StopCOVID NI – Privacy Information

Data Controller Contact Details

Department of Health (DoH)
Castle Buildings
Stormont
Belfast
BT4 3SG

Contact- Chief Digital Information Officer Group

CDIO@health-ni.gov.uk

Data Protection Officer

Charlene McQuillan

DPO@health-ni.gov.uk

Introduction

The purpose of this information notice is to explain how the 'StopCOVID NI' Proximity app works, what data is collected by the app, and who has access to that data and the purposes for which they use it.

Use of the app is entirely voluntary and is available to download for free from the Apple App Store and the Google Play Store. The app runs on iPhones that support iOS 13.5 and higher, and Android phones running Android 6.0 and higher. The App is intended for persons aged 11 years of age, or older. You will be asked to confirm that you are 11 years or older when you download the App. The App is only intended for use by individuals resident in Northern Ireland. You will be asked to confirm residency and will be discouraged from using the App if you do not meet this criteria. We accept no liability for improper use, outside these defined conditions.

The Data Controller

The Department of Health (DoH) in Northern Ireland is the Data Controller – it has decided the means and purposes for the processing of data collected and used by the app. The DoH, working with the Health and Social Care Board and Public Health Agency (PHA), has commissioned all app related systems for processing all data. The DoH provides strategic direction for the app.

The DoH is therefore responsible for your personal data and has determined its responsibilities for compliance with its obligations under data protection laws. The DoH has provided access to speak to someone via '**0300 200 7896**' Monday-Friday (excluding bank holidays) between the hours of 8:30am – 5:30 pm, should you wish to raise an issue in relation to how your data is managed by the App, though note that you also have the right to contact the Data Protection Officer in this regard.

What the app does

The purpose of the app is to support the public health response to the COVID-19 crisis in Northern Ireland. The app has the following functions:

- Exposure Notification – the app, through use of anonymous 'keys', records when app users' phones have been in proximity to each other, for a sufficient period of time to mean that it is possible that the coronavirus has been passed on. Should an app user test positive for COVID-19, it is possible for them to alert other app users anonymously via the functions supported by the app.
- Registering a Positive Test Result – app users who have a positive test for COVID-19 will receive a randomly generated 'authorisation code' via SMS text message. This process is managed via a separate test registry, administered by the Regional Business Services Organisation (in accordance with its statutory functions as defined in the Health and Social Care (Reform) Act (Northern Ireland) 2009). This is separate from the app, in order to keep personal and identifiable information separate from the app.
- Other Functions – the app will collect Metric data which do not identify you in order to create aggregate views of how the app is being used and the impact it is having on

controlling the spread of the virus. Here is a list of the app metrics which, are collected from your app. The collection of these metrics is essential in order to prove efficacy and gain **Cє** accreditation:

- The total number of app users
- The total number of instances where 'diagnosis keys' have been uploaded
- The total number of 'exposure notifications' triggered

The DoH will not know any of these instances related to any individual app user, simply total numbers (for the region) of 'authorisation codes' and 'exposure notifications' in any given time period. **While this data is not identifiable, as a precaution,, we treat the metrics as if they were identifiable 'health data', in order to ensure this information is fully protected in line with data protection legislation.**

You are not requested to enter any personally identifiable information on the app. The 'app settings' give you the ability to delete the app and any information stored on the phone while using the app. The information collected is essential in allowing the App to meet its obligations for formal approval as a medical device and **Cє** accreditation; in line with requirements published by the Regulator, MHRA. The regulator, in line with stated policy for the period of the COVID-19 pandemic, has granted a 6 month approval of the app for use, until formal permanent accreditation is obtained. Appropriate interim assurance on reliability and effectiveness has been provided to the regulator. Your explicit consent is obtained during the on-boarding process in order to enable the release of the diagnosis keys and to enable decisions to be taken on an automated basis. Collection of the metric data is essential for the DoH meet its regulated obligations in relation to **Cє** accreditation, and to allow the DoH to support the essential public health function of contact tracing in delivering infection control measures in the context of the COVID-19 pandemic.

The phones of those who are using the app emit anonymised coded 'keys', 'Identifier Beacons', which change every 15 minutes. These 'keys' are stored on the user's phone for 14 days before being discarded. When close to each other, app users' phones exchange these anonymous 'keys', and if they are in close proximity with another user for a significant period of time (currently defined as 2 metres or less, and a duration of 15 minutes or more), both will store the anonymous 'key' of the other phone for 14 days.

'Authorisation Codes' are anonymous random six digit alphanumeric codes generated to verify that a positive test has been received by the app user, allowing 'exposure notifications' to be sent via the app, when the user enters a valid 'authorisation code.' On entering the code, the user is asked to release the anonymous keys their phone has transmitted over the previous 14 days: these are then known as 'diagnosis keys'. These are then released to the secure regist (see details below – HSCB AWS account), supporting users of the app, to be shared with other app users.

'Diagnosis keys' are anonymised identifiers generated on entry of an 'authorisation code' on the app, and stored in a secure registry, maintained in a Health & Social Care Board secure cloud services account (on behalf of the DoH) on Amazon Web Services (based in London). Every app user's phone regularly checks for 'diagnosis keys' and where these match a significant contact episode's anonymous 'key' stored on their phone, over the previous 14 days, an 'exposure notification' is enabled. The notification is generated on the app user's phone, not in the secure registry.

Where **'Exposure Notification' (ENS)** is mentioned, this refers to an anonymous notification received, via the app, that you have been in contact with an unnamed individual who has tested positive for COVID-19, and that contact was recent enough, and for sufficient time, at a close enough distance to mean that you may have been infected. **You will receive an instruction to self-isolate so that you can avoid passing the infection to others.**

The DoH is content to give a firm assurance that it has no intention to add to the functions of the 'StopCOVID NI' app, beyond those identified above.

Future updates of the app may occur to improve the performance of existing functions, or to implement improvements in the Google-Apple operating system that may occur to improve performance, within the scope of existing functions (outlined above). The DoH is considering the future development of versions of the app, to address accessibility in terms of languages other than English. This decision will be balanced against public health benefit and cost (balanced against other health priorities).

How the app works

Let's look at each feature in the app in detail.

How Contact Tracing works

Existing manual contact tracing processes rely on you being able to remember who you have been in contact with recently, and for how long. In many cases you may not even know those people (for example, if the contact happened on a bus or train, at a concert, a restaurant or some other public venue).

The app uses technology developed by Apple and Google where anonymous rolling identifiers are exchanged between mobile phones. A random and unique identifier is generated by you phone every 15 minutes (range – 10 to 20 minutes). If you are close to someone, who also uses the app on their phone, your identifier will be saved on that person's phone and you will record their identifier on your phone. All identifiers collected will remain on your mobile but you can't see them, nor can anyone else. These anonymous identifiers cannot identify you, to other users, or to the DoH.

If a person using the app subsequently receives a positive COVID-19 diagnosis, they will receive a text message containing an 'authorisation code' via SMS. The Business Services Organisation test registry generates a test notification to all those who have a registered mobile phone number on their records, or who have registered for testing via the website https://www.nhs.uk/ask-for-a-coronavirus-test. The Business Services Organisation does not know who is using the app, so notifications are sent to in relation to all positive tests, where mobile phone numbers have been registered to testing services or for receipt of medical services in NI. All those with a positive test will also receive a phone call from a clinical professional as part of the 'Test Trace and Protect' programme, administered by the Public Health Agency (PHA) under powers available through the 'Health and Social Care (Reform) Act (Northern Ireland) 2009'. On the call, they will be asked if they are using the 'StopCOVID NI' proximity app and if yes, if they have not already done so, if they wish to enter an 'authorisation code' to the app to enable the upload of 'diagnosis keys' from their phone. To do this, the PHA will send them a code by SMS, which when entered into the app unlocks an upload function. The person makes a choice to upload 'authorisation code' and release 'diagnosis keys' relating to the anonymised identifiers of significant contacts processed on their own phone, to a secure registry maintained in a Health & Social Care Board secure cloud services account (on behalf of the DoH) on Amazon Web Services based in London; where the 'diagnosis key' identifiers are published to be visible to other app users phones, enabling anonymous 'Exposure Notifications'. The SMS text message is delivered using the Gov.UK Notify service https://www.notifications.service.gov.uk/ .

Every two hours, the latest 'Diagnosis Keys' from the app Registry will be downloaded by every user's phone. These will be used to check for matches against the identifiers of the contacts that have been collected by your phone. If there is a match, you will be notified in the app that you were in close contact with a person who was diagnosed with COVID-19; this is called an 'Exposure Notification'. **You will be advised to self-isolate in order to avoid passing COVID-19 to others.**

For all this to work, you have to allow 'COVID-19 Exposure Notification Services' on your phone. You can also choose to allow your phone to display notifications so that you also receive an alert on your phone that you have been exposed to someone who has tested positive for COVID-19. You can turn off this functionality, if you change your mind, in the settings page of the app.

It is important to note that proximity measurement never reveals the identity of any person using the app to other app users, and never reveals who has been diagnosed positive. Also, the PHA and DoH will not know if you receive an 'exposure notification'.

Automated processing. The generation of exposure notices on the app is an automated process, not involving a human. The automated process is carried out by use of anonymous identification keys, and measurement of Bluetooth signals to calculate that app users' phones have been close enough for long enough to constitute a significant contact, sufficient to put you at risk of having been infected. It is necessary for the app to do this in an automated way, in order to protect your identity and the identity of other app users. In accepting terms and conditions you are consenting to this process. If you need to discuss this with an individual, you can call '**0300 200 7896**' Monday-Friday (excluding bank holidays) between the hours of 8:30am – 5:30 pm. **App users can express their point of view and contest the decision.**

What app metrics are collected

1. Collected regionally

The app will collect Metric data, which does not identify you, to create aggregate views of how the app is being used and the impact it is having on the control of the virus. Here is a list of the app metrics which, are collected from your app. The collection of these metrics is essential in order to prove efficacy and gain **Cє** accreditation:

- The total number of app users
- The total number of instances where 'diagnosis keys' have been uploaded
- The total number of 'exposure notifications' triggered

The DoH will not know any of these instances related to any individual app user, simply total numbers (for the region) of 'authorisation codes' and 'exposure notifications' in any given time period.

2. Generated by services on the phone

The following data is generated by Exposure Notification Services running on your phone if you turn it on.

- Identifiers sent and received between phones that have ENS turned on.
- Identifiers (diagnosis keys) uploaded to the Health & Social Care Board (HSCB) secure cloud services account (on behalf of the DoH) on Amazon Web Services (based in London) (AW

Registry if you are COVID-19 positive and you agree to upload them.

- Identifiers (diagnosis keys) downloaded from the AWS Registry to your phone for matching.

The above identifiers are random alpha numeric values that cannot be used to identify you or anyone else. These are generated, collected and matched on your phone if you enable ENS.

3. Automatically collected from your phone:

As a consequence of how traffic passes across the Internet, your internet protocol (IP) address is also inevitably transferred to our network servers. An IP address is typically made up of 4 sets of numbers (e.g. 1.2.3.4) and is assigned to you by your mobile phone or Wi-Fi service provider. Under the GDPR your IP address is regarded as your personal data.

While your data travels with the IP address it is considered personal data. The DoH does not use your IP address to identify you; furthermore the IP address is removed and deleted at the 'font door' of the HSCB AWS account, and the information becomes anonymous again and cannot be linked back to you. We do **not** store the IP addresses. However we do process IP addresses in line with data protection legislation to ensure that they are processed lawfully.

The legal basis for data processing

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 together form a framework for regulating the processing of personal data in the UK from 25th May 2018. In relation to 'Metrics' and 'IP address and app security tokens' the '**processing is necessary for the performance of a task carried out in the public interest**' as per GDPR Article 6(1)(e). The legal basis for the data processing is The Health and Social Care (Reform) Act (Northern Ireland) 2009,

- Section 2(1) the duty to promote in Northern Ireland an integrated system of health care designed to secure improvement in the physical and mental health of people in Northern Ireland and in the prevention, diagnosis and treatment of illness, and

- Section 2(3)(g) the duty to secure the commissioning and development of programmes and initiatives conducive to the improvement of the health and social well-being of people in Northern Ireland, and

- Section 3(1)(b) the power to provide, or secure provision of, such health and social care as it considers appropriate for the purpose of discharging its duty under section 2; and do anything which is calculated to facilitate, or is conducive or incidental to, the discharge of that duty.

In relation to Special Category data, Article 9(2)(i) applies to the processing, **'processing is necessary for reasons of public interest in the area of public health'**. Under DPA 2018, Schedule 1, Part 1 condition 3 is met in relation to Article 9 as follows:

Public health

3 .This condition is met if the processing—

- is necessary for reasons of public interest in the area of public health, and
- is carried out—

- by or under the responsibility of a health professional, or
- by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

The 'public interest' and 'public health' arguments apply equally to children in the 'post-primary' age group. They are as likely to become infected, and spread that infection to others. While the immediate effects on their health from COVID 19 infection are likely to be of a lower magnitude than those experienced by an adult, the longer term impact of disruption to education, and general societal economic downturn, are likely to have a significant and long-term adverse health impact for younger people. As such, younger people have a right to benefit from public health measures that might prevent such adverse outcomes and it is in their best interests to have access and use of the app for these purposes.

The app cannot function beyond the initial 6 month MHRA Exemption from device regulation during COVID-19 without attaining **C**є accreditation. The metrics data, collected at a regional level, are essential in demonstrating efficacy (which will be essential for attaining accreditation). The app cannot be used beyond the 6 month exemption without accreditation. A mobile smartphone **cannot** link via a network to transfer data without use of an IP address and app security tokens. This information is deleted at the earliest opportunity and not stored anywhere in the infrastructure.

'Diagnosis Keys' are released from the phone by the permission of the data subject. They are essential for letting others know that they are at risk of having been infected via the 'exposure notification' process. A person using the app may receive 'exposure notifications' by using the app, utilising the published 'diagnosis keys' of others. They may however decline to enter an 'authorisation code' on receipt of a positive test result, or may decline to release their 'diagnosis keys' for publication. While it is not anticipated that anyone would wish to use the app in such a manner, it is technically the position that release of 'diagnosis keys' is not essential for an app user to consent to this publication process, in order for them to benefit from notification by others. Technically it is arguable that at the point where 'diagnosis keys' exit a user's phone, they are associated with an IP address and app security tokens, and as such are personally identifiable. Though IP addresses vary, and are not static, some more recent rulings have deemed them 'personally identifiable'. Once the IP address and app security tokens have been deleted on entry to the networking layer, the 'diagnosis keys' are non-identifiable. Once stored in the app registry, the 'diagnosis keys' are clearly non-identifiable, and can be published without risk of re-identification. The app is voluntary to use, as is this feature of the app and the legal basis for the processing of the 'diagnosis keys' is 'consent', namely GDPR 6(1) (a), and GDPR 9(2) (a), 'explicit consent', in relation to the processing of special category data. Consent is sought for release of the 'diagnosis keys' on the app at the point of release.

In circumstances where an Information Society Service (ISS) is offered directly to children an the data controller is relying on consent, Article 8 of the GDPR (and Chapter 2, section 9 of t

DPA 2018) provides that:

- only children aged 13 years and over may lawfully provide their own consent for the processing of their personal data;
- an adult with parental responsibility must provide consent for processing if the child is under 13; and
- in such cases, the controller must make reasonable efforts, taking into consideration available technology, to verify that the person providing parental consent does, in fact, hold parental responsibility for the child.

Furthermore, if the ISS is an online preventive or counselling service, section 9 provides that the Article 8 requirements do not apply and Recital 38 of the GDPR says that parental consent should not be necessary in the context of preventive or counselling services offered directly to a child. This indicates that in this context it will be in the best interests of the child to consent for themselves. **The Department deems the app a preventative service because the app has a single purpose, namely to deliver an exposure notification service, aimed at informing app users at the earliest opportunity, that they have potentially been infected, and that they should self-isolate (getting a test if they develop COVID symptoms). This prevents those who have been infected (and not yet developed symptoms) from passing the infection on to others.** Therefore the children using the App can provide their own consent for the release of the diagnosis keys. However for children in the11-12yo age group, the app advises the app user to seek support from a parent / guardian to upload diagnosis keys. The Department believes it is unlikely that children under the age of 13yo would be able to progress this stage of the app without parental input, given that it would not be possible for someone in this age group to book a test, without such support from a parent / guardian. Without a test and test results the child would never be using this feature of the app.

Security measures

All data stored on your phone is encrypted by the app using the built-in encryption capability of your phone. Data is also encrypted when it is being uploaded to our servers. The app does not store or transmit identifiable information. The app **does not access** GPS functionality on the phone, or access any form of location data from the operating system.

The proximity measurement feature uses a **fully decentralised** privacy model which means that the matching of identifiers and diagnosis keys happens on your phone and is not externally performed by the DoH. This ensures neither tracking of peoples' movements, nor knowledge of with whom, or when, app users have been in contact with each other.

There is a range of security processes and technologies in place to prevent unauthorised access to the data while it is stored on our servers, including data encryption, modern firewalls and intrusion prevention.

When 'Diagnosis Keys' are uploaded to AWS servers with your IP address, the IP address is stripped from the information at the earliest possible opportunity which renders the information anonymous.

Who processes your data

The DoH has overall responsibility for the app and has directed the Health and Social Care Board (HSCB) and Public Health Agency (PHA) to deliver services in relation to the app, as Data Processors on behalf of DoH. Therefore there are a number of data processors and sub-processors involved in the delivery of the app, who may process data in relation to the app.

Data processors

The following provides a list of data processors and sub processors involved in delivery of the app.

- NearForm are the app developers who will be providing technical support on the running of the app. Their services are delivered via HSCB GDPR compliant contracts.
- Big Motive Ltd are the design team who have worked with NearForm to design the user experience and content for the app.
- Gov.UK Notify provide the service to enable the sending of an SMS to your phone which contains the 'Authorisation Code' needed to enable your phone to release 'Diagnosis Keys'. Their services are delivered via HSCB GDPR compliant contracts.
- Amazon Web Services provide cloud storage and cloud services for the data uploaded from your phone. Their services are delivered via HSCB GDPR compliant contracts.
- The BSO provide certain services as a data processor on behalf of HSCB and PHA. The BSO host the Covid test registry for lab results. They operate the test registry, gathering the results of testing, positive test results to be notified via SMS text message, and be made available to PHA staff delivering manual contact tracing services, as well as associating results with electronic patient records to ensure appropriate access by clinical professionals supporting clinical care service delivery. They also provide backup support to the SMS function through arrangements with the HSCB. Their services are managed via appropriate agreements with PHA and HSCB.

Contracts and MoUs are in place to govern relationships with the above data processors and sub-processors which set out the obligations of each party and the data controller's obligations and rights with regard to the data that is being processed. All data processing takes place within the EEA area, and as such is subject to legislation in the form of the General Data Protection Regulation (GDPR).

Other recipients

The regional level data (outlined above) is extremely limited in scope. The DoH will make freely available the high level anonymised data, in order for members of the public to see the level of uptake, and the potential of the app to reduce the rate of spread of infection of COVID-19.

Anonymised diagnosis keys are shared with DoH IRL, via a federated server in ROI, in order to enable interoperability of the app cross border, to support users undertaking cross border travel. There is a MoU in place between DoH NI and DoH IRL in relation to this. It is intended that similar arrangements will be put in place with other regions across the UK to support NI citizens travelling across UK borders. This privacy notice will be updated to reflect any further developments.

Data transferred outside the European Economic Area

No data will be transferred outside the EEA. All data processing will be subject to GDPR regulations and obligations.

How long your personal data is held for

No personal data is collected or stored, but we have outlined below how long certain data connected to the app are retained for.

Your IP Address:

Following upload of your IP address to AWS servers, it is deleted once the server network layer has routed the traffic to the application layer. User IP addresses are never transferred to the application layer.

‘Identifier beacons’ on your device:

This anonymous information is retained for 14 days.

Diagnosis keys in AWS registry (HSCB account set up on behalf of the DoH):

This anonymous information is retained for 14 days.

Diagnosis keys on your device:

This anonymous information is retained for as long as is necessary to perform a match check and is deleted thereafter.

Gov.UK Notify SMS Service

All SMS texts and phone numbers, processed on the server, are deleted once a SMS text message has been successfully transmitted. This 'server' is physically / electronically separated from the servers supporting the backend of the app. Different service teams will be employed to ensure that identifiable information (mobile phone numbers and test results) are kept separate from the app operational servers, preventing any individuals information being discoverable with the app.
The flow of data from the BSO test registry through the app backend to the Gov.UK Notify (SMS Platform) to send an SMS text will be managed by different groups to help reduce any risk of re identification.

• The BSO registry contains the mobile numbers of people who have tested positive.

• As the Temporary Exposure Key uploads hit the app backend in Amazon Web Services, it is important this backend data cannot be combined with mobile numbers.

• To help prevent this, the Amazon Web Services backend will never store or log the mobile number.

• The mobile number will exist in the BSO test registry and will exist in Gov.UK Notify as SMS messages are sent. (Being deleted after this action has been fulfilled).

To facilitate reconciliation for issues that may occur within the Amazon Web Services backend, a Job ID will be used to track the flow from BSO registry through Amazon Web Services. When BSO calls the Amazon Web Services REST API it will pass on a Job ID that will be used to uniquely identify the transaction with the Amazon Web Services flow.

This Job ID will be logged within Amazon Web Services so that in the case of any failure during processing, the record in the BSO registry that was not successfully processed can be identified.

In the case of a failure during the Amazon Web Services flow, an alert will be raised within Amazon Web Services and notified to the NearForm support team. The NearForm team will investigate alerts raised and will either address or correct, if the issue is within Amazon Web Services.

If the issue is outside of Amazon Web Services, when appropriate, NearForm will escalate the issue to the BSO support team.

BSO will be required to reconcile the Job ID from registry data to the SMS text records on the Gov.UK Notify platform.

The PHA manual Contact Tracing service will also be telephoning all positive test users, so can be scripted to verify that the recipient has received a SMS; the call handler will also have the capability of sending an SMS from the Manual Contact Tracing system.

DoH / HSCB / PHA- Regional Summary Level Information

The DoH / HSCB / PHA will retain regional summary level information, relating to the number of app users / ratio of exposure notifications to positive cases indefinitely, to support evaluation of the app's effectiveness in pursuance of **C**ϵ accreditation. This process will be conducted in line with requirements outlined by the MHRA, the regulator.

This regional level data will be retained for purposes of research and future pandemic response planning. This does not involve individual level data. Though interim approval has been granted, in order to obtain formal MHRA Regulatory approval, and CE certification, will involve collation of data in evidence of the efficacy of the app. In line with GMGR Disposal Schedule J – Clinical Trials of Investigational Medicinal Products (CTIMPs) – this high level summary data will be retained '*for an appropriate period, to allow further analysis by the original or other research teams subject to consent, and to support monitoring by regulatory and other authorities*'. https://www.health-ni.gov.uk/articles/disposal-schedule-section-j

On occasion of the pandemic being declared as having ended, the app will be stood down. Users will be instructed to delete it from their phone. Any anonymised data present, at that time, in the AWS servers (on behalf of the DoH to support the app function) will be deleted.

Data Subject rights

Users have rights under GDPR when their personal data are processed. The following considerations should be noted. IP addresses are not retained on the app backend, but for transient network routing and network security purposes. Diagnosis keys are not capable of being associated with a person as they are non-identifying by design.

- **Right to information** – a Data Protection Privacy Notice (Notice) is provided via the app itself on those pages which request information and also in the app Settings. The Privac

Notice will also be published on the DoH website. The Notice contains information as prescribed under Article 13 and 14 of the GDPR.

- **Right to rectification –** since no personal data is collected or retained by DoH, it would not be possible for DoH to comply with a request for rectification.

- **Right of access –** since no personal data is collected or retained by DoH, it would not be possible for DoH to comply with a request for access.

- **Right to erasure –** the user can select the Leave function, delete the app at any time, and delete ENS data via device settings – erasing all data processed on the phone. Since no personal data is collected or retained by DoH it would not be possible for DoH to comply with a request for erasure.

- **Right to restriction –** the user can revoke their ENS permission, revoke their exposure notification permission and decide not to upload keys. Ultimately the user can decide to Leave and/or delete the app from their device. Since no personal data is collected or retained by DoH it would not be possible for DoH to comply with a request for restriction.

- **Right to portability –** it is not possible for users to port their keys, for example, from one device to another device as the user does not have access to such keys on their device (save to delete them) and as regards those uploaded to the DoH, the DoH cannot identify which keys belong to which user. Since no personal data is collected or retained by DoH it would not be possible for DoH to comply with a request for portability.

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

- **Right not to be subject to solely automated decision-making including profiling –** if the ENS detects a match between a Rolling Proximity Identifier on the app and a Diagnosis Key downloaded from DoH Diagnosis Key Registry, a decision is made that a close contact has taken place. This decision is based solely on the automated processing of identifiers and keys and does significantly affect users. However, this processing is based on the explicit informed consent of the user, during the on-boarding process. The automated decision-making is an essential feature of the proximity app solution provided, and is core to its function in delivering the public health objective of infection control. If app users wish to speak to someone in relation to an 'Exposure Notification' that they have received via the app, they can call '**0300 200 7896**' and select the option to speak to someone about the notification at the following times: Monday-Friday (excluding bank holidays) between the hours of 8:30am – 5:30 pm. Someone will answer the call and explain the 'Exposure

Notification'. They will have no way of knowing with whom, where or when a 'high risk' contact took place, but they will try to explain the process to app users and its purpose. **App users can express their point of view and contest the decision.** These steps should enable the app user to make an informed decision as to whether to self-isolate to prevent spreading the infection to others. Ultimately if they are still not satisfied or need clinical advice they will be advised to seek clinical assessment by their GP or GP OOH.

Changes to this Data Protection Information Notice

This Data Protection Information Notice may change. You should check it each time the app is updated.

How to complain if you are not happy with how we process your personal information

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

If you are still not happy, you have the right to lodge a complaint with the Information Commissioner's Office (ICO):

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113

Email: casework@ico.org.uk

Website: Information Commissioner's Office

Updated:
7 mins ago

Posted:
July 28, 2020 8:50 am

Legal

Privacy Notice
Cookies
Disclaimer

Mobile Apps

COVIDCare NI
StopCOVID NI

Select Language

Powered by Google **Translate**