Data Protection Impact Assessment

COVID Tracker App

Table of Contents

COVID Tracker App

The Health Service Executive ("HSE") and the Department of Health ("DoH") propose to introduce a national COVID-19 pandemic response mobile application called the COVID Tracker App ("the app"). The app, which will be entirely voluntary, is to support and augment the HSE's COVID-19 pandemic response efforts including contact tracing, symptom tracking, epidemiological analysis, and the provision of a trusted and reliable source of COVID-19 related information to users.

The purpose of this document is to transparently assess the impact of the envisaged processing operations on the protection of personal data and how the rights to privacy and confidentiality of the users are appropriately protected. In light of the scale of the envisaged data processing, types of data processing and use of new technology, the carrying out of this assessment is considered appropriate.

1. Overview

Contact tracing and testing is seen as a cornerstone of strategies employed by countries to contain the spread of the coronavirus and save lives across the globe. The public health framework approach that has guided the development of the national Roadmap for Reopening Society and Business emphasises the role of contact tracing and testing, utilising robust information and monitoring of the disease, and providing clear consistent sustained accessible communication with the public from trusted sources[1].

Within the context of the national public-health led response to COVID-19 in Ireland, the HSE and DoH are jointly developing a mobile phone application. The app will have two purposes.

Purpose 1: To support the national public health response to COVID-19 by

    a) Enhancing the existing HSE contact tracing operation
    b) Monitoring and mapping the spread of COVID-19 symptoms

The app is being developed because using mobile technology can improve the speed and accuracy of manual contact tracing. With mobile technology, contact tracing teams will no longer have to solely rely on a person who has COVID-19 to remember everyone they were in contact with. The app will allow people in close contact with a COVID-19 case to be notified faster, helping us stay ahead of the virus and save lives. Anonymous daily symptom information can be used by public health teams to predict outbreaks and to provide support to manage the risk of outbreaks.

Purpose 2: To support members of the public during the COVID-19 crisis by

    a) Providing COVID-19 related news, information, and national updates on the app
    b) Storing a personal record of symptoms on the app

Providing timely information from a trusted national source is a key part of supporting the public through this crisis and the app is a convenient addition to the current suite of national communication channels for COVID-19 in Ireland. Providing a way for people to record and share their symptoms daily supports their ability to directly contribute to the fight against the virus and to serve as a memory aid if they are in contact with health service providers, the latter also contributing to Purpose 1 above.

2. Roles and Responsibilities

For the purposes of the app, the HSE and DoH are joint data controllers as both are jointly determining the means and purposes of the processing. The HSE is responsible for the development, testing, security, operation and maintenance of the app. DoH's role is to provide strategic leadership for the app and to ensure that government policies are translated into actions and implemented effectively. Both the HSE and DoH will enter into a joint controller arrangement under Article 26 of

---

[1] https://www.gov.ie/en/news/58bc8b-taoiseach-announces-roadmap-for-reopening-society-and-business-and-u/. pg. 4.

GDPR. The CSO has a role in receiving anonymous COVID-19 symptom data from the app via the HSE, which it will use for statistical analysis to assist the DoH and public health specialists in monitoring the progression of symptoms across the country.

An App Advisory Committee has been formed to provide an inter-departmental oversight function in relation to the app development, the terms of reference for which are provided in Appendix A. This group is tasked with, amongst other responsibilities, ensuring that the app is used for its intended purposes, data processing is appropriately bounded in time and scope, that this DPIA report is kept under review and up to date, and co-ordinating the necessary research and analysis to assess the efficacy of the app.

There are a number of data processors and other roles that are assisting the HSE and DoH in designing, building and operating the app, these are listed in Appendix B.

3. Processing Overview

Use of the app will be entirely voluntary and will be available to download for free from the Apple App Store and the Google Play Store. It will run on iPhones that support iOS 13.5 (or later) and Android phones running Android 6.0 and higher. The functions of the app that fulfil the stated purposes are as follows.

3.1 Contact Tracing

The HSE currently operates Contact Tracing Centres to perform manual contact tracing.[2] This is the process where a person who has been infected with COVID-19 is interviewed over the phone to identify the people they have been in close contact with since their symptom onset date minus 48 hours ('infectious period'). A close contact includes where people spend more than 15 minutes within 2 meters of each other. These close contacts are then phoned and given advice to restrict their movements in line with public health policy, thus restricting the spread of the virus. The Contact Tracing function within the app is being designed to augment the current manual contact tracing operation in the HSE as is proposed to work as follows.

When a person downloads the app they can optionally enable its Contact Tracing function. If they choose to do so the person will be asked to turn on the phone's Exposure Notification Services (ENS) service. ENS is a new Bluetooth feature that Apple and Google are introducing to support contact tracing efforts across the globe using iPhones and Android phones in a privacy preserving way.[3]

Continuous scanning – phones with ENS active will continuously scan for other phones nearby with ENS active. This happens regardless of which national contact tracing app is deployed on the phone, provided the phone is running the latest operating system from Apple and Google that incorporate the ENS service. ENS does not operate on a phones that don't have a national contact tracing app

Figure 1- Phones detect each other anonymously without any user action

---

[2] https://www2.hse.ie/conditions/coronavirus/testing/contact-tracing.html

[3] The description of Exposure Notification Services and how it is used in this document is abbreviated and approximate, removing much of the cryptographic underpinnings in an effort to more clearly impart the key matters relating to data protection. For a full explanation of this service please refer to the Google and Apple documentation - https://www.google.com/covid19/exposurenotifications/ | https://www.apple.com/covid19/contacttracing

installed. Phones with national apps from different countries will continuously scan for other phones nearby with ENS active. When proximity is detected, the phones record this by sending each other random IDs without the need for any user action and include information on Bluetooth signal strengths to be used later for distance estimating. A rolling 14 days' worth of theses IDs and accompanying information, recording a person's recent encounters, are securely stored on the user's phone. These IDs cannot be used to identify you. Also, ENS, and thus Contact Tracing can be turned off and on, independent of the other app functions, at any time.

Positive diagnosis - if a person tests positive for the virus the HSE will contact the person by phone as per the current contact tracing processes. As part of the call, they will be asked if they are an app user and if they want to upload their random IDs to the HSE. If they are happy to volunteer their random IDs they are asked for their mobile phone number to which an authorisation code is sent via SMS. When the code is entered into the app, this authorises an upload of their IDs to the HSE. The HSE then publish these IDs, covering only the infectious period, on a publicly available registry. These IDs are subsequently referred to as 'diagnosis keys'. As the diagnosis keys are published publicly, they will also be available to other countries/ jurisdictions using the same Apple and Google Exposure

Figure 2: on positive diagnosis, a person can optionally upload their IDs

Notifications (ENS) software. In keeping with the voluntary nature of the app, users are not obliged to upload their IDs, but this will result in their close contacts not being alerted.

Making diagnosis keys available publicly means that the app will work when travelling abroad and that apps used by visitors from those countries will work here, noting importantly that neither public health authorities in Ireland or in other jurisdictions can identify anyone from the diagnosis keys at any point in the process.

Exposure notification - all apps download all new diagnosis keys every 2 hours from the registry and compare against the recorded IDs on their phone. The HSE registry consists of diagnosis keys from the Irish COVID Tracker App plus diagnosis keys for confirmed COVID-19 patients from other countries and jurisdictions, provided those countries use a national app based on the Apple Google ENS software and there are appropriate agreements in place between the participating national public health authorities.

If there is a match based on the HSE case definition, which is based on European Centre for Disease Prevention and Control recommendations that a close contact is within 2 metres for 15 minutes or more, the phone alerts the user that they have been exposed to someone who has tested positive for COVID-19. The phone displays the most recent date they were exposed and presents advice in accordance with public health guidance for close contacts, including restriction of movements. Exposure notifications (called "Close Contact Alert" in the app) remain visible on the app for 14 days from the date of last exposure. Users can clear exposure notifications from their app at any time via settings. If a user receives multiple exposure notifications relating to different exposure events, they only receive a new alert if the exposure notification relates to a more recent exposure event.
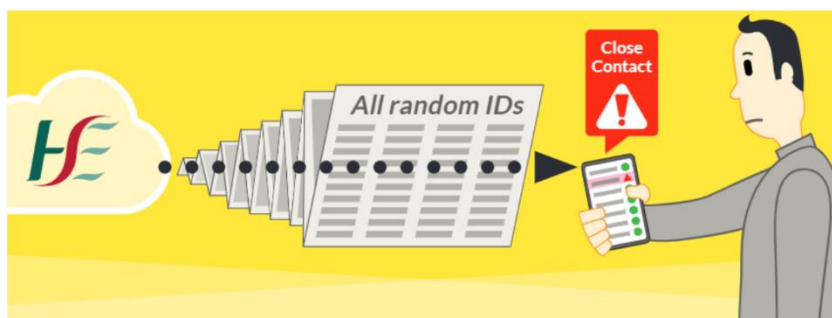
Figure 3: apps download new random IDs and alerts person if a match is found

If a user wants, they can record their phone number on the app asking for a follow-up call from the HSE in the event they get an exposure notification. If a phone number is stored in the app at the time of an exposure notification, it will send the phone number and the date of last exposure to the HSE. The HSE will call the person and guide them as per the current contact tracing operations. The phone number never leaves the phone unless an exposure notification occurs, and furthermore the HSE are not aware of an exposure notification in any way if a user chooses not to provide their number for a follow-up call. Note, if multiple exposure notifications are received by the app user, they will only get one follow-up call and will be informed to monitor for any new alerts.

3.2   EU Interoperability

To ensure contact tracing apps work seamlessly across EU borders, to avoid the need for EU citizens to have to download different contact tracing apps as they visit other member states and to protect those who don't travel from visitors arriving from other countries, the EU initiated an interoperability project in the summer of 2020.

In line with the Irish Governments decision to go live with the national contact tracing app on July 7th and to intensify efforts to achieve interoperability of contact tracing apps, Ireland is participating in the EU interoperability project.

The EU Commission Implementing Decision (EU) 2020/1023, was published in the EU journal on 15th July 2020, which formally approved the engagement of the EU and member states on the interoperability project. It lays down provisions on the role of the participating Member States and of the Commission for the functioning of the federation gateway for the cross-border interoperability of national contact tracing and warning mobile applications.

The project was led by DG Connect, DG Sante (eHealth Network), supported by DG Just, the European Data Protection Board and other relevant parties at EU level.

The EU Commission took on the role of developing a European Federated Gateway Server (EFGS), to be hosted by the EU. The purpose of EFGS is to act as a relay server so that the backend servers in each participating country can communicate with each other to share diagnosis keys and so achieve cross border interoperability. In this way, diagnosis keys uploaded to the Irish backend can be relayed to the backend server in other participating members states, so that their backend server can issue these keys to the app users in those countries. This ensures that Irish travellers who become Covid positive can alert app users in other countries. Conversely, the Irish backend server will receive keys from other countries which can be used to alert Irish app users that they have been in close contact with a visitor from another country who has subsequently tested Covid positive.

Given the advice of the European Data Protection Board (EDPB) in relation to how diagnosis keys should be treated, the EU produced a specific and comprehensive DPIA for the EFGS. As documented by the EFGS DPIA and in accordance with Annex III of the Implementing Decision (EU) 2020/1023, personal data uploaded to the EFGS will be disposed of once either all participating back-end servers have downloaded the respective personal data or 14 days have passed since the upload of the data, whichever is earlier. The EFGS stores the personal data that was uploaded for 14 days. After this period of time, the data is deleted with the help of a scheduling system that executes

a job to delete data whose retention period has expired. The DPIA also provides further details in relation to security measures in place to ensure the safety of the data being processed.

The EU are defined as the data processor for the interop service with each participating member state acting as joint data controllers. In Ireland, the data controller for the interop service is the HSE because it manages the day to day operation of the contact tracing app and will have operational responsibility for the interop service in Ireland.

The EU have established an on boarding process for members states to join the interop service, The associated documentation and participant agreements are used by the EU Commission as the mechanism to ensure all applicants meet the necessary data protection requirements in terms of their role as joint data controller.

Once operational, patients who carry the Irish app and are Covid positive will be advised that should they choose to share their diagnosis keys, these keys will be used to alert users of similar contact tracing apps from other EU member state apps as well as Ireland. Sharing of diagnosis keys by Covid positive patients is voluntary, is consent based and there is no impact on the care or treatment provided to the patient should they chose not to share their keys. Consent is provided once. There is not a separate consent for sharing with Irish app users only because this would result in the user not being protected from people visiting from other countries.

3.3 COVID Check-In

App users can choose to share with the HSE whether they have COVID-19 symptoms or not via the COVID Check-In function. Users can 'check in' once every day, independent of the other functions of the app. This information can create an anonymous collective daily overview of the progression of COVID-19 symptoms and an indicator of the spread of the virus informing public health policy interventions. Further information on this is provided in Appendix C. The Check-In function if used daily can also act as a memory aid for app users if it were needed to recall the onset of symptoms, a key piece of information for contact tracing. Furthermore on entering symptoms, guidance is presented to the user relevant to the symptoms entered in line with up to date public health policy.

The first time a person checks in with the COVID Check-In function they are presented with information on the function and the data processed and asked if they wish to proceed. If they proceed, they are further presented with an option to provide some demographic information about themselves. This information does not reveal a person's identity and is used to give statistical insights into COVID-19 symptoms in the country. The information consists of your sex, age range, your county and town if applicable. All of this information is optional and only prompted for during the first check in. Also, via settings in the app, this information can be updated and deleted at any time.

Figure 4: collecting demographic data

After asking for demographic information, and for every subsequent check in, a person is asked if they have any COVID-19 symptoms, and if so are brought through a series of four questions covering the relevant current symptom indicators as per public health policy: flu; cough; breathing difficulties; temperature. The app stores a rolling 28 days' worth of checked in symptoms, or lack thereof, and are available for users to review. Once filled out, the symptoms for the day plus the previous 27 days of symptoms if available, along with the demographic information, are shared with the HSE. 28 days of symptoms are shared with the HSE each time so symptom progression over time can be analysed.

On receipt of the data the HSE will securely transfer the anonymous data daily to the CSO. The CSO will prepare the data and publish it for the purposes of allowing health officials and public health teams (e.g. DoH, HSE, NPHET, NPHET subgroup IEMAG and other subgroups, HPSC) to interrogate
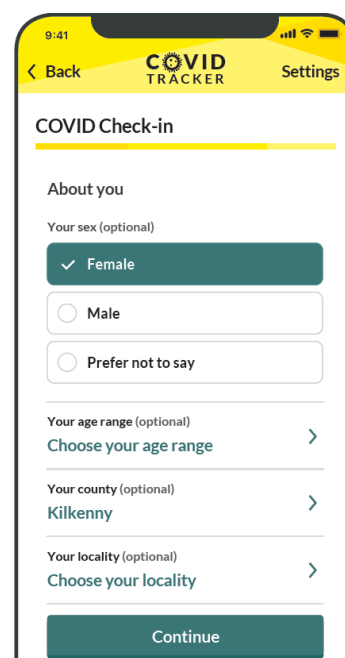
symptom progression over 28 day windows for the country broken down by sex, age range and general area, and for publication as appropriate to the public in line with the remit of the CSO.

3.4   News and information

The app will provide a further trusted convenient channel for the HSE and public health teams to share COVID-19 facts relating to Ireland's efforts to control the pandemic. This will include information such as number of cases, hospitalised cases, cases requiring ICU and deaths trending over time and other related key indicators. The information will also show users app related data such as an overview of the symptoms checked in by app users and the number of app users. The News and Information data is held securely by the HSE and apps on an hourly basis request the latest version of data to display.
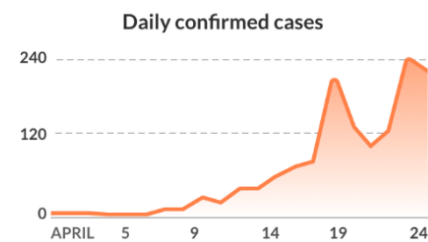
Figure 5: in-app COVID-19 facts and figures

3.5   EU Digital Covid Certificate (DCC) Wallet

The EU Digital COVID Certificate (DCC) is proof (in digital or paper format) that you have either:

- been vaccinated against COVID-19 or
- received a negative COVID-19 test result or
- recovered from COVID-19 in the last 6 months.

The Digital COVID Certificate will help citizens to travel safely and more easily within the EU during the COVID-19 pandemic. For people who want to store their DCC in digital form, the app provides a feature whereby people can choose to scan the QR code in the DCC and store its contents on their phone so they don't need to carry a paper copy of the certificates when they travel overseas. This 'DCC Wallet' feature as they are commonly known, is primarily a convenience feature and users can choose whether they want to use it or not. DCC data is held within the app and not shared. For example, when travelling, people can choose to use the app to display their DCC or present the same information using the paper version of the certificate. Using the digital version, people may be able to be alerted to issues arising such as an early warning for expiry dates for the certificate. You can delete your certificate from the app at any time.

3.6   Other Functions

Metric Gathering – the app seeks permission from the user to collect in-app metrics, and if given, records and shares data relating to how a person is using the app. This permission can be granted or revoked during the initial app 'on-boarding' screens and via the app settings at any time. The metrics collected do not reveal a person's identity and are shared on a daily basis with the HSE. The purposes for the collection of metric data are to understand if there are any functional problems with the app, how users are using the app, the impact it is having to help control the spread of the virus and to guide improvements in its design and functioning.

The types of metric collected include app abandonment points (especially during initial screens), use levels of app functions and constituent screens, numbers of exposure notifications, numbers of positive cases uploading random IDs. The metric data will be transmitted to the HSE on a daily basis by the app at a scheduled time without user action. All metrics will be sent to the CSO to publish for analysis by health and public health teams on a daily basis and used for the purposes outlined. The HSE will also store and analyse metrics in close to real-time relating directly to the performance and functioning of the app. Metrics are collected without the use of any 3rd party tools. A further breakdown of all metrics collected is include in Appendix D.

Leave Function – the app provides a leave function that can be used at any time. Selecting this deletes all app data from the phone. The user will be notified that they can also delete ENS data via the phone device settings as the app does not have direct control or access to ENS data. If Leave is selected, non-identifying security token data that is used to associate valid (device integrity checked)

apps with the app backend is removed from the app backend. If the app is simply deleted from the phone, it has the same effect as Leave, however the security tokens are not removed as the app backend has no way of knowing – they will be deleted after a period of 60 days of not being used.

App Settings – the app will provide a number of settings that can be configured by the user at any time. This section of the app ensures that users are given a clear view of the data that is being processed and allows them to give and withdraw consent. App settings provides the following:

- Contact Tracing function is displayed as on or off and the user is directed to the ENS phone settings where it can be turned on or off;
- The optional phone number for an exposure notification follow-up call can be updated or deleted;
- The demographic data that is included in COVID Check-In can be updated and deleted;
- Exposure notifications can be cleared from the app if relevant;
- A link to the Data Protection Information Notice for convenient access at any time.

Share function – the app makes it easy for users to share it with others who may choose to download it also. Success of contact tracing apps rely on widespread adoption by communities who collectively can help protect themselves and others.

3.7   Systems where personal data will be processed
Personal data will be collected, processed and stored in the following locations and IT systems:

1. The app – on users' phones where data is stored and encrypted on the device.
2. The app backend – the backend services are hosted by Amazon Web Services (AWS). The app uploads all COVID Check-In data, ID uploads and metric data to the backend services. The app also downloads IDs for exposure matching, and news and information from the backend services. All data is encrypted in transit and at rest, and is locked to the EU West Region.
3. HSE Contact Tracing Centre (CTC) services – this is the existing contact tracing centre operation. The app will integrate into the existing HSE contract tracing operations. The interaction of the COVID Tracker App with CTC includes the app sending a phone number for a follow-up call on an exposure notification; and CTC sending a phone number to the app backend to send an SMS code for ID upload authorisation.
4. The European Federated Gateway Server – which will act as a simple relay server for national backend servers to upload and download diagnosis keys from.

3.8   Technical Data Flows and Architecture
Technical data flows and the technical architecture of the app will be further set out in a series of diagrams which will be published online.[4]

4. Scope of Processing
This section of the document describes the data that will be 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.

4.1   Data Subjects
The proposed data processing relates to all individuals in the country that choose to download and install the app that have a smartphone capable of meeting the ENS requirements set out previously.

As stated in section 3.1, phones with ENS active will continuously scan for other phones nearby with ENS active. This happens regardless of which national contact tracing app is deployed on the phone,

---

[4] Technical documents on the COVID Tracker App will be published as soon as they are ready on the HSE and DoH websites and also on https://github.com/HSEIreland/

provided the phone is running the latest operating system from Apple and Google that incorporate the ENS service. ENS does not operate on phones that don't have a national contact tracing app installed. Phones with national apps from different countries will continuously scan for other phones nearby with ENS active

Whilst the Irish app can be used in other countries by those who need to travel, as other countries launch their own national apps, people living in those countries will be encouraged to download their own app i.e. the app released by their own national health authority.

4.2   Data Retention

There are various retention limits on different types of data being processed and these are outlined in tabular form later in this section of the document. An overarching policy of data retention in relation to the app is that no personal data will be processed beyond the period of the pandemic in line with recent European Data Protection Board's guidelines on the introduction of such apps. The terms of reference charge the App Advisory Committee to ensure that an orderly wind down of the app and the removal of all personal data is implemented within 90 days of the end of the COVID-19 crisis. The end of the COVID-19 crisis and the wind down of the app will be determined by Government taking advice from NPHET. The wind down will include measures such as of the issuance of clear guidelines for app deletion, removal of the app from app stores, the secure destruction of all personal data and diagnosis keys from backend servers, and the shutting down of all app backend services.

Users of the app have the right to be forgotten. Selecting the Leave function will remove all data held by the app and any security token data on the app backend. The Leave function will also inform the user that ENS is a phone service and will give guidance on how to remove ENS data via the ENS service settings. Deleting the app from your phone will also remove all app data from the phone, and the security token data will be automatically removed 60 days after last use. The removal of all app data and ENS data can be done at any time, and the HSE has no way of knowing who selects Leave or uninstalls the app.

4.3   IP Address

All API calls to the HSE will unavoidably result in app users' IP addresses being present in data communicated between the app and the HSE servers due to the nature of networking. The HSE will not use IP addresses for identification purposes. As a precaution, IP addresses of users are never transmitted from the networking layer to the backend servers thus minimising the possibility of inadvertently recombining IP address and payload data.

Under these circumstances it is reasonable to consider that the only personal data processed by the COVID Tracker app is:

1. The phone number provided by a user so they can be contacted in the event of an exposure. This is not a mandatory field. Users are given the option to provide this data should they wish to be contacted. Users will still receive notifications, advice and the option to initiate a call with the HSE themselves.
2. The mobile phone number used by the HSE for sending an SMS code to authorise the upload of random IDs to the registry on positive diagnosis. Users have the option not to upload these IDs.

However, without prejudice, this DPIA takes a conservative approach and considers IP address as personal data, and thus acts as a personal identifier. As such all app data transferred to and from the HSE backend servers relating to a person is considered personal data.

4.4   Download and Installation

To install the app, a user downloads the app from either the Google or Apple app stores. Each store will keep a record of the user's download of the app using their unique identifier, AppleID or GoogleID, with the store. Apple and Google are Data Controllers in respect of their respective app stores and gather certain statistics about app usage, such as number of downloads, number of deletions. More information is publicly available in regards how data is processed by the app stores.

4.5   Exposure Notification Services

It is worth going into further detail on the workings of ENS at this stage to support the rest of this section. Each phone that has ENS switched on generates a random daily key, which is stored on the phone, and called a Temporary Exposure Key (TEK). These keys are used to further generate random IDs approximately every 15 minutes called Rolling Proximity Identifiers (RPI), which are used to send to other ENS enabled phones when nearby. RPIs are accompanied by Associated Encrypted Metadata data, which includes protocol versioning and Bluetooth transmission power. The TEK keys are uploaded to the HSE on positive diagnosis and are called Diagnosis Keys at this point. These are publicly available, downloaded by all apps, and used to regenerate the RPIs – which are in turn used check for a match, on the phone, in order to generate an exposure notification. RPI and AEM data are processed on phones only; not available directly to contact tracing apps; are stored for 14 days; are not capable of being used to identify a person; and are not considered personal data.

4.6   Personal Data

The following scope for personal data processing has been determined. All data uploaded to the HSE should be considered to have IP addresses removed at the networking layer of the app backend and put beyond use. A rigorous data minimisation approach has been adopted to personal data processing and only personal data that is necessary for the proper operation of the app will be processed. The following table sets out the personal data that will be processed by the app, along with a description of the data, the type of data, how often the data is processed, who processes it and for how long. A more detailed technical list of all data processed by the app on the phone and on the backend servers will be published online.[5] Furthermore, more detail on the approach to data minimisation is provided in Appendix G, and data retention justification and measures to ensure data retention policies are adhered to are set out in Appendix H.

---

[5] https://github.com/HSEIreland/

Data	Activity	Type	Frequency	Processed By	Retention
Phone number Date of last exposure	A user can choose to store their phone number on the app for a follow-up call by the HSE if they get an exposure notification. The phone number along with the date of last exposure will, without user intervention, be shared with the HSE for a follow-up call if the app user receives an exposure notification. If no exposure notification occurs, it will remain on the phone and never shared.	On initial collection, this is considered personal data. If transmitted to the HSE it relates to a potential COVID-19 case and is considered personal health data.	All users have the option of registering their number with the app during on-boarding or at any time through app settings. Only those that receive exposure notifications will trigger a sharing of the number with the HSE.	The data is processed on mobile phones, and also by the HSE only on exposure notification as part of contact tracing call centre processes. The date of last exposure inform the length of movement restriction advice as per public health guidelines.	This phone number is securely held on the app until the user removes it via settings; selecting the Leave function; or uninstalling the app. The phone number, if sent from the app to the HSE contact tracing operations (CTC) for call back, will be processed as per the procedures for all identified close contacts via CTC.
Sex Age Range County Town (>90 population)	As part of the COVID Check-In function the user can optionally set the following, which will be shared with the HSE at every symptom check in: - Sex – Male, Female or Prefer not to say; - Age Range – 16-39 / 40-59 / 60+; - County; - Town - if applicable. Only towns with 90 or more population are stored to preserve anonymity.	This is considered personal data.	This data is processed each time a person performs a check in.	This data is stored on the phone and shared with the HSE. The HSE process it in order to securely transfer it to the CSO.	This data is securely held on the app until the user removes it via settings; selecting the Leave function; or uninstalling the app. This data is held by the HSE for 1 day after receipt to facilitate its transfer to the CSO. This data is retained by the CSO as anonymous data for statistical and research purposes in line with the CSO's data management policy.
COVID-19 Symptoms	This data consists of either no symptoms, or a yes or no to each of the 4 relevant COVID-19 symptoms: • flu symptoms; • breathing difficulty; • temperature; • cough.	This is considered personal health data.	On each check in this days' symptoms and the previous 27 days' worth of symptoms are shared with the HSE.	This data is stored on the phone and shared with the HSE. The HSE process it in order to securely transfer it to the CSO.	This data is securely held on the app for a maximum of 28 days, or until the user removes it by selecting the Leave function; or uninstalling the app. This data is held by the HSE for 1 day after receipt to facilitate its transfer to the CSO.

					This data is retained by the CSO as anonymous data for statistical and research purposes in line with the CSO's data management policy.
Diagnosis Keys	On positive diagnosis, an app user is invited by the HSE to upload their own diagnosis keys to the HSE. Only those authorised by the HSE can upload their diagnosis keys by typing in a code received by SMS. *The processing of the phone number required to send the SMS is discussed in the next row of this table.*	As this data is only processed when a person is diagnosed positive for COVID-19 it is considered personal health data.	Once per positive diagnosis of an app user.	The phone generates random IDs privately every day. On positive diagnosis, the app requests permission from the user to access these random IDs from the phone and then shares them with the HSE. The HSE publishes them on a public registry. This makes them available to other public health authorities who wish to use them to support raising close contact alerts in their own jurisdiction, provided their apps use Apple Google ENS software. All apps download any new IDs from the registry every 2 hours to check on their phone for exposure events.	Phones generating random IDs retain the data for 14 days unless the user deletes ENS data via phone settings. The registry stores IDs for 14 days. Apps download and process IDs to check for exposure events only for as long as is required to determine if there is a match or not.
Mobile number	On positive diagnosis, the HSE calls the person and if the person is an app user and opts in to upload their random IDs, they confirm their	As this data is only processed for a positive case it is	Once per positive diagnosis of an app user.	The HSE sends the mobile an authorisation code via an SMS to the phone.	As soon as the SMS is sent, the phone number is deleted, and only the code is preserved with the symptom date. The app backend has

Date (symptom onset minus 48 hours)	mobile number to which a code is sent via SMS to authorise the upload. On positive diagnosis, a person is contacted by phone as part of the existing contact tracing operations. If they are an app user, they will be asked to consent to upload their diagnosis keys, and to consent to the use of their contact details collected for contact tracing purposes to send an authorisation code via SMS. The app backend sends a code via SMS to the user, which they can enter into the app allowing the upload of diagnosis keys.	considered health data.		The HSE also stores the code along with the symptom date.	no way of knowing the phone number of a person that either uploads their keys or chooses not to upload their keys. The code is processed long enough to authorise diagnosis keys upload and retrieve the symptom date to determine the appropriate window of diagnosis keys to upload to the registry. It is deleted once this purpose is fulfilled or within 10 minutes, whichever occurs first.
Metrics See Appendix D for full breakdown.	Users can opt in to help analyse performance by recording and sending metric data to the HSE.	Some metrics measure counts of exposure notifications or diagnosis key uploads – this data is considered health data.	In general ,shared with the HSE daily.	The HSE process this data daily and use it to monitor near real-time performance of the app. The HSE securely transfer to the CSO all metric data within a day of receipt.	This data is retained by the HSE as anonymous data for statistical and research purposes for a minimum of 7 years and reviewed for further retention at that stage. This data is retained by the CSO as anonymous data for statistical and research purposes in line with the CSO's data management policy.
IP address and app security tokens	User IP address is required for internet traffic and is present at the networking layer of the app backend, but processed no further. Security tokens, which do not reveal identity, but note that the app installed has passed basic and standard phone integrity checks (e.g. a test that the app isn't running	Considered personal data.	On all app to app backend communication.	The phone and the HSE.	IP address is held in a transient manner on the networking layer for networking and security reasons. It is not persisted, nor logged on the app backend in any other way. The app security tokens are deleted on selection of the Leave function, or the deletion of the app (immediately on the phone, and after 60 days of

	on an emulator). This is primarily to stop illegitimate apps being used to attack the app backend APIs.				not being used by the app backend as the backend is not aware of an app being deleted.

5. Context of Processing

This section of the document sets out the relationship the HSE and DoH has with data subjects, how much control they have over the data processed, what type of people make up the data subjects. It also sets the context in regards the privacy concerns that people may have with the app.

5.1 Design Principles

Through how the app is implemented, the app's governance and the supporting communications, we will ensure a set of design principles are adhered to through the design, build and operation of the app. In particular, governance arrangements are in place via an App Advisory Committee where the terms of reference charge it to uphold a set of principles. These principles include the following.

- The app is entirely voluntary to use;
- The app is used to augment the existing manual contact tracing process;
- The app is used for the purposes set out in the DPIA, and only in the context of the COVID-19 crisis;
- The app is to be decommissioned once the COVID-19 crisis is over;
- The app processes data as set out in the DPIA, the DPIA is accessible to the public and is kept up to date;
- The app does not use location services to track the location of users or for any other purpose;
- The app does not, and will never, reveal the identity of a person infected with COVID-19;
- The app must be able to function while the screen is locked.

The trust of the public in the proposed processing of data and appropriate privacy measures are of paramount importance to engender adoption of the app. The HSE and DoH are committed to transparency in the development and operation of the app and to that end the source code and this DPIA document and related documents will be published to the public online as soon as they are ready.[6] These will be kept up to date to reflect the live operation of the system and the data being processed. Furthermore, robust processes will be put in place to perform security testing and respond to security issues during the development and the operation of the app.

5.2 Privacy Model

As mentioned previously, the Contact Tracing function uses a new Android and iPhone service called Exposure Notification Services (ENS). Only nationally recognised health authorities will be able to produce an app that is authorised to use ENS. Apps that do use ENS have limited levels of access to ENS data. Examples of this includes – apps are not allowed direct access to the random IDs being exchanged with nearby phones (RPIs); they are restricted in checking for exposure matches a maximum of 15 times per day; and they cannot get access to diagnosis keys without the user's explicit permission. In general apps are restricted in how they can use ENS in order to preserve the privacy design of the service. ENS follows what is informally called a 'decentralised' model for mobile app contact tracing, which allows people to get exposure notifications without sharing personal data with a health authority or anyone else. The HSE and DoH are also committed to this design principle. The HSE will independently test the robustness and security of the ENS service.

5.3 Children

Sixteen is the digital age of consent in Ireland. For that reason, prospective app users will be asked to confirm that they are 16 years or older at the time of downloading the app. App store controls will be put in place to restrict availability of the app to the extent that is possible. Google play store can restrict from 16 and above; while Apple app store can restrict from 12 and above – these settings will be applied. It is seen as a significant challenge to reliably seek parental consent to support younger users of the app at this stage. It is not clear at this time how this can be achieved in a practical way that can scale. Furthermore, it is not clear the appropriateness of alerting young people with exposure notifications as they may not be in the presence of a guardian at the time.

---

[6] Source code, DPIA and related documents will be published here - https://github.com/HSEIreland/, and on the HSE and DoH websites

5.4 Novelty and Robustness

The HSE and DoH are heavily engaged with other countries who are introducing similar apps to help stop the spread of the virus. As this use of phones is new, this type of engagement is important, and the project team will continue to engage, contribute and learn from others in the field. Furthermore, the team are in regular contact with Google and Apple, working with these companies to shape the design and functioning of ENS to maximise the value to society and people's health, while protecting the rights to privacy. The use of ENS is considered the best route to a robust working version of the Contact Tracing function. ENS is to provide the ability for apps that implement contact tracing to be functional on both Android and iPhone devices, with the app running in both the background and foreground, a significant challenge to date. Furthermore, it is expected from discussions with Apple and Google that ENS will be heavily optimised and tested for efficient battery use and will not interfere with other Bluetooth peripherals – also a significant challenge to date for current contact tracing apps.

The HSE and DoH are and will continue to engage in its own testing of the app to ensure the product is robust, reliable, and privacy preserving, including testing in an Irish specific context with regard to its particular environment (e.g. building types, typical bus configurations, etc.). The scientific community continues to play an important role in the Irish response to Covid-19. Science Foundation Ireland has been assisting the team throughout the development process and has convened several expert advisory groups to support four key areas: data analytics; Bluetooth proximity analysis; ethics and trust; and human-computer interaction. Lastly, the app will gather metrics, if users agree, which will be used to monitor and refine the functioning of the app and to measure its efficacy against its stated purposes.

5.5 Accessibility

The app has been carefully designed to be clear and transparent in how it works, to ensure consent, where sought, can be freely given, to make it possible for people to opt in (and out) of the functions provided, and to update their data at any time.

User Experience of the app has been tested within behavioural studies informing the app flow and content. There is little interaction required for setting up the Contact Tracing function, no user data is required, and it can run in the background without user interaction – thus reducing to as much as is possible any barriers to entry. Accessibility testing will be included in the app release and subsequent releases. An Irish version will be developed as soon as possible and released allowing people to choose to use the app in Irish or English. The support of other commonly used languages within the country will also be considered.

6. Stakeholder Engagement

A series of public and stakeholder consultations to support and inform the development and subsequent deployment of the app is part of the ongoing project activities. The purpose of these consultations is to gather views, perspectives, and experiences from experts and members of the public on a range of interrelated issues. From a development perspective, the following issues will be explored: privacy, appropriate use of data, cybersecurity, data accuracy, and accessibility. From a societal perspective, the following issues will be assessed: social inequalities, ethical implications, engagement with health services, and user expectations, needs and engagement.

6.1 Engaging the scientific community

Leverage the Irish research and scientific infrastructure is an important part of the Irish response to Covid-19. Throughout the development process the team have engaged with Science Foundation Ireland and their respective centres of expertise for expert advice and guidance in relation to four key areas: data analytics; Bluetooth proximity analysis; ethics and trust; privacy and security; and human-computer interaction. The project will continue to be guided by the input from these expert groups.

6.2 HSE National Patient Forum

The National Patient Forum was established in 2015 as a platform for collaborative partnership and engagement with patients/service users, family members and carers at national level. The Forum

ensures that patients, families and healthcare providers collaborate in policy development, implementation and evaluation and design and delivery of services. Membership of the Forum comprises patients, family members, carers, representatives of advocacy groups, disability organisations and Patients for Patient Safety Ireland. A wide range of organisations and groups are represented at the Forum. The app development team engaged with the National Patient Forum during the initial stages of planning and designing the app to gather their feedback and views. The app development team will continue to engage with the Forum following deployment and in relation to future version updates.

6.3   Ethics review

A panel of Science Foundation Ireland experts reviewed the project at an early stage of development, and this identified key ethics issues for consideration in the development process: public trust; data processing; misuse of data; personal benefits and educational purpose; age; accessibility; all-island; personal health tracking; privacy; future use. At an advanced stage of development, the project will also be considered by the Pandemic Ethics Advisory Sub-group of NPHET. Further, an expert international advisory group on ethics has been convened to review the project. The feedback and advice from these reviews will continue to inform the app development, deployment and version updates.

6.4   Research and evidence for policy

An extensive programme of research and development is informing the development of the app. This programme involves significant cross-governmental and cross-sectoral collaboration across HSE, the Irish Government Economics and Evaluation Services (IGEES), DPER, DoH, the Central Statistics Office, and the Economic and Social Research Institute (ESRI). The following research reports will be made available at the time of launch, on the Department of Health's website, and as part of the app online publications.[7]

1. Literature review: Digital Contact Tracing – Benefits and Enablers
    The purpose of this paper was to review the international literature to answer the following research questions:
    a) What are the benefits of digital contact tracing?
    b) What are the factors that enable effective digital contact tracing - from a development and operations perspective; and from a user and population perspective?
2. Evidence Brief: Profile of Smartphone Ownership and Use in Ireland
    This paper presents a national profile of smartphone ownership, and smartphone usage, and preferences and actions for managing personal information online. Data was from five nationally representative surveys of the Irish population conducted in 2018 and 2019.
3. User Experience: Covid Mobile App-User Perspectives and Experience – A Mixed Methods Study
    This paper summarises the methods and results of a study involving members of the public to provide their views on different aspects of the App design and features; and to observe and gather their feedback in real time while they were using a baseline version of the app for the first time. This process was used to improve aspects of the content and design. This is a well-recognised user experience research technique.
4. Behavioural Insights: Report of Recommendations from the NPHET Behavioural Change Sub-group
    The Sub-group reviewed a baseline version of the App to provide expert input into the design of the App.
5. Behavioural Study: An ESRI Behavioural Research Unit Experiment
    Survey research can provide a comprehensive overview of what might be expected in terms of user engagement. However, this evidence is made stronger when there is an opportunity to observe engagement. Therefore, the ESRI Behavioural Research Unit will conducted a large-scale user experiment. This type of experiment involves different groups of participants using different versions of app for several days, in their everyday life. The research team will gather data from the test versions of the app that the participants will use, and this data will

---

[7] App research and analysis reports will be published here - https://github.com/HSEIreland/

show a comprehensive profile of user engagement. The results of the study will help the development team to identify what features of the app work best in real-life.

7. Compliance with data protection law and other regulatory guidance

This section considers compliance with GDPR, the Data Protection Act 2018, other related legal obligations and data protection guidelines.

7.1   Legislative Framework

Under Section 7 of the Health Act 2004, the HSE is to introduce the app as a COVID-19 pandemic response app to protect the health and welfare of the public. The legal basis for the proposed data processing by the app relies on consent. The processing involves both ordinary and special categories of data and as such both GDPR 6.1(a) and 9.2(a) are used. Clear, explicit consent, in an intelligible and easily accessible form is sought for each of the personal data processing activities listed in the below table. Having regard for the entirely voluntary and discretionary nature of downloading the app, and noting that the HSE and DoH cannot determine whether a person has installed the app or not, it is not considered that an "imbalance of power" (GDPR recital 43) arises. Further information regarding the conditions for consent as set out in GDPR Article 7 are provided in Appendix I.

The HSE currently operate an existing manual contact tracing operation, which the app will interact with in defined ways. This DPIA makes clear these interaction points, what data processed by the app and app backend is possibly processed by the CTC, in what scenarios and for what purposes, and confirms that the user is appropriately informed. This assessment does not include an assessment of the CTC services, save to the points just made.

The following sets out the legal bases for the processing of personal data identified in Section 4 of this document. The processing activity is included in brief for convenience.

Data	Activity	Legal Bases
Phone number Date of last exposure	A phone number can be optionally entered by the user indicating their wish for a follow-up call by the HSE if they get an exposure notification.	The data processing indicates health status. Permission is sought before processing. The legal basis is consent – GDPR 9.2(a). Note, the HSE contact tracing operations on receipt of the data will use the phone number and last exposure date to call and give advice and processed in line with the existing contact tracing operations.
Diagnosis Keys	On positive diagnosis, the user can give their permission to share their non-identifying diagnosis keys with the HSE.	These keys indicates the health status of the person. Permission is sought before processing. The legal basis is consent – GDPR 9.2(a).

	The diagnosis keys are downloaded by all apps to check for a match.	On upload to the HSE, the IP address is stripped. This is done prior to the diagnosis keys being stored and made publicly available on the diagnosis key registry, and prior to being distributed to apps for matching. As such, the data is considered anonymous at this stage.
Mobile number Date (symptom onset minus 48 hours)	Contact details, including mobile number and symptom onset date are gathered as part of the existing contact tracing operation when a person is diagnosed positive. This data, on consent of the person, is further processed to enable the app backend to send an SMS code to authorise diagnosis key upload; and to filter out the appropriate set of diagnosis keys to distribute via the diagnosis key registry.	This data indicates the health status of the person. Permission is sought before processing. The legal basis is consent – GDPR 9.2(a).
Sex Age Range County Town (>90 population) COVID-19 Symptoms	Optional demographic data along with symptom data is recorded on the phone and shared by the user with the HSE on daily check in.	Sex, Age Range, County and Town are personal data – legal basis is consent – GDPR 6.1(a). Permission is sought before processing. Symptom data is special category data – legal basis is consent – GDPR 9.2(a).
	This same data is shared by the HSE with the CSO for statistical processing.	The data that is shared with the CSO does not include the user's IP address and as such, is considered anonymous.
Metrics See Appendix D for full breakdown.	This data is shared with the HSE for analysis.	Metric data processed on the app is a mix of ordinary and special category data. Permission is sought before processing. Legal bases is consent 6.1(a) and 9.2(a).
	This data is shared by the HSE with the CSO.	The data that is shared with the CSO does not include the user's IP address and as such, is considered anonymous.
IP address and app security tokens	The data is part of all app to app backend network traffic.	This processing is an ancillary purpose of ensuring network and information security. Permission is sought before processing. Legal basis is consent 6.1(a).

7.2 S.I. No. 336/2011 Obligations

The app involves gaining access to data already stored on the phone (e.g. app metrics, diagnosis keys upload, symptom data upload, etc.) and storing data on the phone (e.g. news and information, random ID exchanges, etc.) using a webservice and an electronic communications network and as such SI 336/2011 applies. All data that falls under this SI in regards the app is deemed strictly necessary in order to provide a service explicitly requested by a user, and as such the exemption set out in regulation 5 of the SI applies. The exception to this is metric data, where this data access is not strictly necessary in the provision of a service requested, and as such consent is explicitly sought for within the app before in-app metrics are collected.

7.3 Collaboration with the CSO

Anonymous data as outlined previously in this document will be shared with the CSO for the purposes of statistical reporting and analysis. The HSE will work with the CSO in the creation of statistical reports to inform the HSE, DoH and various public health teams on COVID-19 response policy making and measurement. The legal basis for this collaboration is Section 11(1) of the Statistics Act, 1993. An agreement has been entered into to reflect the terms of this collaboration.

7.4 Necessity and Proportionality Assessment

Necessity of processing requires that the proposed measures to be introduced will be effective for the objective pursued and whether it is less intrusive compared to other options for achieving the same goal. Proportionality of processing requires that the advantages of the processing proposed are not outweighed by the disadvantages the measures may cause to a person's rights, and as such, a balance must be struck between the means used and the intended aim.

Necessity and Contact Tracing – the need to operate a form of contact tracing during the COVID-19 pandemic is beyond doubt. The basic operating principle is that on diagnosing a person with the disease, the close contacts of that person are identified, generally through interviews, and appropriate measures are taken in respect of those persons so identified to control the spread of the disease. This is an effective intervention in the fight against COVID-19 and has been deployed worldwide. However, there are inherent challenges to manual contact tracing.

The review of international literature referred to in Section 6 of this document found that manual forms of contact tracing is overly reliant on recall (Leong et al., 2009) and it is argued that, for a highly infectious disease with a long incubation period, capacity to recall decreases and the likelihood of the disease being spread beyond known and usual contacts increases (Hart et al., April 2020). Furthermore, manual contact tracing also requires substantial human resources in the form of contact tracers (Hart et al., April 2020). Emerging literature suggests that manual contact tracing procedures is too slow, lacks efficiency, and occurs at too small a scale to contain Covid-19 (Ferretti et al., March 2020, Hinch et al., April 2020). Additional measures have been introduced in Ireland, and other countries, to aid in the control of the virus, such as severely restricting persons' movements, working habits and general day to day activities.

Key indicators of effective contact tracing are completeness of close contact identification and speed of close contact identification and subsequent follow-up, with a view to quickly and significantly reduce the viral transmission potential. The objective of using a mobile app based contact tracing solution as a supplement to the existing manual contact tracing is to increase the completeness of close contacts identified, and increase the speed in which those close contacts are identified and given the appropriate guidance.

A recent survey of over 2000 people carried out by Amárach Research on the 15th of May 2020 found that 70% of those surveyed would install a mobile app that carried out contact tracing (with 15% undecided). Recent introduction of mobile apps, though new and only published in a small number of countries so far (noting that almost all EU MS countries have indicated plans to introduce such apps in the future), have ranged in adoption from approximately 20% to 40%. Although a small uptake can have an impact on reducing transmission, it is clear that the higher the uptake the greater the positive potential of the measure.

The app user experience research referred to in Section 6 of this document and involving focus group and personal interviews whilst using a baseline version of the app found a high level of familiarity with the proposed app based on prior acceptance and experience with other health-behaviour change apps, and also a high level of willingness to download and use the app. Users reported that the 'ask' was simple and clear, from a trusted source, and for societal benefit. The participants were aware of apps in other countries and responded positively to this development in Ireland. The role of a supporting communications campaign was also highlighted by participants as part of the broader approach to deploying the app.

It is significant to note that Ireland is intending to introduce an app based on the Apple and Google's ENS service. Apps introduced in other countries to date have not been so based (as ENS hasn't been available), and have had significant functional difficulties, namely not functioning, or severely hampered functioning, on iPhones, issues with battery life, and interference problems with Bluetooth peripherals. Furthermore, these apps have generally been based on a 'centralised' approach, where the public health authority require access to significant amount of contact tracing data of positive and close contacts. Concerns over these factors may have hampered adoption.

The use of ENS is intended to solve the referenced issues regarding the basic core functionality proposition of proximity detection. Furthermore, it is based on the decentralised model, removing the need to share contact traces with a central authority. It is also expected that as more and more countries adopt the ENS service, which there is considerable momentum towards across the EU, a consolidation of improvements in product robustness and interoperability across borders will emerge. Alternative approaches to meeting the objectives stated above included the use of a centralised model and GPS/location tracking, and while certain benefits prevail over the proposed approach for Ireland (namely assistance in cluster identification), significant privacy concerns exist with these approaches and they are not being pursued.

In consideration of the objectives sought, the rationale and context for these objectives; the expectation that the proposed Contact Tracing function will be effective and adopted by people in light of the privacy preserving decentralised model chosen, and the ENS technology selected; the indicated support for installing such an app function; and the function being deemed the least intrusive measure to achieve the stated objectives, the proposed data processing in the Contact Tracing function of the app is seen to be necessary.

Proportionality and Contact Tracing – there is a clear and pressing social need for a fast and effective contact tracing operation, one of the main pillars in controlling the spread of the virus. There is a reasonable expectation that the Contact Tracing function in the app will meet the need to increase the completeness and speed of close contact identification and follow-up, when used in combination with the existing contact tracing operation currently in place. The challenges regarding completeness and timeliness of close contact identification and follow-up is a particular concern, especially as movement, social and work related restrictions are eased. The introduction of the Contact Tracing function of the app is expected to help mitigate these issues as person to person interaction increases, especially interactions where people are not known to each other or wouldn't be typically reported during a manual interview process.

Governance safeguards to limit the scope and extent of interference with data protection and privacy rights are in place through the terms of reference of the App Advisory Committee, ensuring data is processed in line with its purpose and principles, including the full wind-down of data processing when the COVID-19 crisis is over, and the ongoing monitoring of the effectiveness of the app and appropriate wind-down if it is not. Through the design and implementation of the Contact Tracing function these rights are further protected by ensuring it is and continues to be entirely voluntary in nature, that users are asked for their clear and explicit consent if they wish to turn on ENS, provide a follow-up call phone number, and upload their diagnosis keys. Importantly, if users wish to not have a follow-up call, they can receive exposure notifications without revealing any personal data to the HSE (save IP address).

Location services are never used to track the location of users, where instead Bluetooth is used to detect proximity without any location data, meeting its purpose in a data minimised way. Consent can

be withdrawn at any time for the processing of all Contact Tracing data and can be deleted under the control of the data subject, independently and without the knowledge of the HSE. There is no consequence to not using the app as the HSE cannot tell who has and who hasn't installed the app. Having taken into account the necessity set out above and the limited interference with data subject rights, the processing proposed under the Contact Tracing function of the app is seen as necessary and proportionate.

Necessity and COVID Check-In – the purposes of this function as previously outlined is to monitor the spread of COVID-19 related symptoms nationality, to provide an aide-memoire for people in recalling the onset of symptom data if needed, and to offer immediate advice on what to do if they have any COVID-19 symptoms. On the first purpose, "Syndromic Surveillance is the real-time (or near real-time) collection, analysis, interpretation and dissemination of health-related data from individual and/or population health indicators to enable the early identification of the impact of potential public-health threats/events which require effective public health action".[8] The current NPHET modelling does not include digital syndrome surveillance. The availability of daily COVID-19 symptom data through the check in function will enhance the existing epidemiological models that are used to track and manage the spread of COVID-19, improving the geospatial view of the spread of symptoms, its relation to virus progression, and to inform policy making for, and the evaluation of, virus management measures. As the data collected is for anonymous, aggregate statistical analysis, complete coverage is not necessary and a sample of the population using this function and providing symptom information would be deemed effective.

On the aide-memoire purpose of the COVID Check-In function, during the current contact tracing process a person who has been diagnosed positive is asked to recall the first day they had symptom onset. This date is important to calculate the viral shedding window so as to inform the period of time to enquire after close contacts. The recollection of the symptom onset date reliably can be a challenge. The use of a manual daily diary could be an alternative, however it is felt that the use of the app as a convenient alternative, which is also seen as adding to the 'national effort to help fight against the virus', would be more conducive to symptom journaling. Overall, the effectiveness of this function as a memory aid will be directly proportionate to its use, though noting that its impact when used, even if with a low uptake, could directly save lives by resulting in a more accurate contact tracing processing for individual cases.

The use of the function for quick and immediate access to guidance in relation to COVID-19 symptoms is expected to be effective for both users that regularly check in, and for those that may only check in once becoming unwell. Overall, in consideration of the objectives sought, the rationale and context for these objectives; the expectation that the proposed function will be effective in achieving these objectives; and the governance measures previously outlined in relation to the app, the proposed data processing in the COVID Check-In function of the app is seen to be necessary.

Proportionality and COVID Check-In – there is an ongoing need to increase the data availability to improve modelling for viral transmission and spread, so as to increase the understanding of symptom progression in combination and in relation to other markers. There is also a need to provide people with a channel via which they can feel they can participate in the 'fight'. Behavioural group studies carried out by DoH have revealed time and again a desire to contribute due to a feeling of powerless during the crisis. By checking in your symptoms every day this satisfies the need for enhanced syndromic surveillance, a memory aid and satisfies the desire to contribute.

The data that is processed as part of the COVID Check-In function will be stored securely on the user's phone, and shared anonymously with the HSE.[9] The demographic breakdown is optional, and clearly indicated as such. Furthermore, the demographic data can be updated or removed at any stage through app settings. The sharing of the data with the HSE is voluntary and if you do not check in, no data will be shared. The data can be removed from the user's phone at any stage. Participation or lack thereof with the function cannot be tied to an individual user by the HSE. The interference with

---

[8] http://hpsc.ie/

[9] Noted caveat – this transfer of data, as with any transfer of data, from the app to the HSE unavoidably contains the IP address. The IP address processing is strictly minimised as stated previously in the document.

individual's rights is considered limited and it is in this context, and in consideration of necessity outlined previously, that the proposed processing by the COVID Check-In function is seen as necessary and proportionate.

Necessity and proportionality of the News and Information – this function gives consistent and convenient and accessible access to facts, figures and graphs regarding people's contribution via the app and other COVID-19 pandemic indicators. It is seen as necessary to provide regular updates on the impact of the virus in a number of convenient and reliable channels. Similarly demonstrating the positive impacts that are achieved through the shared efforts of the entire population is considered necessary to maintain adherence to, and acceptance of, these measures over an extended period. The data processed does not reveal any personal data and has little impact on a person's rights. In line with this, the News and Information function is considered necessary and proportionate.

Necessity and proportionality of App metrics – the processing of app metric data is a supporting form of processing for the performance of the above functions and to monitor their effectiveness. It is also intended to give the public health teams insights into the functioning of the app, such as the number of exposure notifications per day, for use in health policy formulation and measurement. It does not collect, nor share personally identifiable information (save for IP address). Users consent to the collection of the data and can turn this on and off at any time. It is considered to have little interference with individuals' rights and is seen as necessary and proportionate.

7.5   Technical and Organisational Measures

Technical and organisational measures will be put in place prior to the launch of the app to ensure the information processed in relation to the COVID Tracker app is carried out only as detailed in this DPIA and ultimately only for the purposes intended. The HSE is designing, developing and putting in place the required organisational measures to ensure the privacy preserving approach to the app and the protection of the fundamental rights of individuals to privacy and data protection are established and maintained.

The organisational security measures implemented include the following.

- The HSE has engaged a specialist information security advisory at an early stage in the design, development, testing and operational planning of the app.
- An appropriate separation of roles will be employed, for example developers will manage the development and test environments, and the operations team will manage the production environment. The development team will have no access to the production environment, or data stored there.
- The app will be independently tested from an information security perspective. This will include the app on the phone and the app backend services.
- The Open Web Application Security Project (OWASP) will be a reference for the assessment of the App.
- All access to the app backend databases will be logged and the audit trails of this activity will be preserved. Audit logs of access are captured and reviewed for compliance by HSE IT Security.

The app backend uses Amazon Web Services (AWS) and the highly available services that it provides, and in so doing, the HSE has ensured an appropriate level of availability of the backend infrastructure to support the potential high level of take-up of the app. All services will be configured with appropriate availability groups in the Dublin region data centre from AWS and ensure the data resides only in Ireland. The use of AWS ensures that the solution can scale up and down in an elastic fashion to deal with demand.

Technical privacy and security measures are implemented via encryption at a number of levels and include the following.

- Data in the app - all data that is gathered and stored on the phone will be encrypted. On both the iOS and Android devices, the encrypted data will only be accessible once the app is launched, and then only by the app itself. The encryption does not rely on the device level

encryption that may or may not be enabled on the device itself. All ENS data – Diagnosis Keys, Rolling Proximity Identifiers, and Associated Encrypted Metadata – are stored encrypted by the phone's Exposure Notification Services.

- Data in transit – the data being transferred from the app to the app backend is encrypted using TLS v1.2 in transit (note - device fall back to earlier versions of TLS is not supported). Minimum TLS and cipher requirements are defined to prevent weak ciphers being used and leaving to potential for a "man in the middle" attack. The app will implement certificate pinning to ensure that the only site it will negotiate a TLS session with is the COVID Tracker App backend in AWS and not any other TLS enabled service. This also ensures that only COVID Tracker Apps will be able to negotiate a session with the AWS backend and limit any potential attack surface and removes the potential for attackers to flood the app backend with fraudulent symptom data.
- Data in the app backend – once the data has been received by the networking and routing layer of the app backend and processed, it will then be transferred to a database where it will be stored in an encrypted format. This database is not accessible from the Internet and is only accessible on a private network connection in AWS, from application servers.

A number of security hardening measures are in place to protect against malicious actors, these include the following.

- The HSE has engaged a Penetration Test and Application Security team to analyse the app code prior to release and ensure the technical security measures have been implemented correctly.
- This team will also perform Penetration Testing and Application Security Testing on the AWS API gateway (this is the service that the app communicates with in the app backend).
- Web Application Firewall is implemented to provide an application layer assessment of API traffic to remove potential threats prior to the data being processed by the API gateway.
- Continuous Vulnerability Assessment will be engaged for the API gateway and AWS services for as long as the service remains active.
- The team will be analysing the Bluetooth communications for Exposure Notification Services to ensure the integrity of the user device is maintained. The design of the app and contact tracing ensures that there is no requirement to "pair" the device from a Bluetooth perspective.

The app backend processes data in a secure manner, ensuring that inappropriate access is restricted at all times. The following sections speak to the various data sent by the app to the app backend.

Symptoms check-in data – this data once received by the app backend is transmitted securely to the CSO using a PKI-based sFTP from AWS to the CSO on a daily basis. The data is encrypted with the CSO Public Key. The data is retained by HSE for 24 hours from the day of receipt in case in order to facilitate the transfer of the data to the CSO. The data can be accessed by HSE Operations staff in appropriate roles. These roles are authorised by the HSE CIO. Audit logs of access are captured and reviewed for compliance by HSE IT Security.

Mobile numbers – when an app user has opted to share their mobile number with the HSE in case of an exposure event, the app calls an app backend API to share this number on such an event occurring. The mobile numbers shared are held within the app backend securely for the minimum period necessary to receive a HTTP 200 OK success status response code from the HSE API. The data can be accessed by HSE Operations staff in appropriate roles. These roles are authorised by the HSE CIO. Audit logs of access are captured and reviewed for compliance by HSE IT Security.

Diagnosis Keys – a request for Diagnosis Keys is triggered by the manual contact tracing operations based on a positive test result as part of COVID-19 core clinical pathway. The contact tracing centre will securely send the phone number and date (symptom onset minus 48 hours) to the app backend. The app backend in turn calls the Twilio service to generate a code and send an SMS to the phone. Twilio returns the code and this is stored for verification in app backend along with the date. The phone number is removed from the app backend at this stage. The code and date is retained for a maximum of 10 minutes.

The app user receives an SMS, enters code in app and consents to upload diagnosis keys. The app then calls an app backend API using an HTTPS POST with the Diagnosis Keys and the code. The app backend ensures a code match and uses the date information to store the appropriate Diagnosis Keys in the Diagnosis Key Registry. The code and date information are deleted from the app backend at this stage. A Web Application Firewall is used to monitor across all API services in particular the diagnosis key upload API for malicious activity.

App indicators and metrics – this data once received by the app backend is transmitted securely to the CSO in the same manner as described above for symptom data. The data is also securely stored on the app backend for real time, or near real time, analysis of the app performance and functioning. The data can be accessed by HSE Operations staff in appropriate roles. These roles are authorised by the HSE CIO. Audit logs of access are captured and reviewed for compliance by HSE IT Security.

IP address and security tokens – as mentioned previously and noting here for completeness, IP addresses are processed in the app backend at the networking layer and no further for the purposes of networking and network security only. The IP address is not logged on any service by the app backend. Also, as mentioned security tokens are created to protect the app backend from malicious actors. The first connection of an app to the app backend contains security measures such as ensuring the device is valid and not an emulator or a bot. This establishes the means of validating subsequent traffic from the app over its lifetime.

7.6   Exercise of Data Subject Rights

Users have rights under GDPR when their personal data are processed by data controllers. The following considerations should be noted. IP addresses are not retained on the app backend, but for transient network routing and network security purposes. Diagnosis keys are not capable of being associated with a person as they are non-identifying by design. Symptom data and related demographic data are anonymous once processed by the networking layer and cannot be associated with a person. A phone number if provided, to which a diagnosis key upload code is sent, is processed in a transient manner and is immediately deleted on SMS sending. A phone number if provided for a follow-up call is processed in a transient manner and deleted as soon as it is transferred to the contact tracing operation, and in that regard data subjects can exercise their rights under the contact tracing operation processes.[10]

Right to information – a Data Protection Information Notice (Notice) is provided in the app itself on those pages which request information and also in the app Settings. The Notice contains information as prescribed under Article 13 and 14 of the GDPR.

Right of access – the user can access data via the app itself and also submit a data subject access request to the HSE.

Right to rectification – the user has a right to have inaccurate personal data rectified and can make requests to have their data rectified to the HSE for data not processed on the phone, and can update data via settings on the app as set out in this document.

Right to erasure – the user can select the Leave function, delete the app at any time, and delete ENS data via device settings – erasing all data processed on the phone. Further deletion requests can be sent to the HSE.

Right to restriction – the user can revoke their ENS permission, revoke their exposure notification permission, decide not to upload keys, decide not to upload symptoms, sex, age range, county and town. Ultimately the user can decide to Leave and/or delete the App from their device.

Right to portability – it is not possible for users to port their keys, for example, from one device to another device as the user does not have access to such keys on their device (save to delete them) and as regards those uploaded to the HSE, the HSE cannot identify which keys belong to which user.

---

[10] https://www.hse.ie/eng/gdpr/data-protection-covid-19/

Right to object – the user can use the Leave function to delete the information from the app; the user can delete the app from their device and the user can delete ENS data via device settings.

Right not to be subject to solely automated decision-making including profiling – if the ENS detects a match between a Rolling Proximity Identifier on the App and a Diagnosis Key downloaded from HSE Diagnosis Key Registry, a decision is made that a close contact has taken place. This decision is based solely on the automated processing of identifiers and keys and does significantly affect users. However, this processing is based on the explicit consent of the user, when they enabled the service on their phone. If a user submits health symptoms which match symptoms of COVID-19, the app will present an advice message in line with public health policy. This is advice and not a confirmed diagnosis of COVID-19. The app is not making an automated decision as to whether or not a person has COVID-19, but based on the symptoms submitted, they are providing advice. The HSE provide similar advice in its current advertising campaign on the TV, radio, in print media and on social media.

7.7   International Transfers

One of the data processors, Twilio, is based in the USA and their server is outside the EEA. Twilio process the mobile number of users (obtained by the HSE outside the app through the existing contact tracing operations) in order to send an SMS message containing a code to a user who has been tested positive which enables that user to upload their keys Twilio have binding corporate rules (BCRs) in place to protect the data they process from the EU. Binding corporate rules (BCR) are data protection policies adhered to by companies established in the EU for transfers of personal data outside the EU. Note, AWS data centres used are located within the EU.

7.8   Subject to patient consent, diagnosis keys are shared with other countries and jurisdictions, provided those countries use a national app based on the Apple Google ENS software and there is an agreement in place between the participating national public health authorities. The Irish health system currently has agreements in place with Northern Ireland and the EU.
Appointment of Data Processors

All of the data processors are appointed under Data Processors Agreements in compliance with Article 28 of the GDPR.

7.9   Compliance with approved codes of conduct

Article 35 (8) of the GDPR provides that in assessing the impact of processing operations, due account should be taken as regards compliance with approved codes of conduct. Since early April, both the European Commission and the European Data Protection Board (EDPB) have issued documentation on the use of mobile apps for the fight against the COVID-19 pandemic that are relevant for the purpose of this DPIA.

The European Commission issued a recommendation on the 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis. The eHealth Network issued recommendations for a common approach to mobile tracing apps. The app has been assessed against these recommendations and it complies with all recommendations set out.

The EDPB issued Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak.[11] While the guidance is neither prescriptive nor exhaustive and the purpose is to provide general guidance, the app was assessed against the recommendations and obligations outlined in the documents. The app complies with conditions set out therein with exception of PUR-1. The App is a COVID-19 pandemic response app, and not solely one that performs contact tracing. In consideration of this and deciding to proceed with a pandemic response app, the following factors were taking into account.

- The app aligns with all other aspects of the guidelines 04/2020
- The relationship of PUR-2 and paragraph 40 with PUR-1 is noted, and both PUR-2 and paragraph 40 are completely adhered to.

11

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

- The relationship of symptom tracking and exposure notification is clear. To establish a robust exposure notification the window for viral shedding in line with public health policy of the index case must be determined. To assist in determining the window the recall of symptom onset is required, and the use of symptom tracking is highly desirable. Symptom onset recollection is a necessary part of contact tracing operations presently and is considered part of contact tracing.
- The potential for confusion of the introduction of similar multiple apps in app stores.
- The objective to have high adoption of the app to maximise the positive impact it is felt would be undermined by the diffusion of HSE COVID-19 apps on the app stores in relation to the pandemic.
- The clear messaging that the app will be a pandemic response app.
- The careful design of the app and the functions therein to be used independent of each other ensuring that they are both entirely optional. COVID Check-In can be used or not, while independently, Contact Tracing can be used or not. Both the functions have their own settings screens in the app, and their respective data is shown separately and can be updated separately.
- The clear alignment of purposes of the app functions with respect to the response to the pandemic.

The detailed assessment of the app against the above guidelines are to be published online.[12]

8. Identify and Assess Risks

Appendix E sets out the risks that have been identified for the project and the levels for those risks *if not mitigated*. Overall risk score for each risk identified is calculated as the product of the risk likelihood score and the risk impact score (i.e. likelihood score X impact score). The following sets out the metrics used in documenting the risk assessment.

Likelihood	Score
Highly Unlikely	1
Unlikely	2
Possible	3
Likely	4
Highly Likely	5

Impact	Score
Negligble	1
Minor	2
Moderate	3
Major	4
Critical	5

Overall	Score
Low	1-7
Medium	8-14
High	15-25

9. Identify Measures to Reduce Risks

An evaluation of the identified risks in the previous section has been carried out and a series of measures have been detailed that seek to mitigate those risks to an acceptable level. The table in Appendix F sets out these mitigation measures and an assessment of the risk impact due to their introduction. The table also sets out if these mitigation measures have been approved.

10. Sign off and Record Outcomes

Item	Name/Date	Notes
Risk measures approved by:	Muiris O'Connor, Department of Health; Fran Thompson, HSE 29/05/2020	Approved and confirmed risk measures to be implemented ahead of data processing.
Residual risks approved by:	Muiris O'Connor, Department of Health; Fran Thompson, HSE 29/05/2020	Approved.

---

[12] https://github.com/HSEIreland/

HSE DPO advice provided:	Jim O'Sullivan, 28/05/2020	Advice included below.
Department of Health DPO advice provided:	Mary Saunderson, 28/05/2020	Advice included below.
DPO advice accepted or overruled by:	Muiris O'Connor, Department of Health; Fran Thompson, HSE 29/05/2020	Advice accepted.
This DPIA will be kept under review by:	Muiris O'Connor, Department of Health; Fran Thompson, HSE	As per the terms of reference of the Governance Committee.

HSE DPO Advice:

I am happy, through the extensive process of engagement with the implementation team since the project commenced, that the DPIA has been completed to my satisfaction.

My opinion as the Data Protection Officer of the HSE is that it is in order to take the necessary steps to user-test and ultimately launch the app subject to the necessary data controller and data processor agreements being concluded.

I am satisfied that the use of the app in the community will assist with the contact tracing process and that the Covid Check-in function will help with the overall monitoring and management of the spread of COVID-19. In that regard, I believe that the introduction of the functionality of the app is both necessary and proportionate based on the principle of data minimisation and privacy by design and the necessary legal basis under GDPR i.e. consent has been established. I also note the intention to publish the DPIA and source code etc. which is helpful from a transparency perspective.

From a data privacy perspective, I note the decentralised nature of the app and I am satisfied that members of the public who download the app do so voluntarily, freely give their consent to use of their data and are free to delete the app at any time. I also note that the use of the app is limited to the duration of the pandemic with data being anonymous at all times.

I believe that the risks to personal and special category data are well articulated and the mitigation measures have reduced the residual risk to acceptable levels. I also note that the risk section requires sign-off by the project sponsors.

I welcome the intention to keep the operation of the app under review particularly in relation to uptake which is vital to its success.

Department of Health DPO Advice:

I note that the purpose of the App is to support the national public health response to COVID-19 and to support members of the public during the COVID-19 crisis. The HSE and DoH are joint data controllers. The HSE is responsible for the development, testing, security, operation and maintenance of the App. The role of the Department of Health is to provide strategic leadership for the App and to ensure that Government policies are translated into actions and implemented effectively. The HSE and DoH will enter into a joint controller arrangement and agreements will be in place with all data processors involved before the App rollout.

I understand that the App is based on a decentralised model, is voluntary to use and will only be used for the purposes set out in the DPIA. Measures are in place to decommission the App and delete all personal data when the COVID-19 crisis is over and a COVID Tracker App Governance Committee will focus on ensuring controls are in place for the safe, secure and appropriate ongoing operation of the App. I note that the source code and the DPIA will be made available to the public. The DPIA will be updated as required. The App does not reveal identities of persons infected with COVID-19 and will not use location services to track the location of users or for any other purpose. There has been public and stakeholder consultations to support and inform the development of the App. There will be processes put in place to perform security testing and

respond to security issues during the development of and the operation of the App. I note also that advices have been received, and the lawful basis for the processing will be based on consent under Article 6.1(a) and 9.2(a) of GDPR.

The Data Protection Information Notice, which I note from the DPIA can be accessed at any time, should make clear the different purposes the App will have, that an individual can choose which purposes they wish to sign up for and withdraw their consent at any time. It is essential that it is made clear to people in easy to understand language the purposes for processing their personal data, who it will be shared with and in what form and how long it will be retained for. The voluntary nature of this App should be emphasised, making it clear that the use of the App is entirely at the choice of the user and no detriment arises to them from not downloading it. However, the fact that the App has different purposes still may present challenges in providing data subjects with clear and understandable information.

With regard to the risk assessment, I note that a number of risks have been identified and that controls are outlined to address and reduce the risk to individuals' personal data. These will need ongoing review.

For this App to make an effective contribution to contact tracing, enough people must upload and use it. Public buy-in and trust in the way the App will be used will be key to this. If limited numbers use the App, a question will arise as to whether the data processing in the App is necessary. Consideration must also be given in this regard, to the proportion of the population that cannot use the App. There should be ongoing review of the uptake, effectiveness and use of the App, as well as continued engagement with stakeholders as the App is rolled out. The purposes of the App in relation to the response to COVID-19 are set out, this should also be assessed on an ongoing basis to ensure the App is not being utilised for any other purpose.

The risk in relation to children using the App has been reduced, however, these risks should be kept under review as the App is rolled out and further steps taken if required.

I agree that the DPIA should be reviewed and updated to reflect any material changes to the processing as this project progresses. I recommend that a copy of the DPIA should be sent to the Data Protection Commission.

11. Document Version History

Version	Date	Description
1.0	22/06/202	Initial publication
1.1	27/07/2020	Update of document to reflect that Ireland is to commence sharing of Diagnosis Keys, both giving and receiving. This means that the HSE Diagnosis Key registry will contain IDs from the COVID Tracker App, and IDs relating to verified positive cases of other ENS supported app users in other countries. This also means that Diagnosis Keys uploaded by users will also be shared via other public registries in other countries, as well as the Irish HSE Diagnosis Key registry – as it was at launch. This change is reflected in this document and the Data Protection Information Notice.
1.2	08/10/2020	DPIA updated to include a section that describes the introduction of the EU Interoperability service from October 2020.
1.3	14/07/2021	Updated to provide users with the option to store their EU Digital Covid Certificate (DCC) on their phone. This is intended as a convenience feature so people don't need to carry their paper certificate. Users can choose to disable the proximity detection feature in the app if they just want to use the app for storing their DCC. The wallet app is a standalone feature and data is only stored within the app.

Appendix A - Governance

COVID Tracker App Advisory Committee - Terms of Reference

An App Advisory Committee will be established to support the HSE in the national rollout and ongoing operation and development of a mobile app as a technical measure to enhance the existing contact tracing processes. The committee is to make recommendations to the App Implementation Team and make submissions to the HSE CEO and the HSE and DoH Data Protection Officers as it deems necessary, in line with its obligations. The committee is to support, guide and oversee the activities of the implementation team in the following regard.

- Oversee that any enhancements of the mobile app are in line with the app design principles set out in this document;
- Oversee that the functioning and use of the app is aligned with the purposes of the app as set out in this document;
- Oversee that the ongoing development and use of the app aligns with public health policy;
- Oversee that effective monitoring is in place to assess the ongoing efficacy of the app in contributing to the HSE COVID-19 response;
- Oversee that the app is wound down within 90 days if the app is assessed as ineffective as part of its efficacy monitoring process (above), or if, on taking advice from NPHET, the COVID-19 crisis is declared over by Government;
- Oversee that due consideration is given to relevant guidelines issued by the European Data Protection Board and the European Commission;
- Oversee that the app is and continues to be used in an entirely voluntary basis, and if anything should undermine this principle to report to Government, with proposed appropriate measures, including the potential to legislate, to protect the voluntary nature of the app;
- Provide guidance and advice and cross sectoral knowledge in the ongoing operation and development of the app;
- Oversee the implementation of a communications plan to ensure the app is rolled out in a transparent manner that supports its voluntary adoption;
- Oversee that the app processes data in line with the DPIA and that the data controllers keep the DPIA up to date and public;
- Oversee the transparent rollout and use of the app through the public release of documentation and source code.
- Oversee the ongoing organisational and technical measures in securing the processed data.

Membership

Membership will be established on the basis of nominations of senior HSE officials appointed by the HSE CEO. Furthermore, the following organisations will be invited by the HSE CEO to nominate a suitable representative - the Department of Health, the Department of Public Expenditure and Reform (Office of the Government CIO), the Central Statistics Office, Science Foundation Ireland, and nominees from civic organisations. The HSE CEO will nominate a suitable chair.

Additional members from other organisations may be invited to attend and contribute from time to time as the Committee sees fit in line with its terms.

Meetings & Reporting

- Meetings will held be as needed and will be regulated by the members of the committee in line with the evolving requirements of the rollout and operation of the app.

App Implementation Team

- In addition to the broader oversight governance set out in this appendix, the HSE internal App Implementation Team reports into a HSE Steering Group for Testing and Contact Tracing. The App Implementation Team is led by the HSE CIO, Fran Thomson, and in respect of the app's implementation, reports into the Steering Group.

App Design Principles

The app design principles that the App Advisory Committee is charged with overseeing the upholding of are the following.

- The app is entirely voluntary to use;
- The app is used to augment the existing manual contact tracing process;
- The app is used for the purposes set out in the Data Protection Impact Assessment, and only in the context of the COVID-19 crisis;
- The app is to be decommissioned once the COVID-19 crisis is over;
- The app processes data as set out in the DPIA, the DPIA is accessible to the public and is kept up to date;
- The app does not use location services to track the location of users or for any other purpose;
- The app does not, and will never, reveal the identity of a person infected with COVID-19;
- The app must be able to function while the screen is locked.

App Purposes

The COVID Tracker App is designed to serve as a nationwide COVID-19 pandemic response mobile application. The app, which will be entirely voluntary, is to support and augment the HSE's COVID-19 pandemic response efforts including contact tracing, symptom tracking, epidemiological analysis, and the provision of a trusted and reliable source of COVID-19 related information to users. Specifically, the app will have the following purposes.

Purpose 1: To support the national public health authority's response to COVID-19 by

a) Enhancing the existing HSE contact tracing operation
b) Monitoring and mapping the spread of COVID-19 symptoms

Purpose 2: To support members of the public during the COVID-19 crisis by

c) Providing COVID-19 related news, information, and national updates on the app
d) Storing a personal record of symptoms on the app

Other

- Funding requirements for this initiative will be the responsibility of the HSE.
- Secretariat to the App Advisory Committee will be provided by the HSE.
- The existence and operation of the App Advisory Committee will continue until such time as the app is wound down.

Appendix B – Data Processors

Data Processors

The following provides a list of data processors regarding the app.

Amazon Web Services is where the HSE processes the information uploaded from devices. AWS are a data processor**.**

NearForm were chosen to develop the App and are regarded as a data processor as, during development and testing, they may have access to some personal data.

PFH Technology Group are the existing ICT partners of the HSE and provide operational support for AWS.

Twilio send a text message with a one-time validation code to enable a user who has received a positive or presumed positive diagnosis to upload their non-identifying Diagnosis Keys to the HSE.

ISAS are providing data protection and information security advice to the HSE and DoH as well as vulnerability assessment and penetration testing on the app and AWS backend services.

Apple and Google

The following is a note on Apple and Google's role.

The app can be downloaded free of charge from the Apple App Store and the Google Play Store. In this regard they are independent controllers as they process account names in order to make the app available. This processing activity is separate to the processing of personal data on the app. Furthermore, although Apple and Google have developed a COVID-19 Exposure Notification Services service, which is used in the app, neither company obtain any information from the app or the Exposure Notification Services service itself.

Appendix C – Syndromic Surveillance

Note on syndromic surveillance (COVID-19 symptoms) and data processing

Syndromic surveillance is used for early detection of outbreaks, to follow the size, spread, and tempo of outbreaks, to monitor disease trends. For citizens, syndromic surveillance provide reassurance that an outbreak has not occurred and provides early indicators of recovery.

Optimal syndromic surveillance requires real-time health data to provide immediate analysis and feedback to public health emergency teams, and to test and inform public responses. Digital and location-based methods of symptomatic surveillance maximise detection while preserving limited health service resources.

For Ireland, digitally enabled syndromic surveillance enabled by the COVID Tracker App will provide real-time epidemiological information not currently available to then National Public Health Emergency Team (NPHET) responding to COVID-19. This syndromic surveillance will not replace but will augment existing public health surveillance measures and modelling.

The anonymised data will be securely stored and processed by the Central Statistics Office. Anonymised micro-data will be presented on an internal-facing dashboard with geo-spatial mapping to be used by the NPHET for decision-making, and NPHET sub-groups engaged in epidemiological modelling, and health communication.

Aggregated daily indicators will be made available publicly for the purpose of national public health communication and citizen engagement through the App, in addition to current public reporting systems.

Appendix D – App Metrics

The metric data to be collected during the operation of the app cover 4 areas: adoption and use; contact tracing; symptom tracking; and, epidemiology. The purpose of the first three areas is performance monitoring, while the fourth is analysis and modelling. Data is measured daily for each indicator and can be reported daily, cumulatively, or as events occur.

Indicator area	Indicator focus	Output indicator	Description
App adoption and usage	App adoption	1. Number app downloads	Number of App Downloads from the Google Play Store and the Apple App Store. This metric supports monitoring national roll-out; provide early warning of non-adoption; monitor trends in adoption; monitor adoption numbers vs potential adoption numbers.
	Active app users	2. Number of app users with app active	Number captures how many people that open the app at least once on a daily basis. Monitor trends in active use; provide early warning of lowering active use.
	App abandonment	3. Number of app users who delete the app or select the Leave function	Track the number of users who delete or Leave the app. Monitor trends in abandonment; provide early warning of abandonment.
		4. Number of app users who drop out of the on-boarding process	Track the number of users who commence but don't complete on-boarding. Monitor trends in abandonment; provide early warning of abandonment and on-boarding difficulties.
Contact tracing	Active contact tracers	5. Number of app users who have exposure notification services enabled	Tracks the daily size of the contact tracing network. Used to monitor the scope and activity of the app-enabled contact tracing network.
	Close contact exposure and diagnosis	6. Number of close contact notifications	Tracks the number of close contact notifications that are being raised for users that fit the close contact case definition. Monitor the scope and activity of the app-enabled contact tracing network.
		7. Number of close contact notifications who tap in-app notification	Tracks the number of close contact events that are being raised and if the user reacts to the in-app notification. Monitor the effectiveness of the in-app notification as an alert mechanism. Monitor the scope and activity of the app-enabled contact tracing network
		8. Number in app contact tracing network with a positive diagnosis	Tracks the number of users in the network with a positive diagnosis for COVID-19. Disease monitoring and

			epidemiological modelling; quality assurance of app functioning and configuration.
		9. Number of app users who uploaded diagnosis keys	Tracks the number of users in the network with a positive diagnosis for COVID-19 who have uploaded diagnosis keys to alert other users. Disease monitoring and epidemiological modelling; quality assurance of app data. Measure user engagement with contact tracing operations.
		10. Number of matched diagnosis keys per positive exposure notification	Measure the number of exposure events per positive exposure notification. Monitors the configuration of how ENS is used to trigger exposure notifications.
		11. Number of days between app notice of exposure and communication of positive test result	Tracks the number of days between app notice of exposure and upload of diagnosis keys (indicating a positive test result) for relevant users. Disease monitoring and epidemiological modelling; quality assurance of app functionality and configuration.
		12. Ratio of exposure notifications to positive cases	Used to understand the relationship between exposure notifications and positive diagnosis within the app user network. Disease monitoring and epidemiological modelling; quality assurance of app functionality and configuration.
Symptom tracking	User symptoms	13. Number of symptom check-ins	Monitor population coverage of symptom tracker data
		14. Number of check-in no symptoms: check-in with symptoms	Monitor population coverage of symptom tracker data

Appendix E – Identified Risks

The following sets out the *unmitigated* risks that have been identified for the project.

No.	Risk	Likelihood	Impact	Likelihood Score	Impact Score	Overall Risk
1	The app is a COVID-19 pandemic response app. The purpose of the app is to support and augment the HSE's COVID-19 pandemic response efforts through the use of a mobile app. There is a risk that the scope of the purpose will increase to include, for example use by other public bodies, or for enforcement purposes	If the app is successful there is a high risk that other uses will be seen as attractive to introduce. Also, uses may include informal use in the private sector for purposes the app is not intended for	Any increase in app purposes has the potential to impact all users of the app, and to potentially undermine public confidence in the app	4	5	20
2	Data may be collected about children in the app. How will the app determine the age of the user and how will child consent be collected brings additional risks	If unmitigated it is certain that children, under the digital age of consent, will attempt to use the app	Data would be processed potentially on the basis of consent without it being validly collected; unsupervised reception of an exposure notification may not be understood or may cause disproportionate alarm without a guardian present to assist	5	4	20

3	Risk that suitable ways of withdrawing consent are not built into the app in particular as consent is used as a legal basis for data processing	It is very likely that data subjects will seek to withdraw consent and if not provided for explicitly and carefully via mitigation there is a high likelihood of manifestation of risk	Data subjects have a right to withdraw consent at any time. Inability to exercise this right in an easy and cost-free manner would be a serious breach of data subjects' rights.	5	4	20
4	There is a risk of pollution of diagnosis keys due to bad actors	It is somewhat likely that someone will try to inject bad data into the diagnosis key registry	This would compromise the system and at scale would undermine it resulting in many false exposure notifications and high impact on users	4	5	20
5	Users losing control of their mobile device allowing people to see personal, and sensitive personal data.	Highly likely that this will happen to a small number of people.	If this occurs, users may have their symptoms, or an exposure notification warning accessed by third parties, known or unknown to them, and suffer distress.	4	4	16

6	A pandemic response app may not give sufficient benefits to support the case for the proposed large scale data processing	The introduction of a novel approach to contact tracing using technology in a novel manner give rise to a significant risk.	The potential for mass processing of data by the HSE could have a significant impact on the rights of data subjects	4	4	16
7	Sufficient people must use the App in order for it to make an effective contribution to contact tracing. Consideration must be given to what part of the population cannot use the App, e.g. people with no or outdated device, children etc. The risk is that data is collected about a proportion of the population but does not bring the expected benefits.	There is evidence from other countries that take-up of the App has been slower than they expected	If limited number of people use the app then it calls into question whether the data processing in the App is necessary.	4	4	16
8	Risk that the Bluetooth proximity and power measurements record that a close contact occurred however a false positive was recorded e.g. reading was made through wall/glass and the person was not a genuine close contact	While Bluetooth is the more accurate solution compared to other solutions available, it is not absolute	People would be designated as being in close contact with a person infected with COVID-19 and asked to follow public health guidelines, including quarantine	4	4	16

9	Risk that the Bluetooth proximity and power measurements do not record that a close contact occurred and no contact is recorded when a positive contact actually did occur (a false negative).	While Bluetooth is the more accurate solution compared to other solutions available, it is not absolute	People who have been in close contact are not identified and asked to self-isolate potentially spreading the virus	4	4	16
10	Risk that data will be transferred outside EEA and not subject to GDPR.	Many services transfer data outside of the EEA unless specified in advance that this may not occur	Data controllers and data subjects may not be able to enforce their data protection obligations and rights	4	4	16
11	Risk of insecure methods of data transfer are used that allow access to user's symptoms, or any other data transferred to the HSE (if it could be identified as coming from their specific phone).	Likely that attempts will be made to intercept transfers	Special category data from symptom tracker needs to be transferred securely.	4	4	16
12	Effectiveness in border areas where people live and work either side of borders could undermine effectiveness and thus justification of data processing proposed	The likelihood of this risk occurring is high for a number of people	The impact on effectiveness of app for those that live for example in Ireland and work in Northern Ireland, and vice versa in regards the Contact Tracing function would be significant. Similarly for those on holidays or indeed also working or visiting other countries regularly, or visitors from other countries to Ireland would be significantly impacted	4	4	16

13	Risk that bundling of related features in the pandemic response app infringes on the data protection principle of data minimisation	Without careful consideration and design the likelihood of this occurring is high as the app	The impact would be a potential infringement for all users that would wish to not participate in all functions provided by the app	4	4	16
14	The use of analytic data gathered from the device for the purposes of how the users interact with the app, daily use, app abandonment, contacts, exposure events, etc., is not anonymous and unexpected to the users. Risk to users that data is not anonymous.	Unmitigated, there are possibilities to intentionally and/or unintentionally use metric data from the device for purposes other than the stated intent	If metric data is inappropriately processed, it could have a significant impact on data subject rights and also greatly undermine users confidence in the app	3	5	15
15	Users are not given sufficient information about how the app works, what data will be collected and for what purpose in a comprehensive way	The requirement to have excellent communications about the app is understood	If the transparency information is not provided in a comprehensive way then this will impact the number of people who will use the app and as consent is used as a legal basis can lead to it not being given without being fully informed	3	5	15
16	Risk that Contact Tracing can be used to identify and track people's location and for profiling purposes, rather than tracking the virus	Uploaded contact traces or data in relation to contact occurrences may be difficult to protect against re-identification and tracking	If conducted then there would be a major risk to the data subjects and their right to privacy	3	5	15

17	Individual perception of symptoms can be subjective or lack of understanding of symptoms could lead to misreporting. User might not record their symptoms regularly enough.	Very likely to happen in some cases	Mass roll out of the symptom tracking application capability could result in data of variable quality of self-reported symptoms for a small to moderate number of cases, which could reduce quality of analysis and actions	5	3	15
18	As the app knows when a person is uploading their diagnosis keys, risk the app can be used to display the COVID-19 status of a person and be used outside of its purpose	If any COVID-19 status is visible in the app, it is possible it will be used	A third party could attempt to make decisions about the data subject based on their COVID-19 status as recorded in the app.	3	5	15
19	The use of the app may continue indefinitely or longer than justified by the defined purposes	If unmitigated, the app could continue to operate on people's phone unless a positive intervention is put in place	Swapping of random IDs could continue and statistical data continue to be gathered without a supporting purpose. Exposure notifications wouldn't occur assuming manual contact tracing operations cease.	3	4	12
20	IP address is present in all data transfers from the app to the app backend	Apps are often designed to capture information from the mobile device such as the device IP address	The capture of IP address and other identifiers from the device permit the data subject to be identified	3	4	12
21	The risk that SMS code provider can identify that particular person with particular notifications and then infer the COVID-19 positive status of the device owner	The App will send and receive one time codes so this risk is likely to occur. There is a need for an Authorisation token to prevent spamming of the API. The use of push notifications via SMS is	There would major impact for users if they could be tracked.	4	3	12

		the optimum method of doing this.				
22	There is a risk of pollution of symptom statistics data and metric data by bad actors	It is somewhat likely that someone will try to inject bad data into the symptom or metric data API	This could compromise the statistical data, and obviate the need to process that data in the first place	4	3	12
23	Technical issues with the app that would reduce function or interfere in a negative way in the working of the other phone's function, thus reducing user engagement, lessening the app's effectiveness, and weakening the case for data being processed.	App could have potential issues around a. Technical – users blame the App for loss of battery life or other similar issues b. Usage – the operation of the App is hindered by the interface with the mobile device operating system	Technical issues with the App reduce user engagement and lessen its effectiveness in providing contact trace data.	4	3	12
24	Role of Apple and Google may process data in a non-privacy enhancing way in the future, or in a way that is not desirable in respect of the rights of data subjects, that is unexpected	Exposure Notification Services from the start has been designed to protect privacy in a data minimised way, in line with the EDPB guidelines from the start of their endeavour	If Apple or Google started to gather and use contacts data for their own purposes form within the Exposure Notification Service this could impact on individuals' data protection rights.	2	5	10
25	Integrity of data is compromised. The diagnosis keys, or mobile number uploaded to HSE servers is erroneous or corrupted, meaning it is unusable or unreliable.	Unlikely to happen if standard development practices are followed	If this happened on a large scale contact tracing efforts could be negatively impacted and users might lose confidence in the app.	2	5	10

26	Users may decide to turn off the Bluetooth service on their phones for battery life or other reasons.	Users have the ability to turn on or off various services on their phones and are somewhat likely to do so.	Turning off Bluetooth would disable the Contact Tracing function	3	3	9
27	Continually downloading Diagnosis Keys may consume a user's network data allowance.	Some users may still be on Internet packages that have a low monthly data limit.	This could incur additional costs for the user.	3	3	9
28	Users can't exercise their data protection rights or don't know where to go to exercise them.	The requirement to be able to allow users to exercise their rights is well known and reasonably unlikely.	Failure to provide for users rights would have a major impact on users and affect the number of people who will use the app	2	4	8
29	Where the data is stored on servers of US companies, US Government could use the Cloud Act to attempt to access the data	The likelihood of this risk occurring is unlikely as there are already protections in place	The impact is likely only to be on a very small number of users as personal data held on app backend is minimal (transient IP addresses, transient mobile numbers)	2	2	4
30	Patients may be less likely to upload their diagnosis keys when advised they will be shared with other countries as a result on interop capabilities going live	The likelihood of this risk occurring is low based on experience to date with interop with Northern Ireland contact tracing app	The impact is limited only to those individuals that are diagnosed as covid positive, are using the app and agree to upload their diagnosis keys	2	2	4
31	As interop goes live, users will be downloading diagnosis keys derived from Irish app users plus keys derived from compatible apps in other countries, which will consume more of the users network data allowance.	It is almost certain that the data downloads will increase as Ireland receives more diagnosis keys from more countries	This could incur additional costs for the user.	3	3	9

Appendix F – Mitigated Risks

The following table sets out the risks identified for the projects, measures to mitigate these risks and whether those measures have been approved.

No.	Risk	Measures to Mitigate Risk	Likelihood with measures in place	Impact with measures in place	Residual Risk	Measures approved	Remaining risk to data subjects
1	The app is a COVID-19 pandemic response app. The purpose of the app is to support and augment the HSE's COVID-19 pandemic response efforts through the use of a mobile app. There is a risk that the scope of the purpose will increase to include, for example use by other public bodies, or for enforcement purposes, or for other purposes not in line with the original purpose	- Implement clear and transparent communication including DPIA and source code publication - Terms of reference of the App Advisory Committee to include the purposes and to charge the Committee with ensuring data is processed in line with those purposes and any changes are carefully assessed, are lawful, are lawfully introduced, and reflected in the DPIA - Ongoing assessment of the app, the data it processes and in particular an ongoing assessment for changes from an ethical, data and privacy perspective - Ensure app is entirely voluntary to use - Monitor continuously for misuse that violates the app's voluntary nature with a view to legislating if required to protect this design principle - Charge Governance Committee with wind down once the COVID-19 crisis is over	2	1	2	Yes	Little risk remaining to data subjects if all measures are implemented as all changes require to respect legislation, and informal (outside of public bodies) use will be protected if misuse is detected
2	Data may be collected about children in the app. How will the app determine the age of the user and how will child consent be collected brings additional risks	- The app will check that age is 16 years or older at the start of the on-boarding journey after installing the app. - The integration with the app stores will prevent the use of the app by children under the age of 16 on the Google Play Store; and under the age of 12 on the Apple App Store (the next restriction is under 17, which excludes 16 year olds who are old enough with regard to digital consent - 12 if the next available restriction below 17) - Communication to ensure parents understand the age intention of the app	3	2	6	Yes	Scope of children at risk is significantly reduced with the introduction of mitigants, though not entirely. To be kept under close reviewed during rollout of the app.

3	Risk that suitable ways of withdrawing consent are not built into the app in particular as consent is used as a legal basis for data processing	- App to provide ability to change consent settings for all consents given, individually, via settings at any time - Use the Leave option on the app - this will delete any personal data held on the mobile phone, and any data that can be linked to their phone on the app backend (i.e. security tokens) - Delete the app from their mobile phone at any time - will leave security tokens for 60 days until removed from lack of use - People can write to the HSE asking for any identifiable personal data to be deleted where it was processed on the basis of consent (noting IP address is transient, diagnosis keys and symptom data are anonymous)	1	1	1	Yes	Introduction of mitigants through careful design ensures that it is clear for users how to withdraw consent at any time to their data being processed
4	There is a risk of pollution of diagnosis keys due to bad actors	- Put in place an appropriate HSE authorisation step so that only those authorised as having tested positive for the virus can upload their keys - Ensure network and WAF security measures are put in place to block attacks of scale - Ensure device integrity checks are first performed by the app during the on boarding, and to ensure for all traffic to the app backend is protected via this means	1	1	1	Yes	After mitigation it is unlikely to occur
5	Users losing control of their mobile device allowing people to see personal, and sensitive personal data.	- Ensure app can run in the background and when locked (current apps on iPhone require running unlocked at significant risk). - The communications plan for the app will remind people that they should take suitable precautions to protect their mobile device.	4	3	12	Yes	This risk remains as the symptom data is in the App and even with a clear communication plan other people will have access to user's mobile phones.

6	A pandemic response app may not give sufficient benefits to support the case for the proposed large scale data processing	- Carry out of an analysis of benefits to support the introduction of an app is to be carried out and inform launch decision. - Use decentralised model to reduce data processed directly by HSE. - Use new Apple/Google ENS to significantly increase likelihood of product robustness. - Continued engagement with scientific and other groups to carry out research to continuously assess benefits and effectiveness. - Inclusion in TORs for App Advisory Committee to monitor effectiveness and benefits and to wind-down processing if appropriate. - Implementation of a robust testing including a large field test ahead of launch to the public - Engage intensively with other countries to align and to increase awareness and understanding of approaches used - Ensure app is entirely voluntary	2	1	2	Yes	The analysis and testing ahead of launch along with appropriate ongoing governance to measure effectiveness with appropriate sunset significantly reduces the likelihood and impact of this risk.
7	Sufficient people must use the App in order for it to make an effective contribution to contact tracing. Consideration must be given to what part of the population cannot use the App, e.g. people with no or outdated device, children etc. The risk is that data is collected about a proportion of the population but does not bring the expected benefits.	- Terms of Governance Committee to ensure Committee continuously monitor and assess for impact and effectiveness including adoption and to wind down of app if considered ineffective - Use Apple/Google Exposure Notification Services to remove technical problems that are significantly undermining bespoke Bluetooth implementations of the Contact Tracing function - The app is to be used to augment the processing of the existing manual contact tracing process to ensure that all people are included in a form of contact tracing, where app assists in this process - Ensure effective communications strategy to maximise potential for adoption - Carry out research to gauge public appetite and perception to app to confirm potential	2	1	2	Yes	Combination of measures once implemented will increase confidence and function of the product, assess appetite potential ahead of launch, and put ongoing measures to assess and review.

8	Risk that the Bluetooth proximity and power measurements record that a close contact occurred however a false positive was recorded e.g. reading was made through wall/glass and the person was not a genuine close contact	- Engage in comprehensive testing with the app and in an Irish environment - Use ENS to benefit from extensive capability of Google and Apple to do extensive testing - Create a well-designed communication plan to ensure those that may be susceptible to causing false positives understand what they can do (e.g. Luas driver to turn off Contact Tracing while working) - Introduce anonymous metrics to gauge the rate of app based close contacts numbers to app based diagnosed positives to monitor for over reporting of close contacts	2	3	6	Yes	There is still a risk that people would be designated a close contact in limited cases where they should not have been
9	Risk that the Bluetooth proximity and power measurements do not record that a close contact occurred and no contact is recorded when a positive contact actually did occur (a false negative).	- Ensure app is used to augment the existing contact tracing operation - Engage in comprehensive testing with the app and in an Irish environment - Use ENS to benefit from extensive capability of Google and Apple to do extensive testing - Create a well-designed communication plan to ensure those that may be susceptible to causing false positives understand what they can do (e.g. Luas driver to turn off Contact Tracing while working) - Introduce anonymous metrics to gauge the rate of app based close contacts numbers to app based diagnosed positives to monitor for under reporting of close contacts	2	3	6	Yes	Implementation of mitigation measures will greatly reduce the likelihood and impact, in particular ensuring that the app compliments and does not replace manual contact tracing
10	Risk that data will be transferred outside EEA and not subject to GDPR.	- Data processing agreements to be put in place with all data processors involved in the app, which restricts data transfers and storage to the EEA or other locations with which the EEA have approved mechanisms.	1	4	4	Yes	Data may still be processed outside the EEA but will be covered by the GDPR thus removing risk for the data subjects.
11	Risk of insecure methods of data transfer are used that allow access to user's symptoms, or any other data transferred to the HSE (if it could be identified as coming from their specific phone).	- Ensure data is encrypted on the mobile device, in transit over the network, and at the HSE app backend - Test to confirm that the encryption is in place and is effective	1	4	4	Yes	Virtually impossible to intercept data if these controls are implemented.

12	Effectiveness in border areas where people live and work either side of borders could undermine effectiveness and thus justification of data processing proposed	- Ensure that the app is to augment the existing contact tracing and testing operations in Ireland and that under this umbrella, of wider operational cooperation and coordination, that app interoperability is considered. - Ensure that engagement with the UK and Northern Ireland specifically in regards wider contact tracing and testing operational coordination and cooperation is pursued. - Ensure the COVID-19 Tracker app can be installed by people in Northern Ireland - Engage with the UK and Northern Ireland in relation to cross border app interoperability - Engage with Google and Apple in relation to cross border interoperability - Engage at an EU level in regards cross border interoperability	3	2	6	Yes	Through a commitment of ongoing engagement and exploration of coordination and cooperation possibilities with other countries, and the implementation of the mitigation measures, this risk is seen as significantly reduced.
13	Risk that bundling of related features in the pandemic response app infringes on the data protection principle of data minimisation	- Ensure the guidelines from the EDPB are carefully assessed - Ensure that features are clearly aligned with the purpose of the app being a COVID-19 response app - Ensure the Terms of the Governance Committee charge the committee with the above obligations - Engage the scientific community to independently assess the HCI and ethics aspect of the app to inform decisions - Ensure that the app's features can be used independent of each other and that this is clear to the users - Data geolocked to datacentres in Ireland.	2	2	4	Yes	Implementation of all mitigation measures will ensure that people can choose how their data is processed by selectively using or not the individual features within the app. There remains a small risk that users may not be aware of these options and careful and ongoing review of user experience is required.
14	The use of analytic data gathered from the device for the purposes of how the users interact with the app, daily use, app abandonment, contacts, exposure events, etc., is not anonymous and unexpected to the users. Risk to users that data is not anonymous.	- App must first get user consent before metric data is collected or shared with the HSE - All metric data must by anonymised (or anonymised at the earliest processing point - noting IP address as per DPIA) and carefully reviewed for any re-identification potential - Release source code to ensure transparency of processing - Ensure app does not use 3rd party analytics tools to gather metric data, which could unintentionally or otherwise be recombined to re-identify people - Ensure app governance appropriately reviews and protects against this as per above	1	1	1	Yes	The risk has been mitigated as far as possible by anonymising the personal data so that there is little risk to the data subjects of their data becoming identifiable or useable in profile building or similar activities.

15	Users are not given sufficient information about how the app works, what data will be collected and for what purpose in a comprehensive way	- Careful consideration of UI/UX in regards information in the app screens informing people about what the app does - Engage in behavioural research to gain direct feedback on effectiveness of in app information - Data protection information notice (DPIN) - available in the app at all appropriate screens (all consent screens) and in settings at all times, in app stores, HSE and DoH websites - Implement a communications plan to inform people about the app, what it does and what data is processed	1	1	1	Yes	Correct implementation of all mitigations leaves little risk to data subjects
16	Risk that Contact Tracing can be used to identify and track people's location and for profiling purposes, rather than tracking the virus	- Adopt a decentralised approach for the Contact Tracing function - Do not use location services for Contact Tracing - Adopt the Google and Apple API implementation, which is receiving significant worldwide analysis from privacy experts - Open source code for inspection - Do not pass IP addresses from networking layer to application layer in app backend to protect against re-identification potential - Implement security testing and assessment of app in this regard	2	3	6	Yes	After mitigation measures are implemented little likelihood remains
17	Individual perception of symptoms can be subjective or lack of understanding of symptoms could lead to misreporting. User might not record their symptoms regularly enough.	- Users centric testing to be carried out on understanding and adjust wording to ensure best method to use to increase reliability of data. - Communications plan will encourage people to self-report their symptoms each day	3	2	6	Yes	Some residual risk of low quality data remains after mitigation. To be reviewed as rolled out.
18	As the app knows when a person is uploading their diagnosis keys, risk the app can be used to display the COVID-19 status of a person and be used outside of its purpose	- The app will be designed to not show the COVID-19 status of a person - The Governance Committee will oversee the app processes data in line with its purposes and the DPIA	1	1	1	Yes	With mitigation implemented there is minimal risk

19	The use of the app may continue indefinitely or longer than justified by the defined purposes	- European Data Protection Guidelines state that contact tracing apps should remain active only for the period of the COVID-19 crisis, and as such this will be adhered to. - Terms of Governance Committee to charge Committee to implement an orderly wind down of processing of personal data within 90 days of the COVID-19 crisis ending (declared by Government) - Introduce measures through the app and communications to prompt user action as appropriate as part of any wind-down - Continual review by Committee as previously stated for effectiveness	1	1	1	Yes	Little risk remaining to data subjects if all measures are implemented
20	IP address is present in all data transfers from the app to the app backend	- The app backend will not processing IP addresses at the application layer. This means no IP address leaves the network layer on the backend. - All app backend logging does not log user IP address	1	1	1	Yes	IP address does not leave app backend network layer and as such HSE cannot recombine with payloads to identify data subjects
21	The risk that SMS code provider can identify that particular person with particular notifications and then infer the COVID-19 positive status of the device owner	- Ensure appropriate data processor agreement is entered into for SMS delivery service to protect confidentiality and thus protect data subjects - use known and trusted SMS provider for this service	1	3	3	Yes	After mitigation it is unlikely to occur
22	There is a risk of pollution of symptom statistics data and metric data by bad actors	- Ensure network and WAF security measures are put in place to block attacks of scale - Ensure device integrity checks are first performed by the app during the on boarding, and to ensure for all traffic to the app backend is protected via this means	2	2	4	Yes	After mitigation it may still occur, but at a small scale and likely to be statistically insignificant

23	Technical issues with the app that would reduce function or interfere in a negative way in the working of the other phone's function, thus reducing user engagement, lessening the app's effectiveness, and weakening the case for data being processed.	- App to be tested for impacts on other phone functions such as battery life, interference with Bluetooth peripherals, etc. - Use Apple and Google ENS to benefit from their ability to optimise functioning of the exposure notification service beyond what any app developer can	2	2	4	Yes	The mitigations will go some way to reducing the risk however the residual risks will not be known until app is fully tested
24	Role of Apple and Google may process data in a non-privacy enhancing way in the future, or in a way that is not desirable in respect of the rights of data subjects, that is unexpected	- Continually monitor and engage with Apple and Google to understand their plans and feedback regarding Ireland's requirements - Continually review plans and how data is processed and implement an exit from reliance on Exposure Notification Services if it falls out of line with GDPR - Work with other countries to engage with Google and Apple, and to collectively monitor the performance and behaviour of ENS	1	2	2	Yes	With mitigations implemented it leaves little net risk.
25	Integrity of data is compromised. The diagnosis keys, or mobile number uploaded to HSE servers is erroneous or corrupted, meaning it is unusable or unreliable.	- App and related technology infrastructure to undergone extensive information security testing to identify and rectify any issues. - All traffic in transit is encrypted - Certificate pinning and other security mechanisms are implemented to protect against 'man in the middle' attacks	1	4	4	Yes	The proposed risk treatments should largely remove risks to data integrity.
26	Users may decide to turn off the Bluetooth service on their phones for battery life or other reasons.	- Integrate into communications and within the app a clear message so people understand the impact of turning off Bluetooth on their phone - Clearly show, if people go into the app, that the Contact Tracing function is turned off (must respect consent)	2	3	6	Yes	It is difficult to ensure that users never turn off Bluetooth.
27	Continually downloading Diagnosis Keys may consume a user's network data allowance.	- Use a design that minimises the size of data downloads required - current estimates for Ireland and ENS is ~1MB per week downloaded. The amount of traffic sent to and from the device should not use up any significant portion of the user's monthly allowance or credit.	1	2	2	Yes	The residual risk would be one relating to the number of infections that would cause a jump in traffic

#	Risk	Mitigation					
28	Users can't exercise their data protection rights or don't know where to go to exercise them.	- Provision of a DPIN to ensure it is clear to data subjects what rights they have, how to exercise them and with whom. - Ensure access to DPIN at all times via the app, and app related website - Implement a decentralised model for exposure notification to ensure limited personal data processed on app backend - Symptom data collected to be anonymous	1	1	1	Yes	There is only a small risk of this occurring based implementation of mitigation measures
29	Where the data is stored on servers of US companies, US Government could use the Cloud Act to attempt to access the data	- Data at rest in AWS is to be encrypted. - Data geolocked to datacentres in Ireland.	1	2	2	Yes	There is little residual risk due to the small amount of data held on AWS servers by the HSE relating to the app that can be utilised, and it will be encrypted via mitigants.
30	Patients may be less likely to upload their diagnosis keys when advised they will be shared with other countries as a result on interop capabilities going live	The script (and backup information) used by clinicians when they advise patients they are covid positive and invite patients to upload their keys will be updated to provide reassurance to patients that uploading the keys will not be used to identify them as an individual and adds value even if they are not travelling overseas themselves.	2	1	2	Yes	There is little residual risk with this mitigating action in place
31	As interop goes live, users will be downloading diagnosis keys derived from Irish app users plus keys derived from compatible apps in other countries, which will consume more of the users network data allowance.	We will engage with the major mobile network providers in Ireland to see if this data can be zero rated	3	1	3	Yes	Users using some of the smaller networks may still be affected if they refuse to zero rate this data

Appendix G – Data Minimisation

The COVID Tracker App has been designed in a manner to minimise the amount of personal data processed in order to fulfil its defined purposes. The following are design approaches that highlight putting the principle of data minimisation into effect.

- Close contact warnings are designed so that they can be generated without the collection of a person's phone number for call back. The collection of the phone number is optional.
- Phone numbers if collected for call back purposes on generation of a close contact warning is only transferred to the HSE at the point of generation of the warning. If a close contact warning is not triggered by the app, then the phone number never leaves the app.
- Demographic data that is submitted at time of symptom check-in is optional and the app can function without this data.
- The use of a "decentralised" model for the contact tracing function allows phones to process data on a phone to generate close contact warnings locally without having to upload contact traces to a centralised server.
- On sending an upload code to a phone to authorise the upload of diagnosis keys, the mobile number that is used to send an SMS to is deleted immediately from the app backend before the diagnosis keys are uploaded to the app backend. This avoids the inadvertent or otherwise recombination of diagnosis keys with mobile phone number.
- IP address data that is included in all internet traffic between the app and app backend is not logged and terminates at the API Gateway stage (network load balancer) and is never sent onwards to the application layer. This prevents inadvertent or otherwise recombination of IP address data with any payload data sent by the app to the app backend.
- The retention period for all personal data is set out in Section 4 of this document and has been carefully examined to be only as long as is necessary for the fulfilling of its purpose.
- Cross pollination of personal data between the primary functions of the app is not performed, and each of the functions can be used without the use of the others.
- Where the identification of personal data has been collected is not necessary anonymisation of such data has been employed. Details of said anonymisation follows.

Anonymisation

Diagnosis Keys - no personal data is used in the derivation of the diagnosis keys. The keys are created on the phone via pseudorandom cryptographic means using no personal data as input. These 'random IDs' are stored on the phone, until such a point that a person is diagnosed positive. The keys can be uploaded to the app backend once a person has access to an upload authorisation code. This code is delivered by SMS on foot of a call from the HSE to the diagnosed person.

The keys alone are not capable of identifying a person, however care is needed to ensure that no personal data is associated with the keys on the diagnosis key registry. This care has been taken as follows. 1) The IP address that accompanies the keys to the HSE app backend servers during upload does not progress past the API Gateway, and thus is not available for recombining with the keys at a later stage. 2) The phone number that is used to send the upload authorisation code via SMS is removed as soon as the SMS is sent, thus preventing recombination of the phone number with the diagnosis keys at a later stage. 3) The only data that is published to the registry is the diagnosis key data without any personal data present, be it IP addresses/phone number or any other personal data. The keys are downloaded by all apps periodically where the Google and Apple ENS API restricts how the

keys can be used to check for a match for exposure so as to restrict public health authorities from misusing the API to potentially reveal the identity of the diagnosed person. In light of the preceding, it is considered there is no reasonable likelihood that a person can be identified using diagnosis keys.

Symptom Data – the purpose of the COVID Check-In function does not necessarily warrant the collection and ongoing processing of personal data. The presence of IP address with the symptom data upload from the app to the app backend could be argued to make symptom data uploads personal data. As has been previously articulated IP address data is stripped at the networking layer of the app backend, and no means are available to recombine the IP address with symptom upload at a later stage exists.

IP address data aside, the approach to the protection of anonymity of the COVID Check-In submitted data by data subjects is to ensure that the data, without modification, can be considered anonymous. In other words, while anonymity can be achieved in the general sense by collecting data that might be considered personal data, and subsequently performing anonymization techniques such as randomisation or permutation, in regards the COVID Check-In function, the goal is that the data itself, at point of collection, without post processing cannot be used to identify a person.

Care has been taken in regard the use of the demographic information that is optionally provided along with the symptom data. This demographic data includes the following:

- Sex: Male / Female / Prefer Not to Say
- Age Range: 16-39 / 40-59 / 60+ / Prefer Not to Say
- County / Prefer Not to Say
- Town / Prefer Not to Say

Also, the symptom data itself includes the setting of "Yes" or "No" for the primary four COVID-19 symptoms. Note town above is a "Settlement", which is a geographical boundary that formed part of the Small Area Population Statistics in Census 2016.

The controllers in consultation with the CSO, made an assessment of the population levels of each settlement when divided by the specified Age Ranges and Sex. The minimum population for any cohort across all settlements is 4. It should be noted that knowledge of participation in the use of the COVID Check-In function is not available, and this adds protection to the anonymity of the data. Also, in regards the lowest cohort population (4 in this case for one settlement) – is at the higher age range. The expectation is that less individuals of the high age range will be users of the app due to less of that age range are owners of smartphones and thus makes it less likely for singling out, and for inference attacks to bear any fruit.

Lastly, in light of the above, the controllers are of the view that the COVID Check-In data cannot be used to identify a person by using all the means reasonably likely to be used by the controllers themselves. Furthermore, in light of the above, and given the added assurance that the CSO will further inspect data as it is received and before publication with a view to ensuring anonymity is protected, that the data cannot be used to identify a person by using all the means reasonably likely to be used by 3rd parties. Ongoing review of the symptom data sent by the HSE to the CSO to identify and remove risks of re-identification attacks will be performed.

Appendix H – Data Retention

The following table sets out further details in relation to the justification for the retention of each of the personal data fields and also the measures to ensure that the retention policies are adhered to.

Data	Retention	Retention Justification	Retention Measure
Phone number Date of last exposure	This phone number is securely held on the app until the user removes it via settings; selecting the Leave function; or uninstalling the app. The phone number, if sent from the app to the HSE contact tracing operations (CTC) for call back, will be processed as per the procedures for all identified close contacts via CTC.	The justification to store the phone number on the app until a person removes it via settings/Leave/uninstalling is to carry out the wishes of the person to receive a call back if they get a close contact warning, which could happen at any stage.	The removal of the phone number from the app is self-managed by app users. If the phone number and date of last exposure has been sent to the HSE to perform a call back due to an exposure notification alert, the app backend will immediately delete your number once it is transferred to the HSE CTC. The HSE CTC will then process your number in line with the current contact tracing operations for contact tracing purposes.
Sex Age Range County Town (>90 population)	This data is securely held on the app until the user removes it via settings; selecting the Leave function; or uninstalling the app. This data is held by the HSE for 1 day after receipt to facilitate its transfer to the CSO. This data is retained by the CSO as anonymous data for statistical and research purposes in line with the CSO's data management policy.	The justification to store the demographic data on the app until a person removes it via settings/Leave/uninstalling is to facilitate its sharing with the daily check-in data in line with the user's choice to do so. This is a convenience so that users are not asked if they would like to enter this demographic data each time. The uploaded data is held for 1 day after receipt to give sufficient time to ensure it is securely transferred to the CSO, as data is transferred daily in batch.	The removal of demographic data from the app is self-managed by app users. The removal of uploaded data to the HSE is automatically removed 1 day after receipt.
COVID-19 Symptoms	This data is securely held on the app for a maximum of 28 days, or until the user removes it by selecting the Leave function; or uninstalling the app.	The justification to store the symptom data on the app until a person removes it via settings/Leave/uninstalling is to support the person reviewing their symptoms as an aide-memoire, and to facilitate the sharing of the 28 days' worth of symptoms at each daily check	The removal of symptom data from the app is automatic after 28 days or self-managed by app users on Leave/uninstall.

	This data is held by the HSE for 1 day after receipt to facilitate its transfer to the CSO. This data is retained by the CSO as anonymous data for statistical and research purposes in line with the CSO's data management policy.	in. 28 days is considered a window of epidemiological significance that generally covers the period of symptom onset through to recovery. The uploaded data is held for 1 day after receipt to give sufficient time to ensure it is securely transferred to the CSO, as data is transferred daily in batch.	The removal of uploaded data to the HSE is automatically removed 1 day after receipt.
Diagnosis Keys	Phones generating random IDs retain the data for 14 days unless the user deletes ENS data via phone settings. The registry stores IDs for 14 days. Apps download and process IDs to check for exposure events only for as long as is required to determine if there is a match or not.	Each phone holds up to 14 of daily random IDs to potentially upload and publish on the registry to allow other app users to check if they were in close contact in the last 14 days. 14 days is considered a window of epidemiological significance that generally covers the potential for viral transmission. The registry stores up to 14 days' worth of IDs for the above reason. IDs are downloaded for the purpose of checking for a close contact.	Phones automatically delete generated daily random IDs after 14 days. The registry automatically deletes random IDs after 14 days. Downloaded IDs to phones are deleted after checking for a match is performed.
Mobile number Date (symptom onset minus 48 hours)	As soon as the SMS is sent, the phone number is deleted, and only the code is preserved with the symptom date. The app backend has no way of knowing the phone number of a person that either uploads their keys, or chooses not to upload their keys. The code is processed long enough to authorise diagnosis keys upload, and also to retrieve the symptom date to determine the appropriate window of diagnosis keys to upload to the registry. It is deleted once this purposes is fulfilled or within 10 minutes, whichever occurs first.	The justification for retaining the mobile number for the period set out, is to send the SMS to enabler a user to upload their diagnosis keys. The date is retained for the purpose of stripping out diagnosis keys prior to this date when they are uploaded. The epidemiological window of significance (viral shedding) is from this date onwards. The code is retained for the purpose of authorising the upload to ensure the diagnosis key registry does not get polluted with fake submissions.	The mobile phone number is automatically removed as soon as the SMS is sent. The date and code are removed automatically once they are used, or after 10 minutes – whichever comes first.

Metrics See Appendix D for full breakdown.	This data is retained by the HSE as anonymous data for statistical and research purposes for a minimum of 7 years and reviewed for further retention at that stage. This data is retained by the CSO as anonymous data for statistical and research purposes in line with the CSO's data management policy.	This data is retained for the purposes of monitoring the efficacy of the app and improving it.	This data is manually reviewed by the HSE and the CSO in line with their policies for the retention of statistical and research data.
IP address and app security tokens	IP address is held in a transient manner on the networking layer for networking and security reasons. It is not persisted, nor logged on the app backend in any other way. The app security tokens are deleted on selection of the Leave function, or the deletion of the app (immediately on the phone, and after 60 days of not being used by the app backend as the backend is not aware of an app being deleted.	This data is retained for as long as it is needed for the purposes of network communication. Security tokens are retained on the app and the app backend to protect the API layer of the app backend from being subjected to attacks and pollution of fake data.	The IP address is automatically removed after it has served its primary networking purpose. Security tokens are deleted when a user selects Leave or automatically after 60 days of lack of use.

Appendix I – Conditions of Consent

As set out in the document, the use of the app is entirely voluntary in nature and will continue to be so. The controllers have no means to detect use or lack of use of the app by any identifiable individual's phone. A supporting governance mechanism is provided to oversee the fulfilling of this principle in practice, ensuring that the voluntary nature is protected, and that consent is freely given. Article 7 of GDPR set out a series of conditions when the processing of personal data is based on consent. An assessment of these conditions are set out as follows.

Data	Demonstration of Consent	Clearly Distinguishable	Right to Withdraw	Conditionality / Freely Given
Phone number Date of last exposure	The phone number is shown in settings, which can be accessed at any stage, and demonstrates that the number has been recorded under users' own volition and a call back will be triggered if the data is present.	The phone number is collected on a screen of its own, setting out the reason for its collection, its optional nature, and for consent to the specific purpose for its processing – the option of a call back from the HSE.	Users can change their mind regarding consent at any stage via the app settings. Deleting the phone number via app settings, clicking Leave or uninstalling the app are the means to withdraw consent at any stage. If the phone number and date has been shared with the HSE for call back as part of CTC, the app backend automatically and immediately deletes the phone number and date once it has transferred to CTC. Once with CTC the data is processed in line with existing contact tracing purposes.[13]	Phone number entry is optional and is not conditional on the functioning of Contact Tracing function within the app. Furthermore, there is no dependency on, or conditionality relating to, the processing of this data beyond the specific purpose for its processing – the option of a call back from the HSE.
Sex Age Range County	The demographic data entered is shown in settings, which can be accessed at any stage, demonstrating that the	The entering of demographic data the first time requires the user to go through a screen dedicated to describing the data	Users can change their mind regarding consent at any stage via the app settings. Deleting the demographic data via settings, clicking	Demographic entry is optional and is not conditional on the functioning of the COVID Check-In function within the app.

---

[13] HSE CTC data processing, and data subject rights and their exercising, can be found at - https://www.hse.ie/eng/gdpr/data-protection-covid-19/

Town (>90 population)	data has been recorded under users' own volition.	processing involved and asks for consent. The demographic data is collected on a screen of its own, where each field is optional, allowing users to skip the provision of this data.	Leave or uninstalling the app are the means to withdraw consent at any stage. Demographic data held by the HSE and the CSO is not relatable to any specific individual, and as such removal is not possible.	Furthermore, there is no dependency on or conditionality relating to the processing of this data beyond the specific purpose for its processing – the sharing of demographic data as part of the optional COVID Check-In function. Demographic data cannot be reasonably used to identify a person and as such the controllers have no means, nor does it seek them, to identify whether a specific person has or has not shared demographic data.
COVID-19 Symptoms	The act of entering and sharing symptom data with the HSE is timestamped and recorded on the phone each day, which can be viewed at any time by the user via the COVID Check-In function. This historical record is retained on the phone for 28 days. The only means of sharing symptom data is to first give consent to the sharing of said data.	The entering of symptom data the first time requires the user to go through a screen dedicated to describing the data processing involved in the function and asks for consent.	Users can change their mind regarding consent at any stage and remove any symptom data held on the phone by clicking Leave or uninstalling the app. Symptom data held by the HSE and the CSO is not relatable to any specific individual, and as such removal is not possible.	Symptom entry is optional and is not conditional on the functioning of the Contact Tracing function within the app. Furthermore, there is no dependency on or conditionality relating to the processing of this data beyond the specific purpose for its processing – the sharing of symptom data as part of the optional COVID Check-In function. Symptom data cannot be reasonably used to identify a person and as such the controllers have no means, nor does it seek them, to identify whether a specific person has or has not shared symptom data.
Diagnosis Keys	The phone settings keeps a record that a person has consented to turning on or off Exposure Notification Services on the phone. Turning on this service means that diagnosis keys will be stored on the phone.	The phone settings screens in relation to the diagnosis keys are provided by Apple and Google and are separate to the app screens. The settings screens are related only to the specific purpose of exposure notification.	The user can turn on and off the Exposure Notification Services at any time in the phone settings, and can also delete any ENS data at any time in the same place. Diagnosis keys held by the HSE is not relatable to any	The processing of diagnosis keys is optional and is not conditional on the functioning of the COVID-19 Check-In function. Furthermore, there is no dependency on or conditionality relating to the processing of this data beyond the specific purpose for its processing – exposure notification.

		Before uploading of diagnosis keys the app asks on a dedicated screen, which describes the data processing involved, for consent. This is complemented by the phone also prompting the user for consent to allow the app to access the diagnosis keys.	specific individual, and as such removal is not possible.	Diagnosis keys cannot be reasonably used to identify a person and as such the controllers have no means, nor does it seek them, to identify whether a specific person has or has not uploaded diagnosis keys.
	Also, before uploading diagnosis keys the user is asked for their consent, and after the upload of the keys, the app presents a confirmation of upload message to the user.			
Mobile number

Date (symptom onset minus 48 hours) | When a mobile number that has been collected by CTC is processed for the purposes of sending an authorisation code for upload of diagnosis keys, a record that a person has consented to this act is maintained by CTC. | A person is phoned by the HSE on a positive diagnosis and is asked separately and clearly on the phone if they are an app user and if they consent to sharing their diagnosis keys. | The processing of the mobile phone and date of symptom onset is transient. Once the mobile number has been used to send an SMS it is immediately deleted. Also, the date of symptom onset is deleted once upload of keys has occurred or 10 minutes have passed, whichever occurs first. | CTC ensures that when a person is called to inform them they are positive for the virus, they will be asked if they are a COVID Tracker App user and if they are happy to share their diagnosis keys. This is an optional step and manual contact tracing interview continues as per normal.

Furthermore, there is no dependency on or conditionality relating to the processing of this data beyond the specific purpose for its processing – publication of the diagnosis keys on the public registry to support exposure notification. |
| Metrics

See Appendix D for full breakdown. | The record of consenting or otherwise to the sharing of metric data with the HSE can be accessed at any time via app settings. | During the initial screens of the app after app installation, a user is presented with a screen that is dedicated to asking consent for the recording and sharing of metric data. | The app settings metrics screen supports the turning on and off of the metric recording and sharing at any time. | The processing of metrics is optional and is not conditional on the functioning of the COVID Tracker App.

Furthermore, there is no dependency on or conditionality relating to the processing of this data beyond the specific purpose for its processing – support the understanding of the use and efficacy of the app for the purpose of improving it.

Metrics cannot be reasonably used to identify a person and as such the controllers have no means, nor does it seek them, to identify whether a specific |

				person has or has not recorded and shared metric data.
IP address and app security tokens	The app is an internet connected one, and as such network routing and security tokens are processed as normal. The existence of the app on a user's device is considered demonstration that consent was received.	The act of downloading and installing is considered clearly distinguishable as per the norm with internet connected apps. Consideration was given to including explicit text immediately in the app initialisation screens about IP address and security tokens, though this caused more confusion as to what was being consented to leading to queries as to why the app was doing something regarding networking that other apps weren't, even though internet connect apps process the same type of network related data. The approach adopted was to include technical detail of IP address and security tokens in the Data Protection Information Notice in more detail and link to this in the "Your Data" screen, and also make the DPIN available via the app store so it can be accessed ahead of download and install, and on the app website.	Selecting the Leave function removes the security tokens from the app backend and the app. Deleting the app will leave security tokens on the app backend for a maximum of 60 days after which they will be automatically deleted. IP addresses are not stored on the app backend and thus cannot be removed.	The COVID Tracker App is entirely voluntary and participation in the wider contact tracing efforts is not conditional on the use of the app.

Furthermore, there is no dependency on or conditionality relating to the processing of this data beyond the specific purpose of the app itself. |