Data Privacy Impact Assessment (DPIA)
Part 3: Full Data Protection Impact Assessment (DPIA)

DPIA Ref (for CDPU use only)	
Process/Project Name:	Jersey COVID Alert App
Project Lead:	Digital Jersey, Digital Health
Project Manager (where applicable):	Rachel Wijsmuller (Digital Jersey)
Person completing form (If different to above)	
Date on which processing will commence:	14/10/2020

In this stage of the DPIA process you must provide full details about the context, necessity, proportionality and risks associated with the process/project/proposal. The information you provide will supplement the information provided in Part 2: Screening. It is vital that you fully complete every section.

The aim of this process is to identify and mitigate risks. Once you have completed your DPIA, you must refer this to your Data Champion for review and sign off.

Part 3: Full Data Protection Impact Assessment (DPIA)
Please provide as much detail as possible, avoiding technical language and acronyms, explaining the proposal in a way that someone with no prior knowledge could easily understand.
Section 1 – Necessity and Proportionality
In this section you must demonstrate why the processing is necessary and proportionate, providing evidence to support your assessment. • The processing must be **necessary** for the specific objective of the process/project/proposal. • It must also be **proportionate**, meaning that the advantages resulting from the processing should not be outweighed by the disadvantages to individuals.
1.1 What do you want to achieve from the process/project and how will your plans for processing personal data help to achieve your purpose? • Clearly state your objective • Provide evidence for why the proposal is necessary. The evidence can consist of facts, statistics, reports etc.
Contact tracing and testing is a strategy employed by Jersey and many other Public Health bodies to contain the spread of a pandemic disease. Contact tracing is a process where a person who has been infected with the disease is interviewed

over the phone to identify other individuals they may have exposed to the disease during their Infectious Period. A close contact event is defined by the Chief Medical Officer according to the disease transmission principles as understood at the time, typically consisting of a duration and distance threshold (e.g. 2 metres for 15 minutes). The identified close contact individuals are then contacted by the Contact Tracing team and given advice to restrict their movements in line with Public Health policy, and potentially directed to testing.

The exposure alert function within the Jersey App is designed to augment the manual contact tracing as described above, by delivering fast notifications to potentially infected individuals to break the chain of transmission sooner than the regular process would allow. Manual contact tracing, based on established medical practice and executed by Authorised Officers, will remain in place as the core process, serving non-app users and providing a vital point of human support and authority.

For healthy users, the app will anonymously warn the user if they have been near someone who has COVID-19 but was not aware of it at the time. The warning is called an Exposure Alert and will be presented as a notification in the app. If the user chooses, they can ask the Contact Tracing Team to call them for specific advice and support if/when they get an Exposure Alert.

For users who are diagnosed with COVID-19, the app lets them anonymously warn people they have recently been near to before the user became aware that they were infectious. Only people with a confirmed case of COVID-19 can do this with the support of the Contact Tracing Team.

While Jersey may contain the spread of the disease locally, the island is also subject to risk presented by inbound travellers. Travellers, particularly temporary visitors, can be difficult to trace, and may not be reachable at all within a reasonable time. The interoperability of the Jersey App with other Apps implemented elsewhere is very important to address the risk presented by imported cases, and to provide Jersey people the same protection when they travel abroad. While no exposure notification apps are currently interoperable, there are programmes at UK and EU level which Jersey is contributing to and expects to be part of at the time the interoperability service is launched. While interoperability is not in place, visitors to Jersey will be advised to use the Jersey App if they wish. With interoperability visitors to Jersey without a compatible national app shall still be advised to voluntarily use the Jersey App while on island, while visitors with a compatible national app will be advised to continue using their own app unless their stay is for three weeks or more.

The Jersey App will have two purposes:

a) To enhance the existing manual contact tracing programme
b) Provide additional protection for our community.

The Council of Ministers has approved the introduction of a Jersey exposure notification app (the "Jersey App") a mobile application to respond the current pandemic. A Code of Practice (the "Code") has been developed to support and guide members of the Advisory Committee (as defined in the Terms of Reference at Appendix A) when making decisions surrounding the Jersey App. It provides a set of principles which should underpin any decisions and offers an understanding of the framework whilst also being transparent as to how users data will be used.

1.2 Describe why existing and/or less intrusive measures would be inadequate

- Describe whether any less intrusive options would achieve the same goal.
- Consider whether existing processes or techniques could be used instead of new intrusive measures
- Clearly outline why the processing is proportionate

The app selected is the least intrusive option available. Personal data required for the service to function is limited to IP addresses.

Optional functionality includes the submission of a mobile telephone number to the App to allow the Contact Tracing Team to contact the App user in the event that they receive an Exposure Alert and have requested a Call-Back.

The app is designed to supplement the existing contact tracing process, not replace it, and will always be voluntary. The exposure alerts generated by the app allow notified individuals to act faster to break the chain of infection, thereby controlling outbreaks.

1.3 What is your intended effect of the processing to the SoJ, the Data Subjects and/or Society and the general public

- Describe benefits or disadvantages to the above

The Jersey COVID Alert is a free app for a user's mobile phone. The app uses Bluetooth to alert the user if they have recently been within 2 metres of someone with COVID-19, for longer than 15 minutes (Close Physical Contact).

Using the Jersey COVID Alert app will help to contain coronavirus outbreaks by interrupting the chain of transmission. The app is designed to support existing Jersey public health measures by allowing you to assess your personal risk of infection.

The app will alert the user if it detects close contact with another app user who has COVID-19 so the user can avoid infecting other people. The user can also get help sooner, reducing the chance of serious complications.

If a user gets COVID-19, they can anonymously warn people they have recently been in close physical contact with that they may be at risk, so they can take action to protect their families and friends.

App Functionality

When a person downloads the Jersey App, they have the option of enabling the Exposure Alert function during set-up, or at any later time in Settings. Users are advised that the App will not function correctly if the Exposure Alert function is not turned on. If enabled, the Exposure Alert function will use the Exposure Notification Services (ENS) within the smartphone operating system to continuously scan for other devices nearby that also have ENS activated.

The ENS allows phones to share anonymous, Random IDs using Bluetooth. The anonymous codes are made up of letters and numbers, and are continuously changed automatically every 5 minutes. Users never see the codes, and the codes cannot be used to identify users or their devices. Using a Random ID means any information about close contact events is collected anonymously without the need to exchange personal data.

When proximity is detected, the phones record this by exchanging random IDs without the need for any user action. In the exchange of Random IDs the devices will include information on Bluetooth signal strengths which is used later to estimate the distance between devices. The device records all the Random IDs that it sees in a rolling 14-day period, older Random IDs are automatically deleted after 14 days.

The Jersey App downloads new IDs every 2 hours from the secure registry of IDs stored on the app servers, which is only accessible by other apps, uploaded by people with COVID-19 (explained below) and compares them against the recorded IDs on the users phone. If there is a contact event matching the Contract Tracing Team case definition, which is based on the 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 COVID-19. The phone displays the exposure alert and presents advice in accordance with public health guidance for close contacts, including restriction of movements. Exposure notifications (called "Exposure Alert" in the app) remain visible on the app for 14 days from the date of last exposure. The date of the exposure is not shown to the user by the app, although technically competent users can search for this in the ENS settings on their smartphone. Users can clear exposure notifications from their Jersey 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.

A user can volunteer to record their phone number on the app asking for a follow-up call from the Contract Tracing Team 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 Contract Tracing Team. The Contract Tracing Team 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 Contact Tracing Team are not aware of an exposure notification having been delivered to any particular user unless the user chooses 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.

COVID-19 Diagnosis
If an individual tests positive for the virus the Contract Tracing Team 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 Contract Tracing Team via the app upload process. If they are happy to volunteer their random IDs, the Contact Tracing Team use the mobile phone number provided by the data subject at the time they undertook their test to send an authorisation code via SMS. The SMS text and authorisation code are also displayed and temporarily stored in the IPHR. A script has been developed to make it clear that the caller does not have to use the app to warn others they may have been in contact with, but they can do, if they wish. When the code is entered into the app, this authorises an upload of the past 14 days' worth of random IDs to the secure publicly available app registry, noting importantly that neither the Contract Tracing Team nor the public can identify anyone from the IDs at any point of the process.

Privacy
A rolling 14 days' worth of random IDs and Bluetooth signal information recording a person's recent encounters, are securely stored on the user's phone but not accessible to the user. The random IDs cannot be used to identify users. If a user wishes they can turn off the ENS therefore disabling contact tracing independent of the other Jersey App functions, namely sharing the App, reviewing the Updates page, or leaving the App.

Users can choose to record their phone number on the Jersey App and ask for a follow up call from the Contact Tracing Team should they receive an Exposure Alert. The user's number will only leave their phone if an Exposure Alert is received and the user has requested a follow up call. No other user personal information is collected or shared by the app.
If the user chooses to request a follow up call, the Contact Tracing Team will retain the phone number for 14 days for the purposes of contacting the user. On the follow up call, the operative will make it clear to the user that any information shared on the call will fall under the Data Protection policies of the Integrated Public Health Record (the IPHR) – a central case management system created for the purpose of managing the pandemic in Jersey. The IPHR is governed separately to the App and has a different set of Governance Documents which may be reviewed online1.

Use of the App
Use of the Jersey App will be entirely voluntary and will be available to download for free from the Apple App store and the Google Play Store. Public Health will publish guidance for different groups who may wish to enforce the app, explaining that the technical basis for the exposure alerts is not strong enough to justify enforcement or compulsion. There is also a feature in the Jersey app to allow users to control the display of Exposure Alerts, preventing use of the app as an entry check or denial of service to users who have been exposed. Users may also leave the app at any time should they no longer wish to use it.
The Jersey App works on Android and iOS devices which support modern operating systems (Android 6.0 and later or iOS 13.5 and later).

Interoperability with other contact tracing applications

The Jersey App has been designed to allow it to operate with other contact tracing applications that also use the Google Apple Exposure Notification system. This provides the Jersey App with the ability to seamlessly deliver Exposure Notifications to a user of another jurisdiction's contact tracing application in circumstances where that user has been in close proximity with an App user and the App user has received a positive COVID-19 test result, or vice versa. The interoperability system operates by the secure exchange of [temporary exposure keys (TEKs)] through a network gateway. The TEKS cannot be used to identify app users and are not considered Personal Data for the purposes of the Data Protection (Jersey) Law 2018. No personal data will therefore be exchanged with any Governments or application users in other jurisdictions as a result of the interoperability of the App with other contact tracing applications.

Section 2 – Scope

[1] https://www.gov.je/government/departments/privacypoliciesretentionschedules/pages/governmentofjerseycoronavirusprivacypolicy.aspx

2.1 Provide full details of the specific personal data that you intend to process

The App uses personal data in the following ways:

1. Contact from Contact Tracing Team – if a user chooses to include their mobile phone number in the App, this will be used by the Contact Tracing Team to contact the user in the event that they receive an Exposure Alert. The App will also automatically send the date of the user's last exposure to another user who has tested positive to the Contact Tracing Team (see App Functionality in section 1.3 for further details).
2. Upload Random IDs – if a user receives a positive Covid-19 diagnosis and agrees to use the App to notify others, the Contact Tracing Team will use the user's mobile phone number to send them a code. The code can be uploaded to the App by the User in order to authorise the upload of Random IDs to notify others who the user may have been in Close Physical Contact with (see Positive diagnosis in section 1.3 for further details). By virtue of the fact that this only happens when a user has a confirmed diagnosis of COVID-19, the Authorisation Code is Special Category Data.
3. Network traffic – All API calls to the app servers will unavoidably result in app users' IP addresses being present in data communicated between the app and the app servers due to the nature of networking. The app firewall does not transmit the IP addresses to the app system and the Contract Tracing Team will never have access to that data. As a precaution, IP addresses are retained for 14 days so that any suspicious activity may be identified by the automatic firewall rules. 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.

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) locked to the EU West Region. Internet traffic between the app and the servers uses IP addresses at the networking layer.
3. The Jersey App may send the Contract Tracing Team the user's phone number (this is at the user's request) for a follow-up call in the event of the user receiving an Exposure Alert. When this occurs the user's phone number and date of exposure is logged in a call queue in the IPHR. If the CTT handler determines that the user is a genuine Direct Contact, they will create a case and the user's data will be processed in line with existing IPHR policies. If the CTT hander does not determine that the user is a genuine Direct Contact the call-back listing is deleted and no data is retained in the IPHR.
4. The IPHR uses the SMS facilitator Twilio to generate an SMS to the user containing the Random ID upload authorisation code. The user's phone number and a random code is sent from the IPHR to Twilio to generate the SMS. The App does not share this personal data however and the phone number sent to Twilio will be the number collected through the testing process and not that stored in the App.

2.2 Describe the volume and variety of personal data you intend to process

Scope of Processing

Only individuals who volunteer to download, install and use the Jersey App will be within the scope of processing. The Jersey App will be published in the UK and Rest of World App Stores thereby allowing both local users and visitors from jurisdictions without an Exposure Alert app to download (depending on departure country) the app either prior to departure or upon arrivals. Cross-border interoperability will be implemented as far as is possible pending the actions of other nations and UK/EU/global interoperability agreements. Other global users may also download the App for academic purposes, although only one app at any time can use the operating system tools on the device and those users will not be able to access the Jersey Contact Tracing Team to authorise their infectious status if they get COVID-19. For this reason users with a home nation app are deemed unlikely to continue using the Jersey App.

Data Subjects

The proposed data processing relates to all individuals in Jersey that choose to download and install the Jersey App from the App Stores.

Children

The age of consent for Contact Tracing is 16. Because using the app may involve interactions with the Contact Tracing Team (e.g. as part of a call back or on diagnosis) it has been agreed that app users must be a minimum of 16 years of age.

Prospective app users will be required to confirm 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 those aged 16 and under where possible, although we note that there are many ways to circumvent app store restrictions and in reality we have little ability to prevent under 16s from downloading and using the app. The Contact Tracing Team have been advised to ask the user to verify their age as part of the call-back script, so that should an underage user have received an exposure alert and have requested a call-back, the involvement of the legal guardian can be sought at the point of interaction with Contact Tracing.

Note that this is for the purposes of compliance with other obligations imposed on the Contact Tracing Team and not for compliance with the Data Protection (Jersey) Law. The App is not relying on consent as its legal basis for processing personal data and therefore consent from children is not requested in relation to using the App to process their personal data.

In summary, 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 Contact Tracing Team themselves.
2. The authorisation code sent to the user by the Contact Tracing team via SMS
3. to authorise the upload of random IDs to the registry on positive diagnosis. Users have the option not to upload these IDs.
4. IP addresses for network communication purposes.

The Contact Tracing Team also use a mobile phone number to send the SMS authorisation code but the mobile phone number used for this purpose is not the number stored in the App however and the App does not process that phone number, only the authorised code sent to the number.

2.3 How long do you expect the processing to last?

Until the pandemic is declared over by the Jersey government, or until the App Advisory Committee deems other circumstances sufficient to cause the app to be taken down before that date (e.g. insufficient take up, grave malfunction). There is no empirical evidence to show the absolute level of uptake at which the app has a positive effect, with theoretical papers citing anything from 15% of the population to 60%. Naive analysis suggests that every exposure alert served to a user who was not identified verbally by a COVID-19 case in interview but was later diagnosed with COVID-19 (within the same episode), is a positive effect as that user has taken action to prevent the spread of COVID-19 as a direct result of the Alert.

Non-identifying analytics are in place to track (1) the number of users, (2) the number of users who contact the Contact Tracing Team after receiving an alert, and (3) the number of those users who then take a test and are diagnosed with COVID-19.

Data Retention

One of the overarching principles of the Jersey App is that no personal data will be processed beyond the period of the pandemic. The Terms of Reference in Appendix A ensure that the Advisory Committee oversees the wind down of the Jersey App and the removal of all (1) uploaded random IDs and (2) security tokens from the servers, as well as removal of the app from the app Stores thereby deleting app data stored on user's phone (i.e. the user's phone number if a CTT call-back was requested and the random IDs collected from other users' apps) is implemented within 90 days of the end of the pandemic.

Users of the Jersey App have the right at any time to select the leave function within the Jersey App. This will remove the limited app data stored in the app, namely the random IDs of other users and the mobile phone number (if provided).

Users can also delete the Jersey App from their mobile which will remove all the app data stored on their device. The security token data stored on the Jersey App servers will be automatically removed 60 days after last use. The Contact Tracing Team have no way of knowing who is using the Jersey App or who has deleted it other than when the user is asked if they are an app user during the call to a newly confirmed positive case.

2.4 Have you considered any approved codes of conduct or certification schemes?
If Yes please provide details in the text box.

☒ **Yes** ☐ **No**	The app development company has completed the standard Modernisation and Digital Non-Functional Review which includes certification assessment (ISO27,001, CE+ and SOC2). The app design confirms to AA standards. The app complies with European Commission Guidelines for mobile contact tracing applications.

2.5 Special category data – Will you be processing any of the following special categories of data?

☐**Race**	☐**Genetic data**
☐ **Ethnic origin**	☐ **Biometric data**
☐ **Political opinions**	☐ **Sex life**
☐ **Religion**	☒ **Health**
☐ **Philosophical beliefs**	☐ **Criminal record**
☐ **Trade union membership**	☐ **Alleged criminal activity**

2.6 Please specify the applicable legal basis or enactment for processing this data

The Contact Tracing Team is comprised of authorised officers appointed under the Loi (1934) sur la Santé Publique, and further defined in the Covid-19 (Screening, Assessment, and Isolation) (Jersey) Regulations 2020.

This processing is deemed necessary for the achievement of Public Health goals provided for by Article 26 of the States of Jersey Law 2005 and the above mentioned Loi (1934) sur la santé publique (Law (1934) on Public Health).

2.7 Please indicate the appropriate processing condition(s) below

General data processing	**Law enforcement processing**
☒ **Consent (for the installation of the app and storing data on the app)** ☐ **Legal obligation** ☐ **Employment and social fields** ☐ **Vital interests** ☐ **Legal proceedings** ☐ **Public functions** ☐☐ **Public interest** ☐ **Medical purposes** ☒ **Public health (for the processing of the data by the contact tracing team)** ☐ **Archiving and research** ☐ **Avoidance of discrimination** ☐ **Prevention of unlawful acts** ☐ **Protection against malpractice and mismanagement** ☐ **Counselling** ☐ **Functions of a police officer** ☐ **Other (please specify below)**	☐ **Consent** ☐ **Necessary for a law enforcement purpose** ☐ **Administration of justice** ☐ **Legal authority** ☐ **Necessary for a legal claim or required by a court** ☐ **Prevent fraud** ☐ **Archiving and research**

Section 3 - Consultation

You should consider seeking the views of data subjects unless there's good reason not to. If it's not appropriate to consult then you must clearly document the reasons why. For example, if the processing is taking place without the knowledge of data subjects and consultation would prejudice a law enforcement purpose then you should make this clear. If the processing involves staff data then you consider consulting them or their representatives.

3.1 Do you intend to consult data subjects?

☒ **Yes**

If yes then outline your plan in **Section 3.2** below together with details of consultation with other stakeholders.

☐ **No** If no then outline why this is the case in the text box. Once completed, outline whether you will consult any other stakeholders in **Section 3.2** below.	

3.2 Consultation Action Log
Explain what steps you will take, or have taken, to consult stakeholders. Stakeholders may include:

- Data subjects
- Union representatives
- Information Security
- Data Champion
- Legal advisor
- Central Data Protection Unit (CDPU)
- Partner agencies
- Data processors

Who	When	How	Outcome
Data Champion -GHE	16 & 17 September 2020	Email, review of DPIA	Minor amends suggested
M&D	Throughout	Email, Teams meetings	M&D completed non-functional review and approval of supplier; M&D managing security testing and assurance; M&D review of technical architecture and integrations with IPHR.
Data subjects	Throughout	Consultation with project participants; detailed test plan pre-launch with defined feedback mechanisms; ongoing review of data subject research in other jurisdictions.	Data subjects are aware of choices and trade-offs they may make by using the app; data subjects able to access clear and complete information about how their data is managed in the app; data subjects able to access clear and complete information about their rights.
DPO	Throughout	Email consultation, document sharing, Teams meetings	DPO input received on Privacy Notice, DPIA, Terms and Conditions.
JOIC	Early overview; review of DPIA	Pre-project consultation, periodic Teams update meetings; review of DPIA	JOIC fully briefed on app.
STAC	Periodically	Attendance at selected STAC meetings to demo app, discuss scientific basis and app sensitivity settings	STAC fully apprised of automated processing for Exposure Alert generation and relevant app parameters.

COM	Project initiation; pre-launch	COM paper submitted and discussed; COM aware of app launch and key messages around privacy.	COM briefed on minimal data usage and app contribution to containing outbreaks.
Contact Tracing	Throughout	Full project engagement	Contact Tracing Team fully briefed and involved in decision-making about app functionality; involved in testing IPHR and app processes.
LOD	Project initiation; periodically thereafter	Emails, Teams meetings	LOD advice used in decision-making and policy setting.
Digital Policy Unit	Throughout	Full project engagement	DPU fully briefed and involved in decision-making.
Digital Health	Throughout	Full project engagement	DH fully briefed and involved in decision-making.
HACT Group	Project initiation; pre-launch	Teams presentation in project initiation; involved in public test plan.	HACT aware of Gov plans and feedback included in test reviews.
SPPP	Project initiation; periodically thereafter	Emails, Teams meetings	SPPP Officers briefed on app, involved in policy decision-making and implementation.
External Relations	Periodically	Email and Teams meetings to discuss interoperability and UK-related matters.	ER assistance secured for UK-related matters; ER briefed on interoperability plans.
CLS Helpline	Pre-launch	Email, Teams and in-person meetings	CLS staff fully briefed and able to provide first line support to the public.
Commercial Services	Pre-launch	Email, Teams meetings	Project has commercial approval.

Section 4 – Information Lifecycle

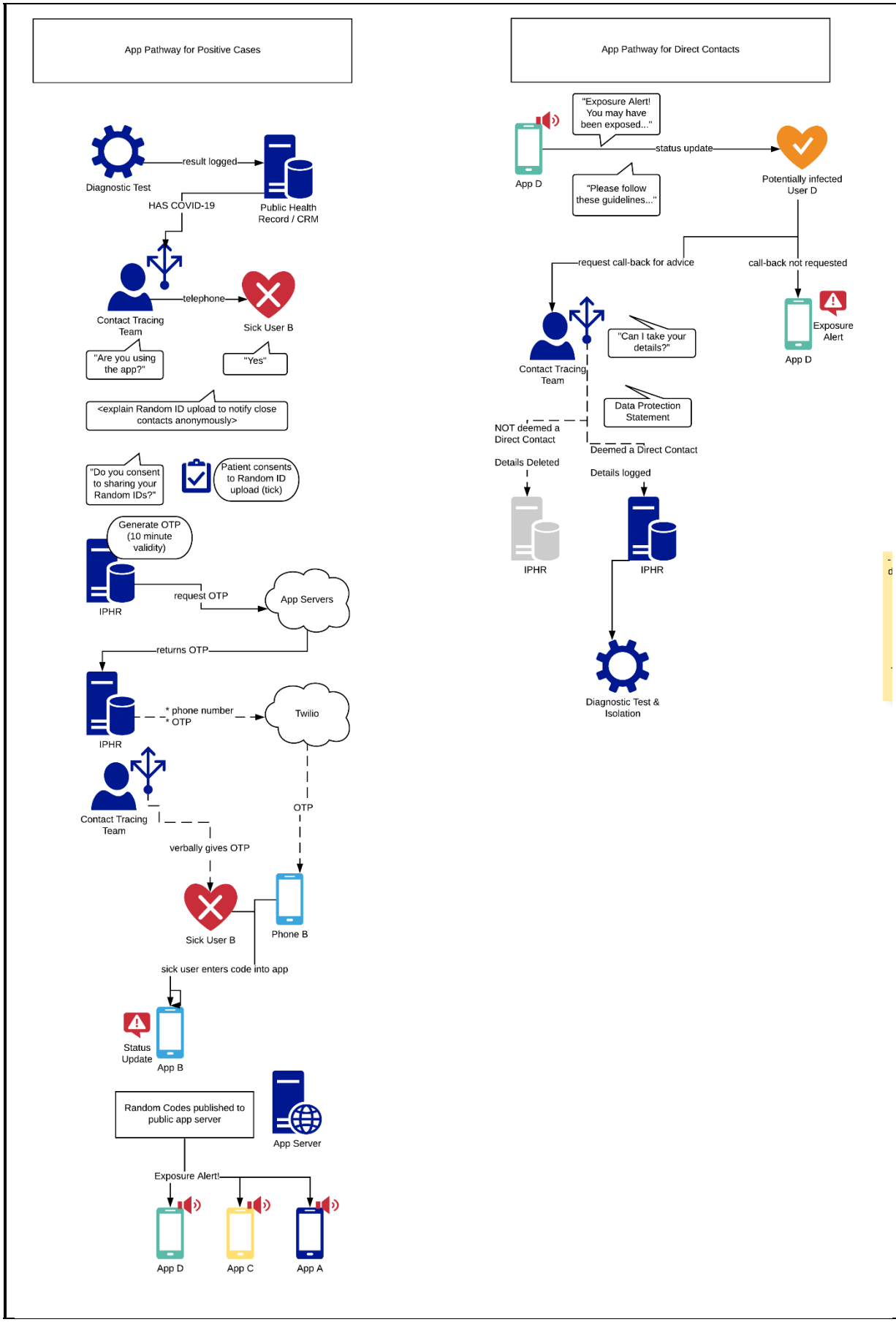
4.1 Provide a full description of the information lifecycle

There are four pieces of user data handled by the app :
1: Mobile phone number for notified exposed users who have requested a call-back
2: Date of last exposure for notified exposed users who have requested a call-back
3: Authorisation code for users with a confirmed diagnosis of COVID-19
4: User IP addresses and network layer security tokens

Stage of Processing	Description
Collection Where does the data originate from, who will collect it and how will it be data obtained?	1. Mobile phone number: the user can choose to enter their mobile phone number into the app for the purpose of requesting a call-back form Contact Tracing when/if they receive and Exposure Alert 2. Date of last exposure: is recorded by the app and stored in the app invisible to the user. 3. Authorisation code: is generated by the app servers and sent to the IPHR on request from the IPHR. At this point it is not associated with any user, it is simply a random code comprised of six (6) numbers. 4. IP and security tokens: are essential identifiers used in internet traffic and are generated by the device (IP) and app (security tokens).

Storage Describe where and how the data is to be stored	1. Mobile phone number: is stored in the app until an Exposure Alert is received. Then the number is sent to a call-back queue in the IPHR with a 14 day retention period. 2. Date of last exposure: is sent with the mobile phone number to a call-back queue in the IPHR with a 14 day retention period. 3. Auth code: is used for authorising the upload of Random IDs and not stored in the app or app servers. The SMS text and code are stored in the IPHR case record, but will be invalid 10 minutes after generation. 4. IP and tokens: are stored in the app. The app servers store security tokens for 60 days, the app firewall stores IP addresses for 14 days.
Use Describe how the data will be used. Describe whether it involves new technology or novel processing.	1. Mobile phone number: is used by a Contact Tracing handler to call the exposed app user to determine if they had a probably genuine exposure and are a Direct Contact, or if their exposure was historic or false positive and not a genuine case. The handler will also provide support and guidance to the user and may refer them for testing. 2. Date of last exposure: as above. 3. Auth code: on diagnosis of COVID-19 the Contact Tracing Team will call the person and ask if they are an app user. If yes, the user is asked to consent to sending their Random IDs to the app servers so that their close contacts can be notified anonymously. If consent is given, the handler will use the IPHR SMS functionality (via third party Twilio) to send the auth code to the user's mobile phone number listed in the IPHR and confirmed verbally by the user. The Authorisation code is valid for 10 minutes and is also displayed in the case record in the IPHR. On receipt the user enters the code into the app to authorise the upload of their Random IDs. 4. IP and tokens: are used for app-to-app server communication (e.g. to fetch app content). IP addresses may be used to investigate malicious internet traffic.
Access Describe who has access to the data throughout the life of the processing	1. Mobile phone number: only the user and the Contact Tracing Team comprised of named and authorised officers have access to the number and only in the event that the user receives an Exposure Alert and has requested a call-back. 2. Date of last exposure: only the Contact Tracing Team comprised of named officers have access to this information and only in the event that the user receives an Exposure Alert and has requested a call-back. 3. Auth code: the app servers generate the code but do not know any information about who/which mobile number the code is for, the Contact Tracing Team can see the code and the user receives it via SMS or verbally from the handler. Twilio, a 3rd party SMS provider and any mobile networks used to send the SMS to the user can also see the code. 4. IP and tokens: these are invisible to the user; only the app, the servers and any internet routing equipment access these identifiers.
Recording Describe the processes for recording the data	1. Mobile phone number: is entered into the call-back settings of the app by the user either during on-boarding or at any point in the Settings menu. 2. Date of last exposure: is only sent to the IPHR call queue when a user received an Exposure Alert. 3. Auth code: once entered into the app and used to authorise Random ID upload, it is deleted from the app. The IPHR records the code in the case record, subject to IPHR retention policies. 4. IP and tokens: the app records the IP and security tokens in its system, the app servers retain security tokens for 60 days, the app firewall retains IP addresses for 14 days.
Processors Describe the use of processors. If a third party is being used then	1. Mobile phone number: the app uses Amazon Web Services to coordinate data sent from the app to the IPHR, all connections are encrypted and no data is persisted in AWS. The Contact Tracing Team can view the number in the IPHR call-back queue.

is a contract in place to regulate the relationship? Will the data be processed outside of the EU?	2. Date of last exposure: as above. 3. Auth code: the app servers generate the code, the Contact Tracing Team communicate the code to the user. Twilio is used to send the SMS containing the code to the user, Twilio is US-based, a DPA is in place and contains the Standard Contractual Clauses. Twilio has also adopted Binding Corporate Rules for its processing activities outside the EEA. The auth code may be processed by mobile networks and Twilio **outside** of the EU. 4. Ip and tokens: only processed by the app and the app servers, IP is processed by internet routing infrastructure.
Sharing • With which external organisation(s) is the data shared, what data is shared, and why? • Describe any sharing that will occur within the SoJ • Outline any national and international sharing or processing.	1. Mobile phone number: is not shared, except to the extent where the IPHR data may be shared for the 14 day duration the mobile number is stored in the Call-Back queue in the IPHR. Further details on how the personal data stored in the IPHR is processed is set out in the DPIA Ref DPIA/11/2020/F 2. Date of last exposure: is not shared, except to the extent which IPHR data may be shared for the 14 day duration the date of last exposure is stored in the Call-Back queue in the IPHR. 3. Auth code: is shared by the app to the extent that IPHR data is shared, 4. IP and tokens: are not shared. IP addresses may be shared with Law Enforcement if malicious internet traffic to the app servers is detected.
Review and Retention Describe your plan for review and retention, linking to a retention schedule where appropriate	1. Mobile phone number: is secured on the app until the user removes it via Settings. When a call-back request is generated, the mobile phone number and date of last exposure are stored in a queue in the IPHR until a handler can review the task. If the case is not deemed a risk, the task (including the mobile phone number and date of last exposure) will be deleted. If deemed a genuine Direct Contact the call handler will store the mobile number and date of exposure in a new IPHR case record governed by IPHR retention policies. The change in Retention Policy is clearly explained to the user on the call. 2. As above. 3. Auth code: is retained in the IPHR case record as per IPHR retention policies. Note that the code is only valid for 10 minutes from generation. 4. IP addresses are retained for 14 days unless malicious internet activity is detected, in which case the IP addresses involved will be retained for as long as required to complete the investigation. Security tokens are stored for 60 days then automatically deleted.
Disposal Describe the process for disposal of data, including when and how.	1. Mobile phone number: the user may delete the number at any time, if the user leaves the App or deletes it from their phone, the number will also be deleted. If the Government of Jersey decommissions the App (i.e. Pandemic over) the number will also be deleted along with other app data. 2. Date of last exposure: can be deleted by the user at any time via the app or via the phone Exposure Notification Service Settings in the smartphone system. 3. Auth code: is deleted by the app after use. Is removed from the IPHR case record as per IPHR retention policies. 4. IP addresses are deleted from the app firewall after 14 days unless needed to investigate malicious activity. Security tokens are automatically deleted after 60 days.
4.2 Diagrams and Tables If you have a diagram or table which describes or demonstrates the processing then please include below.	


App Pathway for Positive Cases
Diagnostic Test
result logged
HAS COVID-19
Public Health Record / CRM
Contact Tracing Team
telephone
Sick User B
"Are you using the app?"
"Yes"
<explain Random ID upload to notify close contacts anonymously>
"Do you consent to sharing your Random IDs?"
Patient consents to Random ID upload (tick)
Generate OTP (10 minute validity)
IPHR
request OTP
App Servers
returns OTP
IPHR
* phone number
* OTP
Twilio
Contact Tracing Team
OTP
verbally gives OTP
Sick User B
Phone B
sick user enters code into app
Status Update
App B
Random Codes published to public app server
App Server
Exposure Alert!
App D
App C
App A
App Pathway for Direct Contacts
"Exposure Alert! You may have been exposed..."
App D
status update
"Please follow these guidelines..."
Potentially infected User D
request call-back for advice
call-back not requested
Contact Tracing Team
"Can I take your details?"
Exposure Alert
App D
Data Protection Statement
NOT deemed a Direct Contact
Deemed a Direct Contact
Details Deleted
Details logged
IPHR
IPHR
Diagnostic Test & Isolation

4.3 Assets Describe the assets that you intend to use.	
Asset	**Description**
Hardware	User devices, AWS servers, the IPHR hosted on Microsoft Azure, covidalert.gov.je website hosted on Gov Sharepoint on Microsoft Azure
Software	The IPHR, the Jersey Covid Alert app, the covidalert.gov.je website, Twilio SMS integration in the IPHR
Networks	The Internet, Twilio's mobile network carriers for SMS delivery
Hardcopy/paper	none
Any other relevant assets	n/a

Section 5 – Full Risk Assessment

Identify and Assess Risks

In this section you must detail **all** data protection risks, as well as any associated with privacy and the rights and freedoms of individuals. The section focuses on specific data protection and privacy principles. **The assessment criteria outlined in italics in section 5.1 applies to all categories** in Section 5 and 6 i.e. for 'likelihood' you must always assess whether it is 'remote', 'reasonably possible', or 'probable.

Severity of impact	Serious harm	Low Risk	High Risk	High Risk
	Some impact	Low Risk	Medium Risk	High Risk
	Minimal impact	Low Risk	Low risk	Low Risk
		Remote	Reasonable possible	Probable
	Likelihood of harm			

Consider the impact on individuals and any harm or damage that might be caused, whether physical, emotional or material. Different levels of interference may occur at different stages of the information lifecycle. The European Court of Human Rights has held that a public authority merely storing data is a limitation on the human rights of data subjects.

Where risks are identified you must take steps to integrate solutions into the process/project and this must be recorded. If any **residual risks are 'high'** then the Office of the Information Commissioner (OIC) must be consulted prior to processing commencing. If this is the case, please discuss with your Data Champion, who will in turn liaise with the CDPU before any approach is made to the OIC. Examples of risk factors are provided at the top of each section – these examples are a starting point and you must ensure that all factors relevant to your process/project/proposal are considered. Further examples are provided within the guidance. If you run out of space then insert more lines into the table. When completing each section, if you are unable to identify a risk relevant to your proposal then please state "**No risks identified**".

Examples of risks to individuals include:	**Examples of corporate risks include:**
• Discrimination • Identity theft • Financial loss • Reputational damage or embarrassment • Physical harm • Wrongful arrest or prosecution • Loss of confidentiality • Inability to exercise rights • Significant economic or social disadvantage	• Failure to protect the public • Loss of public confidence • Civil litigation • Reputational damage • Regulatory action • Breaching other legal obligations

You should identify **lower risk alternatives** such as

- Deciding not to collect certain types of data
- Reducing the scope of processing
- Reducing retention periods
- Taking additional technical security measures
- Providing staff with training and guidance to understand the risks
- Anonymising or pseudonymising the data
- Using different technology
- Using an alternative third party processor

5.1 Fair, Lawful and Transparent

Data must be processed lawfully, fairly and in a transparent manner NOTE: The 'transparency' element does not apply to law enforcement processing, although there is still a requirement to consider providing individuals with information about how their data will be processed.

Example –

- Do you need to create or amend a privacy notice?

Describe the source of risk and the nature of potential impact on individuals.	**Likelihood of harm**	**Severity of harm**	**Initial Risk**	**Mitigation/ Solution**	**Result**	**Residual Risk**
				Describe the mitigation and whether it will be implemented	*Is the risk:* • *Eliminated* • *Reduced* • *Accepted*	*High* *Medium* *Low*

Risk that users may unfairly be denied services or entry to place if they have received an Exposure Alert	Medium	Medium	Medium	The App user can delete all previous notifications with one button preventing the unofficial use of the app as an entry check.	Reduced	Low

5.2 Specific, explicit and legitimate purpose

The purpose for which you process personal data must be specified, explicit and legitimate. Personal data collected must not be processed in a manner that is incompatible with the purpose for which it was originally collected.

Examples -

- Does your project plan cover all of the purposes for processing personal data?
- Are all elements of the processing compatible with the original reason and justification for the processing?

Describe the source of risk and the nature of potential impact on individuals.	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk
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	Medium	Low	Low	Advisory 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 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	Accepted	Low

5.3 Adequate, relevant and not excessive

Personal data processed must be adequate, relevant and not excessive in relation to the purpose for which it is processed

Examples –

• Is the quality of the information adequate for the purposes it is used? • Are measures in place to ensure that data is limited to that which is needed to fulfill the aim of the processing - which personal data could you not use, without compromising the needs of the project?						
Describe the source of risk and the nature of potential impact on individuals.	**Likelihood of harm**	**Severity of harm**	**Initial Risk**	**Mitigation/ Solution**	**Result**	**Residual Risk**
The Jersey App is a response to the pandemic. The purpose of the app is to support and augment the Contact Tracing Team's 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.	Medium	Medium	Medium	- Implement clear and transparent internal communication including DPIA and source code publication by the Government of Jersey account on code hosting site GitHub (linked on covidalert.gov.je) - Terms of reference of the 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 the Jersey 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 - the Advisory Committee is responsible for the wind down once the pandemic is declared over.	Accepted - Strong governance is in place to ensure app scope creep is highly scrutinised.	Low
Data may be collected about children in the app. As the app is anonymous, it cannot perform an age verification check.	Low	Low	Low	Users are asked to confirm their age as the first step 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 (as above users must confirm they are over the age of 16).	Accepted	Low

				- Communication to ensure parents understand the age intention of the App.		
A pandemic response app may not give sufficient benefits to support the case for the proposed large-scale data processing	Low	Low	Low	Analysis of benefits to support the introduction of an app has been carried out and approved by the Scientific and Technical Advisory Cell and the Council of Ministers. - Use decentralised model to reduce data processed directly by the Contact Tracing Team. - 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 Advisory Committee to monitor effectiveness and benefits and to wind-down processing if appropriate. - Implementation of a robust testing - Engage intensively with other countries to align and to increase awareness and understanding of approaches used - Ensure app is entirely voluntary	Accepted	Low
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 unexpected to the users.	Low	Low	Low	App must first get user consent before metric data is collected or shared with the Contract Tracing Team - All metric data must by anonymised (or anonymised at the earliest processing point, noting IP address as per DPIA) and carefully reviewed for any reidentification 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	Accepted	Low
5.4 Accurate & timely						

Personal data processed must be accurate and, where necessary, kept up to date, and every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay.						
Examples – • If you are procuring new software does it allow you to amend data when necessary? • How are you ensuring that personal data obtained from individuals or other organisations is accurate? • Do you have processes in place to keep data up to date?						
Describe the source of risk and the nature of potential impact on individuals.	**Likelihood of harm**	**Severity of harm**	**Initial Risk**	**Mitigation/ Solution**	**Result**	**Residual Risk**
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	High	Low	Low	Engage in comprehensive testing with the app - 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. driver to turn off Contact Tracing while working) - Create pause functionality to allow users to pause while at home alone or in other isolated scenarios - 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	Accepted	Low
Risk that the Bluetooth proximity and power measurements do not record that a close contact that has occurred when a positive contact actually did occur (a false negative).	High	Medium	High	Ensure app is used to augment the existing contact tracing operation - Engage in comprehensive testing with the app - Use ENS to benefit from extensive capability of Google and Apple to do extensive testing- -Create a well-designed communication plan to ensure scenarios that help create false negatives are limited (e.g. phone left in bag/jacket)	Accepted	Medium
5.5 Retention Personal data must be kept for no longer than is necessary for the purpose for which it is processed. Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data.						
Examples – • What are the risks associated with how long data is retained and how they might be mitigated?						

• Has a review, retention and disposal (RRD) policy been established?						
Describe the source of risk and the nature of potential impact on individuals.	**Likelihood of harm**	**Severity of harm**	**Initial Risk**	**Mitigation/ Solution**	**Result**	**Residual Risk**
The use of the app may continue indefinitely or longer than justified by the defined purposes	Low	Low	Low	The Advisory Committee will ensure the App is shut down once the pandemic is declared over	Eliminated	Low
5.6 Security Personal data must be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).						
Examples – • What technical and organisational measures are in place to ensure that the date is protected to an adequate level? • What training on data protection and / or information sharing has been undertaken by relevant staff?						
Describe the source of risk and the nature of potential impact on individuals.	**Likelihood of harm**	**Severity of harm**	**Initial Risk**	**Mitigation/ Solution**	**Result**	**Residual Risk**
Risk that Contact Tracing can be used to identify and track people's location, rather than tracking the virus	Low	Low	Low	The App does not record location or enable GPS tracking. At present the Google store requires the user to switch Bluetooth and GPS with the same button but this does not mean the App uses GPS tracking	Eliminated	Low
Integrity of data is compromised. The random IDs, or mobile number uploaded to the IPHR in a call-back request is erroneous or corrupted, meaning it is unusable or unreliable.	Low	Medium	Low	App and related technology infrastructure has undergone extensive information security testing. - All traffic in transit is encrypted - Certificate pinning and other security mechanisms are implemented to protect against 'man in the middle' attacks	Reduced	Low
IP address is present in all data transfers from the app to the app backend and could be used to identify someone	Low	Low	Low	The app backend will not process 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	Accepted	Low

There is a risk that people will maliciously try to upload Random IDs without a confirmed, authorised diagnosis of COVID-19, creating false Exposure Alerts and causing unwarranted negative consequences for recipients.	Low	Medium	Low	Put in place an appropriate authorisation step so that only those authorised as having tested positive for the virus can upload their Random IDs - Ensure network and application firewall 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 all traffic to the app backend is protected via this means	Accepted	Low

5.7 Data Protection Rights

Data protection legislation gives data subjects various rights (listed below). Limiting or restricting any of these rights is likely to be a significant impact so the justification for any restriction, as well as mitigations, must be fully outlined.

Consider each of the rights listed below and assess whether data subjects would be able to fully exercise these rights. For example:
If an individual makes a subject access request, will you be able to easily identify, retrieve and extract the data to provide to your Data Champion?

1. Right to fair processing information
the right to be informed about the collection and use of their personal data.

2. Right of access (known as subject access)
The right to access personal data and supplementary information in order to be aware of and verify lawfulness of processing.

3. Right to rectification
The right to have inaccurate data rectified

4. Right to erasure
The right to have personal data erased (not an absolute right and only applies in certain circumstances)

5. Right to restrict processing
The right to request restriction or suppression of personal data (not an absolute right and only applies in certain circumstances)

6. Rights regarding automated decision making and profiling
Individuals should be protected from significant decisions being made solely on the basis of an automated decision

7. Right to object
The right to object to processing based on the performance of public task, direct marketing or scientific / historical research.

Describe the source of risk and the nature of potential impact on individuals data protection rights.	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk
Users can't exercise their data protection rights or don't know where to go to exercise them.	Low	Low	Low	Provision of a Privacy Notice accessible on App and website to ensure it is clear to data subjects what rights they have, how to exercise them and with whom - Implement a decentralised model for exposure notification to ensure limited personal data processed on app servers	Users able to exercise their rights Accepted	Low
Users are not given sufficient information about how the app works, what data will be collected and for what purpose in a comprehensive way	Low	Low	Low	- Clear Privacy Notice accessible on app and website explains how personal data is used by the app. -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 impact assessment (DPIA) - information in the App, the covidalert.gov.je website and on Government main website - Implement a communications plan to inform people about the app, what it does and what data is processed	Users able to exercise their rights Accepted	Low
Risk that suitable ways of withdrawing consent are not built into the app	Low	Low	Low	- App to provide ability to change consent settings for all consents given, individually, via Settings at any time - Use the Leave option or delete the app from phone on the app - this will delete any personal data held on the mobile phone. Security tokens are automatically deleted after 60 days.	Eliminated	Low

5.8 External Data Sharing, including the involvement of other Controllers and Processors

Your processing may involve the sharing of personal data with 3rd party individuals, organisations or agencies. Use this section to outline the risks that are associated with any data sharing of this nature, including the necessity and proportionality of any such sharing, the contracts or agreements in place, and any data security issues that this may present.

Examples –

- What contracts, information sharing agreements, data processing agreements or memorandums of understanding are in place?
- What assessments have been made of the 3rd parties to ensure they have adequate provisions for the technical and organisational security of personal data?
- Have suppliers been specifically asked to undertake a DPIA?

Describe the source of risk and the nature of potential impact on individuals.	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk
Role of Apple and Google may include processing 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.	Medium	Medium	Medium	- Continually monitor and engage with Apple and Google to understand their plans - 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	Part of a global problem accepted by anyone with a smartphone.	Medium
The risk that Twilio and any mobile network operators can identify people with COVID-19 because the Authorisation code is only sent to confirmed COVID-19 cases I the Random ID upload process.	High	Medium	High	use known and trusted SMS provider (Twilio) for this service - eventually move to a provider with trusted direct SMS routes to Jersey subscribers - one user cannot identify another user except by exchanging information outside of the app environment (i.e. someone tells someone else)	Accepted Only privileged users at Twilio or in mobile network operators can cause this harm.	Medium
5.9 International Transfers A third country is a non EU Member State, and in these circumstances there are limits to when you can share personal data. Certain conditions must be met – for further information refer to the DPIA Guidance at https://soj/CorporateProjects/GDPR/Pages/DataProtectionToolkit.aspx#anchor-7 .						
• If you will be making transfers, how will you ensure that the data is adequately protected? • Will we share data with a third party processor based outside the EU?						
Describe the source of risk and the nature of potential impact on individuals.	**Likelihood of harm**	**Severity of harm**	**Initial Risk**	**Mitigation/ Solution**	**Result**	**Residual Risk**
Where the data is stored on servers of US companies (i.e. Twilio, Amazon Web Services), US Government could use the Cloud Act to attempt to access the data	High	Low	Low	Amazon would have access to random ID's of infected users for the past 14 days through the AWS server system. The identity of users is not compromised. Terms are in place. Twilio would have access to the mobile phone numbers of users who have been diagnosed with COVID-19, by virtue of the fact that Auth codes delivered by Twilio are only sent to diagnosed users who consent to upload their Random IDs. Standard Contractual Clauses and Binding Corporate Rules are in place	Accepted	Medium

				with Twilio that contractually require them to protect personal data in accordance with data protection law. Twilio is also a large, well known and broadly used telecoms provider that adheres to ISO27001 and is SOC 2 certified. Their ability to comply with data protection was fully assessed by the Government at the time of their original appointment as an SMS provider for contact tracing purposes and they were found to be sufficient. The personal data processed by Twilio in relation to the App is also limited to the authorisation code and no further personal data is shared with Twilio by the App. Based on the White Paper by the US Departments of Commerce and Justice, we do not consider this type of data to be of interest to US National Security Agencies. Disclosure of personal data to the US government is also likely to do them considerable reputational damage.		
Risk that users with COVID-19 mobile phone number and Authorisation code will be transferred to further jurisdictions outside EEA (by Twilio and any mobile network operators used to deliver SMS to Jersey subscribers), which are not identified by Twilio and are not subject to GDPR.	High	Low	Medium	Data processing agreements are in place with Twilio and AWS, the non-EEA data processors involved in the app, which contain the EC Standard Contractual Clauses and require the processors to ensure they have appropriate mechanisms in place with sub-processors located outside the EEA.	Accepted	Low

5.10 Human Rights

The European Convention on Human Rights sets out numerous rights and freedoms. Limiting or restricting any of these rights is likely to be a significant impact and result in a residual high risk so the justification for any restriction, as well as mitigations, must be fully outlined. If your actions will interfere with any of the rights listed below then you must clearly outline why it is necessary and proportionate.

You must first consider: **Article 8: Right to Privacy** – Will the proposal adversely impact an individual's right to respect for privacy in terms of their private and family life subject to certain qualifications?

You must also consider the following:

- Article 2: Right to Life
- Article 3: Prohibition of Torture
- Article 4: Prohibition of Slavery or Forced Labour
- Article 5: Right to Liberty and Security
- Article 6: Right to a Fair Trial
- Article 7: Right to no punishment without law
- Article 9: Right to Freedom of Thought, Conscience & Religion
- Article 10: Right to free Expression
- Article 11: Right to Freedom of Assembly and Association
- Article 12: Right to Marry
- Article 14: Right to Freedom from Discrimination

Describe the source of risk and the nature of potential impact on individuals.	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk
Continually downloading random IDs may consume a user's network data allowance.	Low	Medium	Low	- the design minimises the amount of data - current estimates for 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 - discussions with Telcos - WiFi data connection usage avoids problem	Accepted	Low
Technical issues with the app that would reduce function or interfere in a negative way in the working of the other phone's functions	Low	Low	Low	App has been 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	Accepted	Low

5.11 Additional Risk Factors
Describe any further risks, ensuring that any risks not already identified are included.

Additional risks may for example include:

- Internal data sharing - With which parts within your SoJ department is the information shared, what information is shared and for what purpose?
- If you are processing special categories of data then what risks have you identified?

Describe the source of risk and the nature of potential impact on individuals.	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk
Users losing control of their mobile device allowing people to see any Exposure Alert (if present). Even if the exposure alert notification generated by the phone does not explicitly say “Exposure detected” by virtue of the fact there is a notification, a snooper can infer exposed status.	Medium	Medium	Medium	App design limits personal data present in the app. - Ensure app can run in the background and when locked. - The communications plan for the app will remind people that they should take suitable precautions to protect their mobile device. - User can clear Exposure Alert notifications at any time in App Settings.		Low

				- Users can choose not to allow the App to generate notifications, but must then check the app regularly for exposure alerts. - include in FAQ instructions on how to set app notification permissions so that they will not be visible on the lock screen.		
The Authorisation Codes are intercepted and used to identify an individual's health information by virtue of the fact that the codes are only sent to those who have tested positive for Covid 19	Low	Medium	Medium	Risk of OTP message interception in transit: this may be exploited by mobile network insiders, or sophisticated attackers with special access or equipment. Anyone with such access is likely to intercept other information about the user, such as the content of the call from the Contact Tracing Team, or other SMS messages which could contain further personal and private information. Risk of local access to the app and the device: as the affected individual should be in isolation, access to their mobile device is likely to be restricted. - The Contact tracing Team script includes a check whether the user has their device with them at the time of OTP generation. - After the Authorisation code has been entered in the app, it is not retained or visible in the app. - The app design does not disclose the status of the user as COVID positive after Random ID upload. - The SMS may be deleted by the user after use.	Accepted	Low

Section 6 – Law Enforcement Processing - Additional Risks
This section is only applicable to a process/project/proposal involving law enforcement processing. If you are solely processing non-law enforcement data then move to Section 7.
6.1 Data Logging *Where data is processed electronically then logs must be kept for certain actions. This is to enable effective audit of processing systems, data sharing, and to verify ongoing lawfulness of processing.*
If the data is processed electronically then will a log be retained of the following actions:

Collection *Alteration* *Consultation* *Disclosure* *Combination* *Erasure*	☐ *Yes* ☐ *No (risk must be recorded)* ☒ *Not applicable*

If you answered "no" then you must record this as a risk below.

Describe the source of risk and the nature of potential impact on individuals.	*Likelihood of harm*	*Severity of harm*	*Initial Risk*	*Mitigation/ Solution*	*Result*	*Residual Risk*

6.2 Data Categorisation
When processing data for law enforcement purposes, you must provide where relevant and as far as possible a clear distinction between categories of data subject.

Will there be a clear distinction between different categories of personal data subjects, for example subjects who are:

Suspected of having committed, or are about to commit, a criminal offence *Convicted of a criminal offence,* *Victims of a criminal offence,* *Witnesses to a criminal offence.*	☐ *Yes* ☐ *No (risk must be recorded)* ☒ *Not applicable*

If you answered "no" then you must record this as a risk below.

Describe the source of risk and the nature of potential impact on individuals.	*Likelihood of harm*	*Severity of harm*	*Initial Risk*	*Mitigation/ Solution*	*Result*	*Residual Risk*

Section 7 – Outcome and Review			
Item	Name	Date	Notes
DPIA reviewed by (Data Champion), to include summary of advice, and whether the OIC must be consulted:	Julie-Ann Quail	17/09/2020	Happy with risks identified and mitigation put in place. Would like the DPIA to be reviewed by JOIC if it has not been already
Residual risks approved by (Information Asset Owner):		DD/MM/YYYY	If accepting any residual high risk please consult with your Data Champion and CDPU as the OIC

			will need to be consulted before the project may go ahead.

Review
A DPIA is a process that should be reviewed throughout the lifecycle of the processing – it does not end at go live. Please outline the review process that you will undertake to ensure that the risk mitigations have been successful and that no new risk factors have emerged.
Outline: • Who will be responsible for reviewing the processing • The frequency of review The date of the next review
The App Advisory Committee will be responsible for reviewing changes to the DPIA and ensuring decisions taken are appropriately analysed and reflected in this document.
The date of the next review is the 20th October.

Section 8 – Record Keeping	
The final DPIA should remain with the Information Asset Owner. A copy should be forwarded to the CDPU where a central register will be maintained.	
Date copy forwarded to CDPU at dataprotection2018@gov.je and by whom:	13/10/2020 Rachel Wijsmuller

Appendix A – App Advisory Board Terms of Reference

Status

The Advisory Committee (the "Committee") is a non-statutory advisory body that compromises of representation from various organisations as detailed in the membership section below.

The parties to be Advised are the implementation team (consisting of a subset of the Committee), and the Council on Ministers on request.

Overview

The Committee is established to work collaboratively on decisions in relation to the rollout, ongoing operation, and development of the Jersey App. The Committee will engage with and make submissions to the Data Protection Officer, Law Officers' Department and Public Health as it deems necessary. The Committee is to support, guide and oversee the activities of the implementation team in the following regard:

- Oversee that any enhancements of the Jersey App are in line with the app design principles set out in this document;
- Oversee that the functioning and use of the Jersey App is aligned with the purposes of the app as set out in this document;
- Oversee the ongoing development and use of the Jersey App and ensure it aligns with Public Health policy;
- Use effective monitoring to assess the ongoing efficacy of the Jersey App in contributing to the pandemic response and make necessary recommendations for improvement;
- Oversee the decommissioning of the app within 90 days if the Jersey App is assessed as ineffective as part of its efficacy monitoring process (above), or if, the pandemic is declared over by the Government;
- Oversee that due consideration is given to relevant guidelines issued by the Jersey Information Commissioner, the European Data Protection Board and the European Commission;
- Oversee the Jersey App and ensure it continues to be used on an entirely voluntary basis, and if anything should undermine this principle to report to the Test and Trace Programme Board, with proposed appropriate measures, including the potential to legislate;
- Oversee the implementation of a communications plan to ensure the Jersey App is rolled out in a transparent manner;
- Oversee that the Jersey App processes any personal data in line with the DPIA and that the DPIA is kept up to date and public;
- Oversee the ongoing organisational and technical measures to secure the Jersey App.

Membership

Membership shall consist of representation from the following organisations:

- Contact Tracing Team
- Digital Health
- Digital Jersey
- Digital Policy Unit
- Justice and Home Affairs (Test and Trace Programme)

- Modernisation and Digital

Members are required to send apologies should they be unable to attend scheduled meetings which may be called from time to time to discuss major decisions or review ongoing work. Members are also required to ensure that responses to any action points they have committed to from the prior meeting are submitted in advance.

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, such additional members may consist of:

- Communications Unit
- Government of Jersey Data Protection Officer
- Law Officers' Department
- Public Health Team
- Representative from the Scientific and Technical Advisory Cell (STAC)

Meetings & Reporting

Meetings will be held 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. Meeting minutes will be available on request, selected topics may also form the content for blog posts about aspects of the app development.

Quorum

A quorum shall consist of representatives from at least 3 organisations with a minimum of 5 members present in total. Decisions requiring particular expertise shall not be considered quorate if a representative from the relevant Department is not present.