Privacy Notice Jersey COVID Alert App

This Privacy Notice is for the Jersey COVID Alert App (the “App”) which can be downloaded to mobile devices from the Google Play and Apple App Stores. The App is designed to reduce the spread of Covid-19 by allowing users with a confirmed diagnosis to anonymously alert other App users that they have recently been too close to for too long a period (a close physical contact). It also allows users in Jersey to keep up to date with the latest statistics and receive advice related to the Covid-19 pandemic.

The App has been developed on behalf of Jersey’s Contact Tracing Team who are part of Infrastructure, Housing and Environment who are registered as the Data Controller of personal data submitted to the App. This Privacy Notice provides a broad description of the way your personal information will be processed when submitted via the App.

Your privacy is protected

- The App does not record your location and does not use GPS.
- The App is built with strong privacy protection.
- Use of the App is always voluntary.
- The App will ask your permission to share any data.
- The App can be uninstalled at any time.
- It is extremely unlikely that you could be identified by other users while using the App.

The App has specifically been designed so that it will:

Commented [TM1]: I think this sits better here

- Never know your location
- Never know your name or address
- Never know the Phone’s contacts
- Never know details of your health

Purpose of the App

The primary purpose of this App is to reduce the spread of Covid-19 by providing an Exposure Notification service. If you receive a positive Covid-19 diagnosis, the Exposure Notification service allows you to anonymously alert people you have been too close to for too long a period (a close physical contact) prior to your diagnosis. The App also allows you to receive alerts notifying you if you have been in close physical contact with someone, prior to their diagnosis, who has Covid-19.

The App will also allow you to:

- Keep up to date with local statistics and information about coronavirus in Jersey.
- Be provided with links to trusted information resources.

- Be contacted by the Government of Jersey Contact Tracing Team when you receive an Exposure Alert (if you opt to share your telephone number through the App – see further below).

The Exposure Notification process is achieved through the exchange of anonymous Random IDs generated by the Exposure Notification Services in your smartphone operating system and not by sharing your personal data with other users of the App.

Which personal data the App will collect or store

For Exposure Alerts:

Random IDs exchanged by the Exposure Notification Services are stored for 14 days on your phone for the purpose of notifying you of a possible Covid-19 exposure. The Random IDs cannot be used to identify you and are not considered Personal Data for the purposes of the Data Protection (Jersey) Law 2018. There are two types:

- Random IDs sent by your phone; and
- Random IDs collected from other phones near you.

If you receive an Exposure Alert, no information about the positive case will be shared and you will not know where or when contact with the person who has COVID-19 took place.

For Contact Tracing Team Call-Back:

You may optionally provide your mobile phone number to the App during App set-up or later in settings so that you may be called by the Contact Tracing Team in the event that you receive an Exposure Alert. Your number remains on your device until this occurs. The legal basis for installation of the App and storing of personal data on your device in this way is consent. You can withdraw your consent to your personal data being stored in the App by deleting the App from your phone or removing your phone number from the App at any time.

If you choose to share your mobile number with the App, both your mobile phone number and the date of your last exposure to someone with COVID-19 will be sent to the Contact Tracing Team automatically by the App following an Exposure Alert. The Contact Tracing Team will use your mobile phone number to contact you by phone to provide further specific advice and support. If you did not provide your contact number, the App will not automatically share your mobile number but you are strongly advised to contact the Coronavirus Helpline on 445566 or Contact Tracing Team for support directly.

Your mobile phone number and the date of your last exposure will be stored in a call queue in the Integrated Public Health Record (IPHR) database maintained by the Contact Tracing Team and deleted after use (see the section “Data Sharing” below for further details).

The legal basis for this processing of your personal data by the Contact Tracing Team is that it is necessary for reasons of public interest in the area of public health provided for by Article 26 of the States of Jersey Law 2005 and the Loi (1934) sur la santé publique (Law (1934) on Public Health).

Note that, once you receive an Exposure Alert, your mobile number will be shared with the Contact Tracing Team and stored in the IPHR for this purpose and not on the basis of consent. Withdrawal of consent (by removing the App or your phone number from the App) after an Exposure Notification will therefore not result in your personal data being removed from the IPHR.

Commented [TM2]: Please confirm this is correct and the number is not shared by the App until an Exposure Alert is received?

Further information relating to the processing and retention of data within the IPHR database can be found in a separate Privacy Notice, set out at this link.

For Uploading Random IDs:

If you are diagnosed with COVID-19 you will be asked to consent to the sharing of the Random IDs in your phone so that the app can anonymously alert other app users of their exposure to you. The Contact Tracing Team will ask you to confirm your mobile phone number to send you an Authorisation Code by SMS. The Authorisation Code will enable the upload of your Random IDs in the App. This code is valid for 10 minutes, and is not stored in the app or app servers, but is recorded in your case file within the IPHR database.

The legal basis for the processing of your personal data is that it is necessary for reasons of public interest in the area of public health provided for by Article 26 of the States of Jersey Law 2005 and the Loi (1934) sur la santé publique (Law (1934) on Public Health).

For Networking

IP addresses and security tokens used in the app-to-server communications are only used for networking and for no other purpose (see section on IP addresses below).

IP address data is stored in the firewall system log for 14 days and, if suspicious activity is detected, the data may be shared with law enforcement agencies for the purposes of investigating the activity.

The legal basis for the processing of your personal data is that it is necessary for reasons of public interest in the area of public health provided for by Article 26 of the States of Jersey Law 2005 and the Loi (1934) sur la santé publique (Law (1934) on Public Health).

Do you have to provide your personal data?

There is no statutory or contractual requirement for you to provide any of your personal data. However, if you choose to install the App on your device and choose to upload your mobile phone number, your personal data will be used for the purposes set out in this Privacy Notice.

Special Category Data

In the event that you receive a positive COVID-19 diagnosis and you have given your consent to share your Random IDs, the app processes an Authorisation Code so that the past 14-days

of Random IDs stored on your phone can be automatically uploaded to the secure app servers. By virtue of the fact that this only happens when you have a confirmed diagnosis of COVID-19, and you have given consent to share your phones' Random IDs the Authorisation Code is considered Special Category Data.

The diagnosis itself or any other health related information is NOT processed by the App. The App does not store the Authorisation Code after it has been used. The legal basis for processing this Special Category Data is that it is necessary for reasons of public interest in the area of public health.

The Information submitted by you as a user of the App will not be used to identify you. We recognise the importance of not identifying individual App users.

We only process your mobile phone number if you request a Contact Tracing Call-Back in the event of an Exposure Alert (see 'For Contact Tracing Team Call-back' below). This is entirely voluntary and if you choose not to provide your mobile phone number, you are not precluded from using the App. You may also remove your phone number from the App at any time.

The legal basis for the processing of your personal data is that it is necessary for reasons of public interest in the area of public health provided for by Article 26 of the States of Jersey Law 2005 and the Loi (1934) sur la santé publique (Law (1934) on Public Health)..

There is no statutory or contractual requirement for you to provide any of your personal data.

Data Sharing

If you choose to include your mobile number in the App, both your mobile phone number and the date of your last exposure to someone with COVID-19 will be sent to the Contact Tracing Team automatically by the App following an Exposure Alert. This data is stored in the Integrated Public Health Record (IPHR) database maintained by the Contact Tracing Team for a limited time. Certain personal data in the IPHR may be shared with other Government of Jersey departments and law enforcement in certain circumstances. For further information on this sharing please see the Privacy Notice, set out at this link.

IP address data may also be shared with law enforcement agencies in the event of suspicious activity.

Data Processors

The following third parties are data processors in relation to the App:

1. The App is hosted by Amazon Web Services (AWS) who act as data processors on the Government of Jersey's behalf. AWS are subject to a Data Processing Agreement that restricts their use of your personal data and requires them to protect it in

accordance with the data protection laws. Data stored on AWS is encrypted at rest and is transferred via encrypted connections.

2. Twilio is a US-based third-party SMS provider which is used by the IPHR to send SMS messages. Your mobile phone number may be transferred outside the EEA. The transfer is subject to the European Commission's Standard Contractual Clauses which require that your personal data is protected in accordance with the standards set out in the Data Protection (Jersey) Law 2018.

Retention of personal data

You can remove your mobile phone number from the App at any time. You can also delete the App which will result in data being deleted from your phone immediately. Security tokens used for app-to-server communication will be automatically deleted from the server after 60 days.

Data shared with the Contact Tracing Team will be stored in the IPHR data base. Further information relating to the processing and retention of data within the IPHR database can be found in a separate Privacy Notice set out at this link.

Deleting Data

All Random IDs are deleted from your phone after 14 days. You can delete the App at any time. If you delete the app, the Random IDs stored in your phone will automatically be deleted after 14 days. You can also delete the Exposure Logs yourself via the Settings on the App.

Location Services

If you have an Android Phones

Due to a limitation in the Android operating system, geolocation services must be turned on to allow the random codes to be exchanged via Bluetooth. The App does not access your location data and has no way of knowing your location, however Google may have access to this information. If you have an Android phone you may wish to use the lowest accuracy option for location and turn off Google Location History.

The app does not have permission to use location services on any phone; you can verify this in the App's permissions in your phone settings at any time.

If you have an Apple iPhone

To use the Exposure Alert function, you will need to switch on Bluetooth and Exposure Notifications, this happens automatically in app set-up. The App does not use location data and does not have permission to use location services.

IP addresses

The App system server will never store IP addresses; these are separated from uploaded Random IDs and any associated metadata, by the firewall and discarded.

To protect the system and its users, the firewall stores IP addresses in its system log according to a specified retention policy.

The system firewall logs:

- Are kept for up to 14 days under normal conditions. If an investigation into suspicious activity is required, the logs may be retained for the duration of the investigation.
- Can only be used for ensuring performance and responding to security threats.
- May be shared with law enforcement, as required by law if there is an investigation into suspicious activity.

Children's data

The App is not intended for anyone under 16. As such, we do not knowingly collect personal data from anyone under 16.

Interoperability with other Contact Tracing Applications

The 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 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 you 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.

Your Rights

The Data Protection (Jersey) Law 2018 provides you with rights relating to your personal data:

- The right to be informed about your personal information and how it is being processed;

- The right to make a subject access request;
- The right to have personal data rectified if it is inaccurate or incomplete;
- The right to have personal data erased, in specific circumstances (this does not apply where processing your personal data is necessary for reasons of public interest in the area of public health);
- The right to restrict the processing of personal data, in specific circumstances;
- The right to object to the processing, in specific circumstances;
- Rights in relation to automated decision making and profiling;

Please see below or visit the Government of Jersey's data protection webpages for contact details and further information on how to exercise your rights.

Further information on your rights can be found on the Jersey Office of the Information Commissioner's website at this link.

The App contains a link to the Covid website: https://covidalert.gov.je

Complaints

If you are unhappy with any aspect of this privacy notice, or with how your personal information is being processed, please contact the Data Protection Officer at the following address:

Email: DPO@gov.je

If you are still not happy, you have the right to complain to the Office of the Information Commissioner (JOIC):

Jersey Office of the Information Commissioner
2nd Floor
5 Castle Street
St. Helier
Jersey
JE2 3BT
Email: enquiries@jerseyoic.org
Website: https://jerseyoic.org

Contact us about Security Concerns

If you are a security professional and have found a vulnerability in this website or the Jersey COVID Alert app, we encourage you to let us know so that we can resolve the issue. Please email covidalert@gov.je with "Responsible Disclosure" in the subject line.

Changes to this Privacy Notice

This Privacy Notice will be kept under regular review and any updates will be placed on this website.