Open Rights Group Response to the Cabinet Office "COVID-Status Certification Review – Call for evidence"

Table of Contents

Question 1

Which of the following best describes the capacity in which you are responding to this call for evidence?

Open Rights Group (ORG) is a not for profit and a UK-based digital campaigning organisation working to protect fundamental rights to privacy and free speech online.

With over 3,000 active supporters, we are a grassroots organisation with local groups across the UK. ORG have been advocating for a privacy-minded approach to counter Covid-19 from the outset. In particular, we covered NHSX App shortcomings, supported JCHR efforts to establish legal safeguards for contact tracing, and lodged a complaint to the ICO against NHS and PHE failure to produce a mandatory privacy assessment of the Test and Trace scheme. Furthermore, we engaged with NHS Scotland with legal and privacy reviews, support, and oversight of the data protection impact assessments and privacy safeguards around the Protect Scotland and venue test-and-trace apps.

Question 2

In your view, what are the key considerations, including opportunities and risks, associated with a potential COVID-status certification scheme?

Open Rights Group believes that the planned use of vaccination data for "enabling access to settings or relaxing COVID-secure mitigations" requires careful consideration of its privacy and data protection implications (letter H). To an extent, these considerations will be related to legal considerations (letter B), ethical considerations (letter F) and equalities considerations (letter G).

In particular, in this submission we make the following points:

1. Privacy considerations and the UK data protection framework require Government to clarify and detail the scopes they intend to pursue by establishing this certification scheme. Purpose specification is defined by article 5(1)b of the UK GDPR and Section 36(1) of the Data Protection Act (DPA) 2018. It allows to evaluate the legality of intended uses of personal data, as well as to identify the limits such use should face and the risks that may arise from unintended uses.

2. Once the scope is clear, due attention must be given to the principles of necessity and effectiveness. English courts have adopted a strict necessity test in considering any derogation from the right to private life under Article 8 ECHR, or the protection of personal data under the UK data protection regime. Furthermore, processing must be *necessary* for the performance of a task carried out for health or social care purposes, pursuant to article 9(1)h of the UK GDPR. Any public identity scheme inherently interferes with individuals' right to privacy and data protection. Such interference can be legitimate if it demonstrates that it is fit for purpose, and that there isn't a less intrusive way to achieve the same objectives.

3. We also point out how data protection is meant to be an ongoing process, where necessity, risks and safeguards are continually addressed and reassessed. The UK data protection framework provides a useful tool to deal with this need, namely Data Protection Impact Assessments pursuant to article 35 of the UK GDPR and Section 64 of the DPA 2018. Capacity within the project must exist to assess and meet data protection standards.

4. Finally, we stress the need for primary legislation that clearly spells out the limits to the use of COVID-status certifications, as well as the areas where we

are concerned that the use of such scheme may impact in equality and individuals' rights.

These considerations are developed below. For each of these points, we offer a set of recommendations that are briefly summarised as follow:

- clarifying the aims and policies Government will pursue by establishing this certification scheme;
- being transparent from the outset about the technical solution Government is willing to adopt and their intended uses;
- make Data Protection Impact Assessments a priority and make this documentation publicly available, to reinforce public trust and enable external scrutiny;
- introducing primary legislation to tailor data protection safeguards to these specific circumstances, as well as to introduce an independent oversight mechanism from the beginning; and
- firewalling vaccination data from considerations concerning one's immigration status, as well as close cooperation with Dublin and Stormont to avoid issues with the Irish Border.

0. About the scope of COVID-status certifications

Specifying the objectives being pursued with COVID-Status Certifications will be pivotal for assessing its privacy and data protection implications. Scope shapes individuals' expectations and transparency requirements under the law. Furthermore, it is the point of reference to determine the amount of data that is needed, the risks that may arise, and the security measures that should be adopted to mitigate such risks.

At this stage, we know that Government plans to use vaccination data "to confirm in different settings that individuals have a lower risk of getting sick with or transmitting COVID-19 to others", with the aim of "enabling access to settings or relaxing COVID-secure mitigations".[1] This definition is still too broad and not specific enough to be useful, as it does not address

1 Cabinet Office (2021), *COVID-Status Certification Review - Call for evidence*. Available at: https://www.gov.uk/government/consultations/covid-status-certification-review-call-for-evidence/covid-status-certification-review-call-for-evidence

- what data would be used,
- what those "settings' would be,
- how the likelihood of getting sick, or of transmitting the virus to others , would be determined; nor
- what would be the consequences of that.

Lacking this understanding, a substantial assessment of privacy and data protection issues cannot be performed.

However, we ought to stress our concern regarding the idea of developing a certification system while lacking sufficient scientific understanding of the impact of vaccination on transmission and health status. These concerns have already been raised by many in the previous debates regarding immunity passports, and should be read in conjunction with the World Health Organisation's findings that:

> *"There are still critical unknowns regarding the efficacy of vaccination in reducing transmission [...] Proof of vaccination should not exempt international travellers from complying with other travel risk reduction measures."*[2]

Recommendations:

Before undertaking the development of a certification system, Government should provide greater clarity regarding the policies they intend to adopt following the establishment of a "COVID-Status Certification" system. In particular, Government should detail

- what criteria or characteristics would need be "certified" or proven by this scheme;
- what restrictions would be lifted upon showing proof of this "status";
- what is the causal nexus between the data being used and the consequences for the individual.

The same should apply to any restriction imposed against those who would not have such proof.

---

2 World Health Organisation (2021), *Statement on the sixth meeting of the International Health Regulations (2005) Emergency Committee regarding the coronavirus disease (COVID-19) pandemic*. Available at: https://www.who.int/news/item/15-01-2021-statement-on-the-sixth-meeting-of-the-international-health-regulations-(2005)-emergency-committee-regarding-the-coronavirus-disease-(covid-19)-pandemic

Once this information can be provided, Government should present it to the public and seek further evidence, so that feedback can be given. Government should also make sure that organisations and stakeholders are given sufficient time to review and comment on these proposals.

1. About the necessity test and effectiveness of COVID-status certifications

Personal data is a resource insofar it contributes to the achievement of a result, and becomes a liability as soon as it has exhausted or exceeded such scope.[3] Collecting too much data, or storing it for longer than necessary, increases the risk of data breaches, violations, or other unlawful uses. It also carries the risk of personal data being used beyond the purpose they were originally collected for, especially in aggregation with other data, exposing individuals to abuses or discrimination. Finally, it carries the risk of negatively surprising individuals who would have not expected their data to be used in such ways (also known as "scope creep").

Making sure that as little personal information as possible is being used to certify one's "COVID-status" should be the first step of any scheme or solution being developed by Government. The procedure for assessing necessity is well established,[4] and goes as follow:

- assessing whether the objective being pursued is sufficiently important to justify the use of the data;
- establishing whether such use is rationally connected to the objective;
- ascertaining that a less intrusive measure could not have been adopted without compromising the attainment of the objective being pursued; and
- making sure that a fair balance between the rights of the individual and the interests of the community has been struck.

On top of these considerations, a COVID-status certification would effectively constitute a Public Identity System, although limited in scope. Therefore, it will need to be effective against the problem it addresses in order to be accepted and perceived as legitimate. Effectiveness will be dependent on the uptake, which, in turn, is contingent on public trust.[5] It follows that data protection and privacy considerations

3 See for instance Bruce Schneier (2016), *Data Is a Toxic Asset, So Why Not Throw It Out?* Available at: https://www.schneier.com/essays/archives/2016/03/data_is_a_toxic_asse.html

4 See for instance Bank Mellatt v HM Treasury (No. 2) [2014] AC 700 at §20 (per Lord Sumption) and §74 (per Lord Reed).

5 See Ada Lovelace Institute (2020), *No green lights, no red lines - Public perspectives on COVID-19 technologies*, p. 16. Available at: https://www.adalovelaceinstitute.org/report/covid-19-no-green-

are pivotal in paving the way for the successful deployment of a certification system of this kind.

Finally, public trust is difficult to restore once it is lost. In this regard, the recent failure of the NHSX App provided some valuable lessons. Early plans to develop a centralised and privacy-invasive digital contact tracing solution ended up being dropped in favour of a decentralised and privacy-preserving alternative, thanks to pressure from Open Rights Group and civil society at large.[6] The decision was taken amid public trust concern, and the NHSX App failed to regain the public trust it had lost. In turn, uptake never reached the 80% that was necessary for its functioning,[7] and digital contact tracing spectacularly failed in its objective to allow a "return to normality".

Recommendations:

Government should be transparent about the technical solutions it will seek to develop and adopt from the outset. In particular, such solutions should be presented and accompanied by an assessment regarding the necessity of the collection, the use and storage of this data, and the specific plans put into place to mitigate the risks of misuse and loss of the data. Further attention should be given to alternative solutions, and the rationale that Government relied upon to choose one solution over the other.

2. About data protection and COVID-status certification

COVID-status certifications would inherently engage with the use of health data (such as whether someone has been vaccinated or not), which are sensitive by definition and need a higher level of protection. This system would also apply to a large share of the population in the UK, making it a large-scale use of sensitive personal information. Finally, proofs of vaccination that are linked to a given individual may enable surveillance (e.g. tracking one's movement), restrictions against fundamental freedoms, discrimination, or otherwise expose individuals to consequences that we do not foresee.

---

lights-no-red-lines/

6 Open Rights Group (2020), *Written evidence (COV0019) to the Science and Technology Committee*. Available at: https://committees.parliament.uk/writtenevidence/7529/pdf/

7 Robert Hinch et. al. (2020), *Effective configurations of a digital contact tracing app: A report to NHSX, 14 April 2020 (version 2)*. Available from: https://cdn.theconversation.com/static_files/files/1009/Report_-_Effective_App_Configurations.pdf?1587531217

A system presenting these characteristics needs effective governance to address and mitigate adverse consequences for the individual that may result from the use of vaccination data. Data Protection Impact Assessments (DPIA) should be the baseline of any such governance. DPIAs are a requirement by law — article 35 of the UK GDPR and Section 64 of the Data Protection Act 2018. They are meant to identify risks for the individuals within a given data processing activity, as well as the mitigation measures that need be in place to neutralise these risks. Furthermore, DPIAs are supposed to be carried out before any data processing takes place, and they are meant to be an ongoing process. This allows putting adequate safeguards in place at the upstart, as well as identifying and neutralise any unforeseen threat that may arise.

In doing so, DPIAs allow organisations to deal with risks and uncertainty, while reassuring the public about the security and efficacy of such systems. Unfortunately, past Government responses to Coronavirus have shown significant shortcomings in this regard, with DPIAs being used to downplay risks for the NHSX App,[8] or not being carried out at all for the Test and Trace programme.[9] On top of that, public messages around this matter have been quite alarming, as when the Secretary of State publicly stated his intention to breach data protection laws while misrepresenting DPIAs as "bureaucracy".[10]

Recommendations:

Government should be proactive in setting up effective governance that allows risks to be identified, mitigated, and continually reassessed. In the field of data protection, this must entail the performance of a Data Protection Impact Assessments before any collection or use of vaccination data, as well as periodic reassessments of the risks involved in the deployment and operation of such system.

Finally, Government should not intend these documents for internal use only, but make them publicly available. This would provide much-needed assurance to the public about the security and uses of their personal data, and it would allow effective public scrutiny.

8 Micheal Veale (2020), *Analysis of the NHSX Contact Tracing App 'Isle of Wight' Data Protection Impact Assessment.* Available at: https://osf.io/preprints/lawarxiv/6fvgh

9 BBC (2020), *Coronavirus: England's test and trace programme 'breaks GDPR data law'*. Available at: https://www.bbc.com/news/technology-53466471

10 Source: https://twitter.com/OpenRightsGroup/status/1285260608875700225

3. COVID-status certifications and regulatory safeguards

The UK missed a valuable opportunity to lay the ground for a successful roll-out of a vaccine passport system last year, when the Coronavirus Safeguards Bill failed to pass through Parliament.[11] The Bill, which was drafted by many of the nation's leading academics and practitioners in privacy and data protection,[12] would have provided for the following safeguards:

1. There would be no sanctions levied against an individual for failing to install a contact tracing app, use it, or have it on their person at all times;[13]
2. Any application would be required to have a full public data protection impact assessment available in advance;
3. There would be no mission creep: COVID tracing apps would not be permitted to be repurposed for any other function such as a vaccine passport;
4. There would be no gamification, and no requirement to "play the game"; for example, no obligation to periodically check in or upload data, and no rewards, badges, or trophies issued for doing so;
5. Covid status apps would be used for a singular, specific, and limited purpose, and would not be leveraged as a business opportunity for the private sector to sell goods and services;
6. Apps could not be used as a de facto travel passport required for access to, for example, public transport, shops, or employment;
7. A person's covid status must be made into a protected medical condition in data protection terms, rather than covid status being used as leverage to create a caste system of worthy people in good health and unworthy people with the condition; and finally,
8. There would need to be an independent regulatory body to conduct oversight, provide guidance, and receive complaints about violations of privacy and human rights, and acts of discrimination, related to the usage of an app or the information on it.

Without the Safeguards Bill, we now risk the worst of both worlds: a normalisation of the violations of digital rights and civil liberties which the Bill sought to prevent, and

11 Open Rights Group (2020), *Contact tracing and immunity passports must respect privacy.* Available at: https://www.openrightsgroup.org/blog/contact-tracing-and-immunity-passports-must-respect-privacy/

12 Lilian Edwards and al. *The Coronavirus (Safeguards) Bill 2020: Proposed protections for digital interventions and in relation to immunity certificates*. Available at: https://osf.io/preprints/lawarxiv/yc6xu

13 This logic would be extended to any vaccine passport, either digital or analogue.

a lack of regulatory oversight. But the Bill still provides much that we should draw from for any vaccine passport, such as:

- Distinguishing between a passport use for essential services (employment, education, transport, etc) which ideally would not be permitted, and a passport use for non-essential services (amenities, retail, entertainment, etc) which would be permitted under strict data protection and civil liberties safeguards;
- Discouraging gamification in non-essential services: e.g. no 10% off discount, for showing your vaccine passport;
- Discouraging gamification or tracking in the use of the app: no requirement to periodically upload a covid status or temperature reading;
- Discouraging repurposing of existing apps (test and trace) for vaccine passports; and
- Requiring a full, fresh, from-scratch DPIA for any vaccine passport app.

Recommendations:

Government should advance legislation to set out the limits for data processing, as well as to stipulate when, why and under what conditions individuals would be required to produce such certification.

Above those suggestions, we would recommend that the regulatory oversight proposed in the draft Bill be established immediately, before any work began on the technical aspects of any vaccine passport. This should, ideally, be a new, independent, and time-bound body drawing on the expertise of existing regulatory bodies in data protection, equalities, and employment law.

4. COVID-status certifications and equalities considerations

The most obvious consideration on vaccine passports is that any system cannot be rolled out until all eligible individuals of all ages, from 18 onwards, have been offered a chance to receive one. To do otherwise would risk exacerbating social, economic, and generational inequalities on a possibly unrecoverable scale.

Open Rights Group has worked extensively on issues concerning migrants and data rights, including the immigration exemption[14] and the impact of new data matching

14 Source: https://www.openrightsgroup.org/campaign/immigration-exemption-campaign-page/

powers on non-British citizens.[15] All of these issues remain active and unresolved. Therefore, those issues, by definition, will cascade into any system created to support vaccine passports. There are real risks that migrants whose data rights are already diminished will be obliged to carry a digital passport, and to potentially upload data to it, with the aim of further curtailing their rights and liberties without the recourse available to others. The virus does not recognise citizenship or nationality, and neither must the routes away from it.

We are also concerned about the yet-unexplored implications for vaccine passports and the Irish border. Technology across that border, as in the covid status apps, is interoperable. Civil liberties are not. We must not risk a situation where vaccine passports exacerbate tensions concerning the Irish border by creating a *de facto* ban on employment, commerce, or even everyday socialisation between families and friends.

Recommendations:

We recommend that any vaccine passport must be agnostic to, and completely firewalled from, any data pertaining to immigration status, as has been the case with the test-and-trace apps.

Furthermore, The UK government must work in consultation with Stormont and Dublin to ensure that citizens' rights and civil liberties, both digitally and in real life, are not compromised in any way by the UK's vaccine passport system.

15 Open Rights Group (2021), *Joint letter to National Fraud Initiative re: Consultation extension*. Available at: https://www.openrightsgroup.org/publications/joint-letter-to-national-fraud-initiative-re-consultation-extension/