by this failure.[1]

- People have the right to be informed about the processing of their personal data. Articles 12 and 13 of the UK GDPR set out key requirements around the provision of information to individuals about how their data will be

[1] The range of numbers is due to differences in the date the app was updated on the iOS and Android platforms.

handled. Article 13 sets out the information which must be provided to individuals, and Article 12 requires that this information is provided in a "concise, transparent, intelligible and easily accessible form, using clear and plain language".

- Following the launch of the app, ICO officers were unable to identify an Article 13-compliant privacy notice contained within or linked to from the app. Furthermore, having conducted internet searches ICO officers could not locate the information online. This was raised in a call with Scottish Government and NHS NSS on 1 October 2021, at which point a link was provided to the privacy notice on the NHS Inform website. The ICO explained their concern that this notice was not easily accessible and advised that this must be improved.

- After having been provided with the link to the privacy notice, my staff reviewed this in detail. The privacy notice covered not only the App's but also the NHS Inform website's COVID certificate service, the provision of paper copies by the National Contact Centre and the National Vaccination Scheduling Service. Though the information required by Article 13 of the UK GDPR was provided, ICO staff found the privacy notice was complex, not easily accessible, unnecessarily long and difficult to navigate.

- The issues identified with the privacy notice resulted in media articles published which expressed concern that health data was being shared with large tech companies involved in the delivery of the App[2]. The ICO was advised that these articles "contained quotations which were technically inaccurate" – however the information within the articles appears to have been drawn directly from the privacy notice which illustrates the risk of the content of the privacy notices being misunderstood by the public.

- The privacy notice has been updated on several occasions since the App was launched. It is the view of the ICO that these updates have not addressed the compliance failings identified above.

- It is therefore our conclusion that the App is failing to comply with the transparency principle set out in Article 5(1)(a) as well as Article 12 of the UK GDPR.

[2] Vaccination passport app shares personal data of users with Amazon and Royal Mail - Daily Record, Scots vaccination passport app 'shares personal data with Amazon and Royal Mail' (thescottishsun.co.uk)

During the course of our investigation, we have paid particular attention to the significant public health challenges presented by COVID-19 as well as the role this App plays in addressing them. The ICO recognises that it does not regulate in a vacuum and has considered its regulatory approach throughout the pandemic. This has been communicated to organisations via our website.

We have also considered and welcome the remedial steps taken by the Scottish Government and NHS NSS in light of the initial feedback provided by the ICO, in particular agreeing not to permit third parties to use personal data collected by the App to train their algorithms.

The ICO has given consideration to the public health impact delaying launch to address the failings communicated to Scottish Government and NHS NSS may have had. However in doing so, we noted that the legal requirement to prove vaccine status to gain entry to certain events and venues would come in to force on 1 October 2021 – but that it would not be subject to enforcement until 14 October 2021. Additionally, digital copies of COVID vaccine status were already available to the public via the NHS Inform website. Our view is that more time should have been taken to resolve issues identified by the ICO prior to launch.

Selection of regulatory outcome

The ICO has a range of regulatory tools at its disposal, including monetary penalties. We make our decisions on a case-by-case basis as to which regulatory tool will be most appropriate, and most effective. This case meets many of the criteria set out in our Regulatory Action Policy for issuing a monetary penalty, including the large number of individuals affected, the sensitivy of the data involved, and a failure to follow previous ICO recommendations and advice prior to the App being launched.

Penalties are intended to serve as an appropriate sanction for a breach data protection laws, as well as an effective deterrent. In reaching our decision on this case, we note that the ICO has not, to date, received any complaints about the App. A factor we have also considered is that issuing a penalty in these circumstances would result in less resource available to Scottish Government and NHS NSS to remedy outstanding compliance issues. Given that the privacy notice remains non-compliant, prompt rectification is a priority to ensure that the people of Scotland can be informed about the processing of their data, as is their right.

In this case I have concluded that, on balance, a reprimand would be the most effective and proportionate way to to ensure the infringements identified are swiftly remedied and to deter non-compliance with data protection law in future.

Details of reprimand

The reprimand has been issued in respect of the following processing operations that have infringed the UK GDPR:

- Processing personal data, including special category data, in a manner which was unfair in breach of Article 5(1)(a); and
- Failing to provide clear information about the processing of personal data in breach of Article 12.

Further Action Required

I require the Scottish Government and NHS NSS take certain steps to improve compliance with the UK GDPR. In particular:

1. The privacy notice must be redrafted in order to present the information required by Article 13 in a concise, transparent, intelligible and easily accessible form, using clear and plain language, as is required by Article 12.

Whilst this reprimand does not legally compel Scottish Government and NHS NSS to make the changes set out above, I must be clear that I will consider exercising my power to issue an Enforcement Notice in respect of the issues outlined in this reprimand if the above changes are not completed within the next 30 days. This is particularly important as the app continues to be used. It is also my belief that this route of action will be the most expedient, to ensure the app is now brought into compliance, for the benefit its users.

In particular I note that the Privacy Notice covers processing in relation to the National Vaccination Scheduling Service, which provides appointments for COVID vaccination, and the COVID Status Service - which includes digital and non-digital routes. This combination makes it difficult to clearly understand disparate processing activities. In the interest of conciseness and clarity, you may wish to consider separating out the Privacy Notices for each function.

With this in mind, please provide a copy of the updated privacy notice to Izy Jude [redacted] by 28 March 2022.

The ICO has published detailed guidance on the right to be informed which you may find useful.

Information Commissioner's Office

We hope that the above is clear and assists you in dealing with the outstanding issues of non-compliance however if there are any outstanding questions the ICO remains happy to engage with you on those matters.

Yours sincerely

Steve Wood
Deputy Commissioner
Information Commissioner's Office