# COVIDCert Check NI ‘Verifier app’

# DATA PROTECTION IMPACT ASSESSMENT

|  |  |
| --- | --- |
| **DPIA Ref no. *(Information Governance to provide*)** | |
| **Version 05, 21st Nov 2021** | |
| **Project Name** | |
| **COVIDCert Check NI ‘Verifier app’** | |
| **Business Area** | |
| **Department of Health** | |
| **Information Asset Owner** | **Project Manager** |
| **Dan West (Department of Health);** | **Dr Edward O’Neill**  **COVIDCert Check NI ‘Verifier app’ Solution Manager**  **COVIDCert Check NI ‘Verifier app’** |

Contents

[COVIDCert Check NI ‘Verifier app’ 1](#_Toc86237350)

[DATA PROTECTION IMPACT ASSESSMENT 1](#_Toc86237351)

[1. DPIA COVIDCert Check NI ‘Verifier app’ 3](#_Toc86237352)

[2. Purpose of the COVIDCert Check NI ‘Verifier app’ 3](#_Toc86237353)

[3. COVIDCert Check NI ‘Verifier app’ 4](#_Toc86237354)

[Overview 4](#_Toc86237355)

[How does is work? 4](#_Toc86237356)

[4. Consultation & Stakeholders 5](#_Toc86237359)

[COVIDCert Check NI ‘Verifier app’ Governance 5](#_Toc86237360)

[5. Data Processing Overview and Scope 6](#_Toc86237361)

[Data Subjects 6](#_Toc86237362)

[Purpose of processing 6](#_Toc86237363)

[6. Context of Processing and Data Items Processed 6](#_Toc86237364)

[Use of Data 7](#_Toc86237365)

[7. Compliance with data protection law and other regulatory guidance 8](#_Toc86237366)

[The UK GDPR Lawful Basis for Processing 8](#_Toc86237367)

[Necessity and Proportionality 9](#_Toc86237368)

[COVIDCert Check NI ‘Verifier app’ Data Retention 10](#_Toc86237369)

[Data Rights 10](#_Toc86237370)

[Prevention of COVIDCert Check NI ‘Verifier app’ Scope/ Function Creep 10](#_Toc86237371)

[8. Security Measures 10](#_Toc86237372)

[COVIDCert Check NI ‘Verifier app’ Information Security 10](#_Toc86237373)

[Security Controls in place for the COVIDCert Check NI ‘Verifier app’ 10](#_Toc86237374)

[9. Identify and Assess Risks (what are the risks) 11](#_Toc86237375)

[Verifier 11](#_Toc86237376)

[System Developer and Operator 11](#_Toc86237378)

[Bad actors 11](#_Toc86237380)

[Technical 13](#_Toc86237382)

[Appendix A - Data Processors 14](#_Toc86237384)

# DPIA COVIDCert Check NI ‘Verifier app’

|  |
| --- |
|  |

This DPIA relates to the NI COVIDCert Check NI ‘Verifier app’(COVIDCert Check NI ‘Verifier app’) and describes the process within Northern Ireland to verify COVID Certificates for all eligible certificate holders that can be used for the purpose of international travel and domestic use cases.

This DPIA is also intended to cover processing activity by third party controllers, as set out in Article 35(10) of UK GDPR, once Regulations are made, which will require Covid Verification.

This DPIA is under constant review and is subject change.

# Purpose of the COVIDCert Check NI ‘Verifier app’

The Verifier app has been developed by the Department of Health (DoH), via DHCNI, to enable ‘Verifiers’[[1]](#footnote-2) to certify a member of the public’s Covid Status. It will be used by Verifiers, where the Northern Ireland Executive has decided that it is in the public interest to permit only those persons who possess evidence of, being fully vaccinated against COVID-19 to be present on the Verifier’s premises to minimise as far as possible the risk of transmission of the virus which causes COVID-19.

This DPIA has been drafted in line with UK GDPR. Although personal data is not being processed by the Department of Health (DoH) in relation to this app, this DPIA has been drafted to ensure transparency and to maximise the public’s confidence in the app. It has also been developed to provide appropriate DPIA provision to assist controllers who use the App for verification purposes.

Each Verifier who uses the NI Verifier app is required to have their own privacy

notice and they should make these privacy notices available to the public. A template

for these can be found on the ICO website - make your own privacy notice.

Guidance has also been developed to help assist users of the Verifier App. This can be found here – [online guidance.](https://covid-19.hscni.net/covidcert-check-ni-app-user-guide/)

# COVIDCert Check NI ‘Verifier app’

## Overview

The Verifier app has been developed by the Department of Health (‘DOH’, ‘we’, ‘our’) and DoH has overall responsibility for the functionality and delivery of the Verifier app. It will be delivered by Digital Health and Care NI (DHCNI) team on behalf of the DOH.

This DPIA applies to the NI Verifier app only. There is a separate DPIA that applies to the processing carried out as part of the Covid Certification Service (COVIDCert Check NI ‘Verifier app’) and related COVIDCert NI Cert App , which explains how individual’s data is processed when they chose to use the Service to certify their Covid status.

The Department will not process any personal data in relation to the Verifier App. Users of the Verifier App will temporarily process personal data for the purposes of verifying an individual’s Covid status (as explained below).

## How does this work?

The NI Verifier app allows the Verifier to scan a COVID Pass 2D barcode, displayed by a member of the public from their Covid Certificate, either via the 2D barcode available on the COVIDCert Check NI app, or via a hard copy Covid Certificate, to show their COVID Pass status.

The scanning app, which enables the Verifier to scan the 2D barcode is known as COVIDCert Check NI ‘Verifier app’ and is downloaded as an app to a mobile device used by the Verifier, from the Apple Play Store or Google Play in order to verify COVID certificates. Secure paper vaccination certificates can also be scanned by the NI Verifier app.

The NI Verifier app reads 2D barcodes that are presented to it and allows the Verifier to check the validity of the 2D barcode.

The scanner or verifier views the information contained in the 2D barcode by using the camera on the phone of NI Verifier operator. Once the 2D barcode is successfully scanned a number of results will be returned:

* For domestic use[[2]](#footnote-3), scanning a 2D barcode generated for domestic use and events using the NI Verifier app, will generate a green for a “valid” certification status or a red for “invalid” certification status screen. Citizens presenting a paper certificate for scanning will result in a yellow check screen on the Verifier App status screen. There is no further opportunity to see any further details as a result of that scan.
* For international travel, scanning a 2D barcode generated for travel use using the NI Verifier app, will generate a teal blue “valid” screen and request the user to check the citizen’s identification. A red “invalid for travel” screen will be shown if it doesn’t satisfy the NI vaccination travel rules.

# Consultation & Stakeholders

The NI COVIDCert Check NI ‘Verifier app’ is being established under an Oversight Group chaired by the DoH Chief Medical Officer (CMO). The Steering Group, which reports to the CMO, is independently chaired by Dr Edward O’Neill with membership from DoH, PHA, and HSCB.

Consultation has also been carried out with:

* Venues and verifiers using this app
* Department of Health
* Public Health Agency
* Health and Social Care Board
* NI Privacy Advisory Committee
* Information Commissioners Office
* Committee on the Administration of Justice (CAJ)
* Children’s Law Centre
* COPNI
* NICVA
* NI Human Rights Commission
* Human Rights Consortium
* Belfast Health and Social Care Trust (BHSCT)
* Civica - software development company
* BigMotive – A user experience and software development company
* Political representatives - NI Executive
* Media

## **COVIDCert Check NI ‘Verifier app’ Governance**

A COVIDCert Check NI ‘Verifier app’ Product Team has been formed by DHCNI on behalf of the Department of Health to design, develop and co-ordinate the roll out of the app. This is headed up by Dr Edward O’Neill who acts as the Product Manager for all aspects of the app.

The Product Manager provides expert clinical advice and development prioritisation to the development team product owners. The COVIDCert Check NI ‘Verifier app’ Product Manager, is tasked with, amongst other responsibilities, to ensure that the:

* COVIDCert Check NI ‘Verifier app’ is used for its intended purpose
* COVIDCert Check NI ‘Verifier app’ data processing is appropriately bounded in time and scope,
* This DPIA report is kept under review and up to date, and
* Co‐ordination of the necessary analysis to assess the efficacy of the COVIDCert Check NI ‘Verifier app’.

The COVIDCert Check NI ‘Verifier app’ Product Manager, Product Owners and supporting development teams meet daily to ensure priorities. The Product Manager provides regular updates on the uptake and functioning of the COVIDCert Check NI ‘Verifier app’. Requirement prioritisation is conducted by the Product Manager who in turn directs the development through the Product Owners to the suppliers.

# Data Processing Overview and Scope

This section of the document describes the COVIDCert Check NI ‘Verifier app’ data that will be sourced, processed, how much data is being collected and used, how often it will be processed, how long it will be retained for, and who the data relates to.

## **D**ata Subjects

The proposed data processing within the COVIDCert Check NI ‘Verifier app’ relates to all citizens in NI who intend to visit a location where COVID certificates are verified through the COVIDCert Check NI ‘Verifier app’.

## Purpose of processing

The COVIDCert Check NI ‘Verifier app’ product has been developed by an existing DHCNI software partner Civica (data processor).

Citizen personal information will be used for the following purposes:

* International Travel - The Digital Covid Certificate payload is used to validate and ensure the data is a signed by verified public health authority and the citizen has a valid vaccination for the travel.
* Domestic Use - No citizen data is passed from or to the mobile app. The App sends the entire contents of the signed domestic certificate payload which contains a unique identifier for the CCS endpoint. The response from the server will only be valid or invalid..

# Context of Processing and Data Items Processed

For international travel the app checks the Digital Covid Certificate to ensure:

* It is a valid certificate based on the European Digital Green Certificate Schema
* The payload has been signed by a health authority
* The certificate contains vaccination information
* The vaccination Information: Dose Number is greater than or equal to the Total Number of Doses
* The certificate hasn't expired
* The certificate contains a family name

If the digital covid certificate is intended for travel, then the verifier app will surface the "Given name" and "Family Number" for the user of the app to check against Photo ID.

For Domestic:

* No citizen data is stored or processed in the app.

## Use of Data

Other than name of the individual, which is shown on the 2D Barcode string, there is no personal data processed when using the Verifier App, as personal data is not transferred to the app, instead the App just scans the barcode on the certificate held by the Individual, either on the individual’s COVIDCert App digital certificate, where data is held encrypted within a 2D Barcode, or on the paper certificate where the barcode can be scanned.

This code is generated in the COVID Certificate by the COVID Certification Service (CCS) by the below process:

Within CCS, after the identity matching service successfully matches the users entered data to the vaccination information and provides vaccination details for the certificate, the solution will generate a 2D Barcode (QR Codes) which is securely signed by the issuer to ensure its authenticity for the purposes of travel or domestic uses.

* The 2D Barcode (QR Codes) is used to certify the COVID status of the user.
* The COVID status is validated by scanning the 2D Bar code which checks the signature on the 2D Barcode is valid and displays the appropriate screen associated with the result of the scan:
  + Green Valid Domestic Certificate showing time and date.
  + Blue Valid Travel Certificate showing name, time and date. It also indicates to check ID.
  + Yellow Valid Paper Domestic Certificate. Only valid if scanned from paper ID showing time and date. It also indicates to check ID.
  + Red Invalid Domestic Certificate showing time and date.
  + Red Invalid Travel Certificate showing time and date.
* details associated with the certificate.

A 2D bar code is only created if the data associated with the user complies with the business rules deciding whether a citizen is eligible for a safe COVID status or not.

The Solution uses the NHSD Devolved Administrations and Crown Dependencies Citizens QR Generator.

The reason the solution will use the NHSD service is:

* It is the UK which controls borders for all constituent countries part of the United Kingdom. For this reason, internationally recognizable and verifiable Covid Status QR codes should be signed by a central UK authority.

The UK will be responsible for on-boarding with EU Trust Gateway. This approach avoids Northern Ireland having to negotiate with the EU to get onboarded to the EU Trust Gateway.

# Compliance with data protection law and other regulatory guidance

**The UK GDPR Lawful Basis for Processing**

The Northern Ireland Executive has legislated in the Health Protection (Coronavirus, Restrictions)(No.4) Regulations (Northern Ireland) 2021 that it is in the public interest to permit only those persons who possess evidence of, inter alia, being fully vaccinated against COVID-19 to be present on the Verifier’s premises to minimise as far as possible the risk of transmission of the virus which causes COVID-19.

To that end we process personal information according to the UK General Data Protection Regulation and the Data Protection Act 2018, which will be referred to as Data Protection legislation. Personal data is processed for COVIDCert Check NI ‘Verifier app’ as part of our public task (in line with UK GDPR Article 6(1)(c) and 6(1)(e))[[3]](#footnote-4). In line with the Dept of Health statutory duty which include:

* Section 2(1) the duty to promote in Northern Ireland an integrated system of health care designed to secure improvement in the physical and mental health of people in Northern Ireland and in the prevention, diagnosis and treatment of illness, and
* Section 2(3)(g) the duty to secure the commissioning and development of programmes and initiatives conducive to the improvement of the health and social well-being of people in Northern Ireland, and
* Section 3(1)(b) the power to provide, or secure provision of, such health and social care as it considers appropriate for the purpose of discharging its duty under section 2; and do anything which is calculated to facilitate, or is conducive or incidental to, the discharge of that duty.

Some of the data processed relates to health data which is described as ‘special category data’. In relation to that processing, the following UK GDPR conditions apply:

* **Article 9(2)(g)** – the processing is necessary for reasons of substantial public interest.
* **Article 9(2)(i)** – the processing is necessary for reasons of public interest in the area of public health.

**Necessity and Proportionality**

Civica has been commissioned by DoH to develop the COVIDCert Check Verifier App, and is part of the suite of applications in support of the COVID Certification Service.

**Necessity:**

This processing supports maintaining good public health to combat a rise in infection rates and reducing the spread of Covid-19. This processes also mitigates potential pressures on health services expected over the winter period. Organisations will want to be able to verify an individual's COVID status and check they have been fully vaccinated against COVID-19 for:

* International travel
* Or domestic purposes

Only data necessary for this purpose will be processed, with appropriate technology used and security in place (details can be found in section 6. Context of Processing and Data Items Processed)

**Proportionality:**

A digital app solution is able to do this securely and quickly using complex algorithms to verify digital certificates embedded into the 2D bar codes being scanned. Automated checking is more accurate than humans reading long strings of random characters and numbers. No personal data is stored or transmitted by the App.

The provision of a centrally developed and secure app limits the likelihood for third party apps with different privacy controls. Therefore it has been determined that it is better for a centralised body to provide a digital app rather than rely on the market to produce various different apps, or require venues (particularly smaller ones) to create their own system.

The COVIDCert Check NI ‘Verifier app’ aims:

* To keep the process clear and simple for the public
* To reassure the public about the way their data is managed, and demonstrating alignment with ICO guidance on data minimisation and compliance with data protection legislation
* To securely verify the identity of individuals
* To comply with emerging and changing EU and WHO standards.

**COVIDCert Check NI ‘Verifier app’ Data Retention**

No personal data is collected or stored via this solution. App usage metrics data is sent from the App to the Civica staff to view and analyse the metric data. The metrics data is in aggregated format - no personal identifiable data is shared.

The personal data displayed within the Verifier App is deleted after 10 seconds or at the point the Verifier returns/begins another scan

**Data Rights**

UK GDPR Rights are fully engaged. Rights in relation to the Covid Certification Service (CCS) are set out in the CCS PN and your rights regarding the processing carried out by users of the Verifier App- ‘Verifiers’- should be set out in their Privacy Notices.

**Prevention of COVIDCert Check NI ‘Verifier app’ Scope/ Function Creep**

When citizen information is collected and processed for one reason but is then used or processed in ways beyond the original COVIDCert Check NI ‘Verifier app’ purpose this is called function creep. Measures are in place to ensure this is prevented.

Any technical or functional changes needed to be made to the COVIDCert Check NI ‘Verifier app’ require a formal request be made to the COVIDCert Check NI ‘Verifier app’ programme team. These are then prioritised, costed and applied to a technical backlog for subsequent development.

# Security Measures

Security measures are in place to ensure the information processed is carried out only as detailed in this DPIA and ultimately only for the purposes intended.

## COVIDCert Check NI ‘Verifier app’ Information Security

* No personal data / information is stored in the app. The signed 2D barcode is scanned for the purpose of verification. Hence no personal data is accessible by any user or developer of the app.

## Security Controls in place for the COVIDCert Check NI ‘Verifier app’

COVIDCert Check NI ‘Verifier app’ suppliers comply with both international and industry-specific compliance standards and participate in rigorous third-party audits and penetration testing that verify security controls. As required by the UK GDPR, the COVIDCert Check NI ‘Verifier app’ developers implement and maintain appropriate technical and organisational security measures, including measures that meet the requirements of ISO 27001 and ISO 27018, to protect personal data they process as data processors on its customers' behalf.

COVIDCert Check NI ‘Verifier app’ administrators can run a report on any record to see all the staff who have accessed it, what if any change were made and where that access was appropriate or necessary.

Penetration testing of the App has been performed by Omnisecurity, an approved external party.

# Identify and Assess Risks (what are the risks)

## Verifier

The following table identifies the risks for those who download and use the app for its defined purpose i.e. verifying that an individual’s COVID certificate has been issued by a trusted authority.

|  |  |
| --- | --- |
| *Risk* | There is a risk the app user copies the personal data displayed to them either by writing it down or taking a screen shot in order to steal the personal data of the individuals who QR codes they are scanning. |
| *Impact* | Loss of confidentiality to the individual whose QR code is scanned.  There would be no health impact on the individual. |
| *Notes* | This would be deemed misuse of the App for the purposes of data theft and a breach of the Terms and Conditions, which users are required to agree to. |

|  |  |
| --- | --- |
| *Risk* | There is a risk that the app user scans QR codes that are not COVID status related. |
| *Impact* | There is no impact on the individual whose non-COVID status QR code is scanned. |
| *Notes* | It is thought that this is very unlikely to occur. |

## System Developer and Operator

The following table identifies the key risks for Civica software engineers who will be developing the App.

|  |  |
| --- | --- |
| *Risk* | There is a risk that the engineers share their user accounts. |
| *Impact* | Logs record all activity undertaken against the logged in account. If a concern is raised, then there is no way to distinguish between which user took which actions other than the honesty of the engineers involved.  There would be no health impact on the individual. |
| *Notes* | Can’t see this happening especially as working from home is currently the norm so less likely to use an already logged in device. |

|  |  |
| --- | --- |
| *Risk* | There is a risk that the engineers misuse their privileged access to add malicious code, viruses, etc. |
| *Impact* | Depends on the nature of the code introduced but could lead to poor performance, corruption of data, etc. leading to failure of the App to verify a QR code or being able to display the relevant details to the App user which could lead to an individual being denied access to services.  There would be no health impact on the individual. |
| *Notes* | Not expected to happen but potential exists |

|  |  |
| --- | --- |
| *Risk* | There is a risk that the software versions used to develop the App are not kept up to date or patched leaving vulnerabilities that can be exploited by bad actors. |
| *Impact* | Depends on the nature of the vulnerability but most likely to lead to data theft due to decoded data in the App being able to be read by a bad actor.  Loss of confidentiality to the individual whose QR code is scanned.  There would be no health impact on the individual. |
| *Notes* | The potential does exist |

|  |  |
| --- | --- |
| *Risk* | There is a risk that a maintenance error exposes more data from the decoded QR code than is required for the app user to verify the validity of the QR code and the individual’s COVID status. |
| *Impact* | Loss of confidentiality to the individual whose QR code is scanned.  There would be no health impact on the individual. |
| *Notes* | The potential exists |

|  |  |
| --- | --- |
| *Risk* | There is a risk that engineers misuse their privileged access to introduce code into the App that sends the data read from the QR code to another location effectively stealing the data. |
| *Impact* | Loss of confidentiality to the individual whose QR code is scanned.  There would be no health impact on the individual.  There would be no impact on the individual for access to the service as the data would still be displayed within the App to the user. |
| *Notes* | Not expected to happen but potential exists |

## Bad actors

The following table identifies the key risks for Unauthorised User Group; this group includes ‘script kiddies’, organised crime groups and hostile state actors.

|  |  |
| --- | --- |
| *Risk* | There is a risk that a bad actor gains access to authorised user credentials via a phishing attack or other method. |
| *Impact* | Depends on the account privileges that the bad actor gains access to but could lead to ransomware attack on Civica.  There would be no health impact on the individual. |
| *Notes* | In this risk, an authorised user is a Civica developer with access to the environment where the app is developed.  Bad actors likely to try this but given that no personal or other data is held by Civica for this App it would be of little value to a bad actor to attempt this other than to disrupt Civica activity in general. |

|  |  |
| --- | --- |
| *Risk* | There is a risk that the app is removed from either app store. |
| *Impact* | Prevents individuals from downloading and using the app limiting its effectiveness.  Possibly impacts on venues being able to verify individuals COVID status prior to entry. |
| *Notes* | Can’t provide the service to new users; existing users unaffected; should be resolved relatively quickly.  There would be no health impact on the individual. |

|  |  |
| --- | --- |
| *Risk* | There is a risk that the app is replaced with a malicious app. |
| *Impact* | Depends on what the malicious app does but could lead to theft of personal data as the unauthorised app contains code to copy the personal and other data to another location. |
| *Notes* | The potential exists. |

|  |  |
| --- | --- |
| *Risk* | There is a risk that if a bad actor gains access, they can introduce malicious code, viruses, etc |
| *Impact* | Depends on the nature of the code introduced but could lead to poor performance, corruption of data, etc. leading to failure of the App to verify a QR code or being able to display the relevant details to the App user which could lead to an individual being denied access to services.  There would be no health impact on the individual.  Individual may not be able to access venue. |
| *Notes* | Without mitigation this is likely to be attempted. |

|  |  |
| --- | --- |
| *Risk* | There is a risk that a bad actor gains access to introduce code into the App that sends the data read from the QR code to another location effectively stealing the data |
| *Impact* | Loss of confidentiality to the individual whose QR code is scanned.  There would be no health impact on the individual.  There would be no impact on the individual for access to the service as the data would still be displayed within the App to the user. |
| *Notes* | This is possible but if the bad actor has gained access to the environment where the App is developed then there are more destructive things they can do such as create a ransomware attack on Civica. |

|  |  |
| --- | --- |
| *Risk* | There is a risk that unauthorised users could gain privileged access due to an unattended, unlocked device (i.e. developer’s laptop) (this risk is not related to app users’ mobile phone devices) |
| *Impact* | The impact depends on whose device the unauthorised user is able to access e.g. if it was an administrator account then deletion of parts of the App development environment might be feasible; or a user with normal access may allow the introduction of malicious code or viruses.  The impact also depends on the knowledge and skill level of the unauthorised user. They may have little knowledge of information technology beyond web browsing and online shopping or they may be a ‘at home technical wizard’. |
| *Notes* | Under current conditions where most people are working from home, the biggest threat will come from a family member. |

## Technical

The following table identifies the key risks due to technical issues

|  |  |
| --- | --- |
| *Risk* | There is a risk that there is a technical outage (mobile device network) preventing the Apps being able to scan and verify a QR code. |
| *Impact* | There would be no health impact on the individual.  The individual whose QR code is being attempted to be scanned for access to the service could be denied access if there is a mobile phone network outage. |
| *Notes* | All technical environments are subject to some risk failure. |

## Appendix A - Data Processors

All data processors are appointed under Data Processors Agreements in compliance with Article 28 of the UK GDPR, either via UK GDPR compliant contracts, or MoUs.

Under the terms of these arrangements DoH is the data controller responsible for assessing that all processors listed below are competent to process personal data in line with UK GDPR requirements, as part of existing contracts with these processors. In taking the COVIDCert Check NI ‘Verifier app’ forward HSCB progressed the necessary procurements with third party processors for the COVIDCert Check NI ‘Verifier app’ and as a result HSCB is the holder of the contracts and therefore responsible for ensuring processors are competent to process personal data in line with UK GDPR requirements, on behalf of DoH. This assessment will consider the nature of the processing and the risks to the data subjects.

Under Article 28(1) HSCB will ensure that only processors that can provide “sufficient guarantees” (in terms of its expert knowledge, resources, and reliability) to implement appropriate technical and organisational measures to ensure the processing complies with the UK GDPR and protects the rights of individuals.

Contracts or Memorandum of Understanding (MoUs) will be in place to govern relationships with the data processors, which set out the obligations of each party and the data controllers’ obligations and rights regarding the data that is being processed. All contracts adhere to established BSO Procurement and Logistics Services (PaLs) processes and legal input provided by BSO Department of Legal Services (DLS).

All data processing takes place within the UK area and as such is subject to legislation in the form of the UK - General Data Protection Regulation (GDPR).

The following provides a list ofdata processors involved in delivery of the system.

* **Civica** is a system integrator organisation who were chosen to develop the end-to-end COVIDCert Check NI ‘Verifier app’ platform and are regarded as a ~~sub-~~processor contracted by the HSCB. Civica will provide support on an ongoing basis to the COVIDCert Check NI ‘Verifier app’ configuration for the duration of its operation, as part of their contract.
* **BigMotive** is a software development company who were chosen to develop the COVIDCert Check NI ‘Verifier app’ user interface and are responsible for the configuration of the COVIDCert Check NI ‘Verifier app’ webforms and are regarded as a ~~sub-~~processor contracted by HSCB. BigMotive will provide support for user experience (UX) design on an ongoing basis for the duration of the COVIDCert Check NI ‘Verifier app’ operation, as part of their contract.
* **Belfast Health and Social Care Trust (BHSCT).** BHSCT is a statutory organisation providing VMS, data exchange and CTR services as a processor for HSCB and PHA. BHSCT host the COVIDCert Check NI ‘Verifier app’, VMS and CTR applications separately on their Azure platform on individual instances. Their services are managed via appropriate verbal agreements with HSCB and PHA. A formalised MOU between the parties is being developed.

1. Verifiers’ refers to the organisations/ businesses/ venues who will verify/check COVID certificates using this app. [↑](#footnote-ref-2)
2. Domestic use refers to visiting domestic venues like bars, pubs, clubs, concert halls, stadiums etc. [↑](#footnote-ref-3)
3. This refers to the processing that is necessary for the performance of the official tasks carried out in the public interest. [↑](#footnote-ref-4)