COVID-status certification: data protection expectations

Purpose

This document sets out our expectations on how organisations may develop COVID-status certification schemes in line with the principles of data protection by design and default. It is aimed at organisations involved in the planning and delivery of COVID-status certification schemes, if implemented.

Scope

The Information Commissioner's Office (ICO) produced this document to provide context-specific information for the development of COVID-status certification and its associated processes.

The Cabinet Office defined 'COVID-status certification' as "the use of testing or vaccination data to confirm in different settings that individuals have a lower risk of getting sick with or transmitting COVID-19 to others." The ICO therefore considered the issue with this definition in mind. We do however recognise that a certification scheme's scope could evolve as policy develops.

The ICO recognises the potential benefits of COVID-status certification schemes as part of the UK's recovery from the impact of the pandemic. It is important that organisations design and implement COVID-status certification schemes and the infrastructure that supports them in a data protection-compliant way. The success of any potential COVID-status certification schemes relies on people trusting them and having confidence in how the schemes use their personal data. The ICO's role as an independent regulator is to act in the public interest, and our approach is to always be a pragmatic and proportionate regulator.

Although there are clear parallels and points of relevance, this document does not cover the UK Government's recently published policy paper for a UK digital identity and attributes trust framework. We published a blog and position paper on this subject on 22 April 2021.

Compliance with data protection law

The controllers responsible for the processing must undertake an assessment of the data protection implications of COVID-status certification on a case-by-case basis. The specific implementation may require additional measures and considerations beyond the scope of this document. Controllers and policy makers involved in the delivery of such schemes should refer to any relevant official guidance and monitor updates.

The ICO considers that COVID-status certification would require a data protection impact assessment (DPIA) prior to implementation, given that the processing is likely to result in a high risk to the rights and freedoms of the public. It is also likely that the processing would require large-scale processing of special category data (in this case, health data), which always requires a DPIA. Organisations should keep any such DPIA under review, particularly if there is a change in scope or context that affects the risks of the processing.

The principles and expectations below do not replace a DPIA. However, organisations can use them to support a DPIA's completion.

Principles

The following principles should guide the development of COVID-status certification schemes. They link to the core principles and provisions of data protection law and should support decision-making. The controller should consider how to apply these principles throughout the lifecycle of the COVID-status certification scheme.

Ensure the certification scheme is lawful and fair

Any certification scheme must have a lawful basis for processing personal data and meet a condition for processing special category data[1] under data protection law. If the processing is necessary and proportionate, it is likely that there will be an appropriate lawful basis for it.[2]

Fairness is an important part of data protection law. COVID-status certification schemes should be able to demonstrate that the processing of personal data:

- is necessary;
- is proportionate; and
- meets the public's reasonable expectations for the processing of their data.

Controllers should give consideration to any adverse impacts of the processing and the provision of any safeguards. It is important that the processing of personal data:

- is fair; and

[1] An example of an applicable condition for processing is likely the public health condition (Article 9(2)(i)). Explicit consent is unlikely to be appropriate for a COVID-status certification scheme.

[2] The applicable lawful bases are likely to be public task or legitimate interest, however the controllers involved need to make their own assessment of which basis is appropriate to their processing. Again, consent is unlikely to be appropriate.

- includes measures for people who don’t have access to digital solutions; and
- does not lead to any discrimination against minority or marginalised groups.

Controllers should put safeguards in place to protect against a system that leads to unfair restrictions on accessing services or opportunities. Any COVID-status scheme should make appropriate provision for children and vulnerable people within the scheme.

It is important to note that data protection is not the only consideration in respect of lawfulness and fairness. Other factors, such as equality and human rights law, are relevant.

Set clear purposes for use and prevent scope creep

The circumstances in which COVID-status certification can be used should be clearly defined. Certificates should be used for genuine reasons of public health and economic recovery.

Purpose limitation is a key principle of data protection law. It requires that personal data is processed for a specific, explicit and legitimate purpose and is not used in a manner that is incompatible with those purposes. Whilst it may not be possible at this point in time to identify all likely uses for COVID-status certification, it is important to remember that personal data should not be used in ways that the individual public would not reasonably expect.

Setting out clear, specific circumstances for the use of COVID-status certification schemes would help to ensure compliance. It would also bring benefits such as providing certainty for organisations and building public trust and confidence. This would then help guard against the actual or perceived risk of “scope creep”.

An important safeguard to limit the use of COVID-status certification would be the provision of clear guidance to organisations and the public, which sets out the circumstances when organisations can use certification. Any COVID-status scheme should make the appropriate provisions for children and vulnerable people. This includes considering the necessity of certification in circumstances where children and vulnerable individuals would be in scope. Any scheme should include measures to identify and mitigate risks that may result from the processing, including possible unintended secondary uses. A sensible safeguard would be regular internal reviews or audits. These reviews should include assessing the scheme’s continued necessity.

COVID-status certificates and associated digital solutions must not be used as a way to track, or otherwise monitor, the public’s movements or the behaviours of individuals. For example, they must not be used to track where and when they used their certificate.

Ensure high standards of accountability and governance

Any organisation processing personal data within a COVID-status certificate scheme must do so compliantly. They must also be able to demonstrate that it is compliant with data protection law. Therefore, it is important to have high standards of accountability and governance through the whole system, to ensure compliance with data protection principles. The scheme must have clear roles and responsibilities for the organisations within the scheme and it must take a 'data protection by design' approach.

Ensure the data is accurate and up to date

For a COVID-status certification scheme to be effective, it must give the public an accurate reflection of their status at a given time. Any digital solution must therefore promptly update people's personal data, and the certificate issuer should implement measures to allow non-digital users to quickly update their status.

People should be able to easily understand what their current COVID status means and how it was determined. Similarly, they should know when their COVID-status certificate would be updated following any change in their status, for example a new test result or vaccination.

People should also be able to challenge or notify the certificate issuer where they believe their COVID status is not accurate. Data protection law provides the right to rectify inaccurate personal data and schemes should make clear how people can exercise this right.

Be transparent

Openness and transparency are key to securing and maintaining public trust in a COVID-status certification scheme. People need to understand what is happening with their data and why. This means ensuring that they have a clear explanation of who is collecting and accessing their data at each stage of the scheme. It also means explaining the types of organisations their data may be shared with and how long their data may be kept for. Information about the use of their data, and how they can exercise their data protection rights, must be easily accessible and understandable, using clear and plain language.

Use the minimum amount of personal data necessary

A COVID-status certification scheme should be limited to using only the data necessary to achieve its purpose. This should apply to both the source data required to create a certificate, and minimising the data displayed at the point of validation.

The data the scheme uses must be proportionate, relevant and not excessive. It must be clear why a COVID-status certification scheme needs that data.

Data minimisation is particularly important when status verification occurs. It should only show, verify and hold the minimum amount of personal data for the least possible time.

Organisations should consider whether their verification of a person's COVID-status would constitute processing personal data within scope of the UK GDPR. Where digital verification takes place, for example through scanning a QR code, this would be processing of personal data – even if the organisation did not keep a record.

However, if the only checks are visual and the organisation does not keep a record, for example a visual check of either a hard-copy document or one on a digital device, the ICO does not consider that this would be processing of personal data.

In the event the verifying organisation is processing personal data, they should document their responsibilities as a controller or processor and implement appropriate governance to safeguard the processing.

Organisations should build in reviews to check that the personal data being processed is still relevant. They should delete data that is no longer needed.

Securely process the data

As part of a data protection by design approach, and to ensure strong effective security, organisations must build in appropriate technical and organisational measures to the digital infrastructure of a COVID-19 status certification scheme. The certificate issuer should consider safeguarding against the manipulation and falsification of certificates. They must have appropriate encryption in place and, where appropriate, they should use privacy-preserving technologies.

When designing a digital infrastructure, organisations should take into account good practice from other digital solutions developed to address COVID-19 (such as contact tracing apps), for example the ability to be transparent to users. Planning also needs to take into account security measures for the production and use of non-digital solutions.

Consideration should be given to how the public's rights and freedoms would be impacted if an infrastructure failure made production or verification of a certificate impossible. What would be the default position in the event of failure? What guidance would be given to venues about how to operate under those circumstances?

Keep data for the minimum amount of time

Any data used for a COVID-status certification scheme should be stored for the minimum amount of time necessary. There should be clear justification of retention periods. This may be difficult to articulate, given the uncertain nature of the pandemic, however we would anticipate that a scheme is only likely to be necessary for a limited time. Review periods should be built in and give consideration to anonymisation as well as deletion when the data is no longer required. Where organisations verifying a certificate are processing personal data, they also need to consider appropriate retention periods.

Having a clearly defined use case for the certificates would permit an easier determination of appropriate retention periods for data and enable an understanding of when any scheme is no longer necessary.

The ICO will keep these recommendations under review, taking into account the recovery from the COVID-19 pandemic and the particular proposals under development. We are engaging with relevant stakeholders on this subject. We are open to conversations regarding these recommendations in order to help organisations build data protection by design and default into their scheme, as this is the best way to promote trust and confidence in any solution.