CASTLEBRIDGE

Changing how people think about information

Research Report

Contact Tracing Applications: Data Protection Issues, Risks, and Recommendations

Version Control

Version	Date	Changed By	Comment
1.0	2020/03/30	Daragh O Brien Katherine O'Keefe PhD Peter Davey	Consolidation of research into final report format.

Contents

Acknowledgements

Castlebridge acknowledges the generous inputs from Pat Walshe, former Global Director of Privacy Policy at the GSMA[1], into the shaping of this research report. His in-depth knowledge of this area has been an invaluable guide.

We are also grateful to Phil Booth of MedConfidential in the UK for his time in discussing some of the topics raised in this document.

Thanks go also to Sean McDonald and the Centre for Internet and Society in India for the analysis conducted of the use of mobile phone location data in epidemic responses.

Colin Boylan in Fresh Perspectives Market Research is also thanked for his input based on his experience in clinical market research study design.

We would also like to thank our Singaporean contacts for their input also.

[1] GSM Association (www.gmsa.com)

Executive Summary

Castlebridge have prepared this research report for the purposes of supporting Data Protection Impact Assessment activity in respect of contact tracing apps and associated mobile device-based interventions in public health response to pandemic scenarios or other infectious disease outbreak scenarios.

Outline of Methodology

Castlebridge applied a variant of our Data Protection Impact Assessment/Ethical Impact Assessment methodologies to the analysis of a set of defined use cases derived from media discussion of various uses for smartphone/mobile phone data to support covid-19 response initiatives.

In doing so, we have drawn on our international network of experts in data protection, telecommunications, and clinical data study design, as well as individuals with personal experience of some of the applications discussed, to develop the best possible analysis.

The business needs/use cases we identified for analysis in this report are set out below.

Business Need	Summary Approach
Identification of Close Contacts and support for contact tracing	Use mobile phone data (location or other) to identify close contacts and support contact tracing.
Provide symptom tracking and recording to support epidemiological data capture/analysis	Provide a smartphone app where users can log symptoms they are experiencing.
Notify individuals if they have had close contact with someone who has tested positive	Send push notification from smartphone app to notify the person who has been in close contact
To track population movements to support analysis/prediction of disease trends and effectiveness of containment	Use mobile phone data to identify movements people
Provide information to app users	Use push notification to give targeted information to app users

Summary of Conclusions and Recommendations

Our conclusions and recommendations are summarised below.

Contact Tracing

We conducted an analysis of the data protection impacts and implications of the TraceTogether application from Singapore, as a reference model for contact tracing applications using Bluetooth signals as an alternative to location data.

We have identified a number of potential improvements that are required to the application as implemented in Singapore to improve protections for data subjects.

Overall, we found the approach taken in Singapore to be broadly privacy respectful and in line with the requirements of data protection law.

We note the extensive communication campaign that the Singapore authorities have entered into to inform data subjects about the app, its functionality, and how the data will be used and retained.

Symptom Tracking

Symptom tracking apps provide a potentially rich source of epidemiological data relating to the progression of the illness. They may also provide data to help differentiate the symptoms of other commonly occurring illnesses from those of Covid-19.

There are potential issues of data quality in the context of self-reported symptoms and also consistency of completion of self-reporting which could impact the effectiveness of logged data.

We recommend that they be deployed as a "second wave" application in the context of contact tracing to support the management of close proximity contacts of infected persons. This will help reduce the "noise" in the data that is gathered and will enable causation and correlation factors to be more readily identified.

We also make a number of recommendations regarding the security of data in such applications.

Push Notification of Close Contact

It is questionable if the push notification of a close proximity contact to a person who has tested positive is **necessary** to protection the vital interest of the data subject or another or if it is **necessary** to pursue the public health objective.

It is also possible that push notifications could cause unnecessary distress to data subjects and, absent appropriate context in communication, could trigger unexpected and undesirable consequences for third parties.

In particular, the risk of sending a push notification to a child, or to a vulnerable person, cannot be ignored.

Push notifications should be a supplement to and not a replacement for existing contact tracing and follow up protocols. It is essential that the "human touch" is not lost.

Furthermore, consideration should be given to the "next action" that would be taken by persons in receipt of a push notification. Any action that results in a substantial increase in calls to local primary care facilities should be avoided. Likewise, if the call to action is to contact a central number, this must be adequately resourced to ensure callers are answered in a timely manner and ideally on their first attempt.

Analysis of Population Movement using Mobile Data

Analysis of population movement using mobile data represents a significant risk of mass surveillance and would require either processing on the basis of consent or the processing of anonymised data.

A range of very clear safeguards would be required to balance data protection and data privacy obligations against the objectives of processing this data.

It is important to note that the data is of insufficient granularity to support contact tracing but would, in an aggregate form, potentially support measurement of effectiveness of social controls on movement.

Push Notifications to App Users

Push notifications of a general nature to app users have a lawful basis either on the basis of consent or on the basis of processing in the public interest.

We would question the need for these to be implemented as part of an application or application framework and would recommend instead that an SMS subscription service where people can subscribe for updates by county would be sufficient to meet the need of general communication.

Application Strategy

We recommend against the development of a single application to perform both contact tracing and symptom tracking functions and recommend instead a dual-application strategy to roll out symptom tracking to close contacts of persons who have tested positive to reduce scope for non-relevant data logging.

Introduction

The information processing capabilities of mobile devices have increased significantly in recent years since the introduction of the App Store by Apple a decade ago. Today, app-based data capture can represent an efficient mechanism for engaging with citizens on a variety of topics.

Coupled with this, the near ubiquitous penetration of mobile phones in the Irish market means that mobile devices represent a potentially valuable source of data in the context of contact tracing and other public health functions. As mobile phones allow for a two-way flow of information between the data subject and the public health authority, they can also support the delivery of validated and authoritative information to individuals through official channels.

However, more data is not necessarily more useful information. It is important that any increased information gathering or information sharing capability is focussed on informing right actions to prevent illness and support recovery

In the context of the Covid-19 pandemic, there has been significant focus on the TraceTogether initiative in Singapore, as well as a variety of calls to use mobile phone network data to perform contact tracing and other functions. This research paper will examine the data protection and privacy implications of this approach.

Purpose of this Research Report

The purpose of this research report is to consider the potential use cases for mobile phone related data in the context of contact tracing to help inform data protection impact assessments, the definition of requirements and the implementation of functionality in smartphone applications to support public health responses to pandemic in a manner that will support:

1) The timely collection of quality information to support contact tracing.
2) The effective communication with affected persons of relevant information in a timely manner
3) The establishment and maintenance of trust between the individual and the public health authority to ensure that there is a timely sharing of information to support decisions and inform actions to prevent illness and support recovery

To this end we have applied the Castlebridge Ethical Information Assessment Model to a series of defined “use cases” which may arise in the context of the use of different approaches to mobile device data, or data derived from mobile devices, to support public health responses. We also consider wider implications and considerations in respect of the safety and security of data subjects, and the

protection of their wider fundamental rights and freedoms to ensure appropriate balance is struck.

The report has been developed using a variant of Castlebridge's proprietary data protection impact assessment methodology. A summary of the methodology is set out in the next section of this report. In the interests of conciseness in this document, further details of the methodology can be obtained from Castlebridge on request.

Identified Business Needs and Approaches

A "Use Case" reflects "the requirements of business processes, and business processes are supported by information systems and automated business processes" (Finneran-Dennedy, Dennedy, & Fox, 2014). In the Castlebridge methodology, we term a high level use case a "Statement of Business Need and Approach".

A structured "problem statement" template[2] is defined for each use case which captures, as completely as possible, a statement of the proposed processing, the purposes for the processing, and the identified benefits to data subjects and to the organisation proposing the processing activity.

The identified use cases for review in this report are set out in the table below:

Business Need	Summary Approach
Identification of Close Contacts and support for contact tracing	Use mobile phone data (location or other) to identify close contacts and support contact tracing.
Provide symptom tracking and recording to support epidemiological data capture/analysis	Provide a smartphone app where users can log symptoms they are experiencing.
Notify individuals if they have had close contact with someone who has tested positive	Send push notification from smartphone app to notify the person who has been in close contact
To track population movements to support analysis/prediction of disease trends and effectiveness of containment	Use mobile phone data to identify movements people
Provide information to app users	Use push notification to give targeted information to app users

[2] This template is based on the framework set out in Chapter 4 of (Finneran-Dennedy, Dennedy, & Fox, 2014) and Chapter 10 of (O'Keefe & O Brien, 2018)

Analysis of Needs and Approaches

We conducted a review of the business needs and proposed approaches described above. For each use case we followed the standard DPIA/Ethical Impact Assessment approach used with Castlebridge clients.

Business Need #1: Contact Tracing

This section examines the use of mobile location data and/or other mobile phone technologies to support the tracing of close contacts. For the purposes of this research paper we have identified the "TraceTogether" application from Singapore as a reference model to conduct our analysis against.

The high-level requirement is to use data derived from smartphones to log close contacts to enable public health officials to more quickly and accurately perform contact tracing of persons who may have been exposed to virus through close contact.

Statement of Business Need and Approach

Proposed Processing Activity (What we propose to do)	To process information about the proximity of smartphone users to other individuals using data derived from smartphone to support contact tracing
For the Purpose of	So that close contacts of individuals who have tested positive for Covid19 can be identified quickly and accurately for the purpose of testing and isolation
To achieve benefit (to the organisation)	• To improve speed and accuracy of contact tracing • To reduce potential span of population which may be infected through follow-on contact infection • To allow for more timely testing of potentially infected people
To achieve benefit (to the data subject)	To protect the vital interests of the data subject or others through more efficient use of public health resources

Approach

The key functional requirement identified here is the collection of information relating to close contact between individuals to identify and alert who may have been exposed to COVID-19. As such, the key to quality data required to fulfil the goal is the ability to identify and trace proximity and duration of contact between individual regardless of their geographical location, and to communicate with individuals who have had close contact with people who have tested positive for COVID-19 for to support texting and isolation. The approach for such an app installed on a user's smartphone is:

1) Registering that user's mobile number with a central registration database and generating a unique pseudonymous code for the user's app
2) Using Bluetooth to identify other devices in the user's vicinity with the app installed
3) Calculating a distance between the users, and the duration of the contact
4) Logging all contacts within a defined radius and a defined duration locally on the user's device
5) Requesting data using a secure pin to export data to Public Health Officials where a data subject has tested positive for a defined infectious disease.

Data would be held "on-device" until such time as it is requested by Public Health authorities to assist in contact tracing. A validation key will be provided by public health officials when requesting access to data held on a data subject's device.

This approach differs from other strategies for the use of smartphones for contact tracing as:

1) It does not require the processing of location data from within a public communications network
2) It does not require access *en masse* to retained telecommunications call record data
3) It is not affected by variations in mobile phone cell coverage radius (which can differ between urban and rural locations)
4) It minimises the data that is processed by Public Health officials to determine relevant contacts for tracing

This approach does not envisage any push notification to users that might identify other positive cases in their area and it does not envisage the publication of any data relating to diagnoses through the application.

Analysis of Information Environment

In this section of the Data Protection Impact Assessment we consider the analysis of the Information Environment from a number of key perspectives.

Categories of Data Subject in Scope

The categories of data subject in scope for the proposed processing are:

1) Smartphone app users
2) People who are in close proximity to smartphone app users

Categories of Personal Data in Scope

The categories of personal data that are in scope within the application are:

- Mobile phone number

- Proximity to other devices (based on Bluetooth relative signal strength)
- Pseudonymised identifier for app users
- Linkage data for mobile phone to pseudonymised identifier.

Legal Environment / Lawful Basis

The relevant legislation for consideration here is:

- Data Protection Act 2018
- ePrivacy Directives / SI 336 of 2011
- Health Acts 1947 – 1953 (as amended)
- Communications (Retention of Data) Act 2011

ePrivacy Directive / SI336

Regulation 9(1) of SI336 introduces a prohibition on the processing of location data other than traffic data relating to users or subscribers to a public telecommunications service other than with consent or where the data has been made anonymous.

In this context, data will not be anonymous as it will be possible to reidentify the individual by linking the app user ID back to the registered phone number for the app user in the backend database once data is uploaded from the device.

The data will be pseudonymous.

Therefore, the legal analysis must consider on what basis consent will be obtained, the implications of relying on consent, and also whether consent is a required condition for processing. in this context.

Application of SI336

Regulation 2 of SI336/2011 defines "location data" as:

"*any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service*"

The proposed processing approach does not require the accessing of data held by telecommunications providers that would record the location of a subscriber to a public communications service. Furthermore, the operation of the proposed processing does not actually require the recording of geographic location or any data relating to location but instead is processing signal strength as a proxy metric for distance between two devices.

In this context, the application is not processing location data within the meaning of SI336 or the ePrivacy Directives and therefore no consideration arises at this time in respect of the restrictions in that legislation with regard to the necessity for consent or anonymisation of data.

Communications (Retention of Data) Act 2011

As this app does not require the accessing of retained telecommunications data from the operators of telecommunications services, the restrictions on access and processing of bulk communications data set out in this legislation and the associated CJEU case law (*Digital Rights Ireland*, *Watson/Tele2*, etc.) does not apply in this context.

Health Acts 1947 – 1953 (as amended)

The Health Acts and their associated statutory instruments in respect of public health and infectious diseases establish a range of powers for Public Health officials and a range of obligations and duties for individuals.

S.I. No. 390/1981 - Infectious Diseases Regulations 1981

Regulation 11 of this SI creates a broad power and obligation to perform contact tracing and other investigations relating to the occurrence of an infectious disease.

"*On becoming aware, whether from a notification or intimation under these Regulations or otherwise, of a case or a suspected case of an infectious disease or of a probable source of infection with such disease, a medical officer of health, or a health officer on the advice of a medical officer of health, shall make such enquiries and take such steps as are necessary or desirable for investigating the nature and source of such infection, for preventing the spread of such infection and for removing conditions favourable to such infection*."[3]

In the context of a contact tracer requesting that a user of the application provide the stored data to the health authority for the purposes of reidentification and contact, there is a positive obligation on individuals to comply with this request and consent is not the appropriate basis for processing of data in this regard. The relevant statutory basis can be found in Regulation 11 when read in conjunction with Regulation 19 of SI390/1981 and Section 31(8) of the Health Act 1947.

Data Protection Act 2018 and Regulation 2016/679/EU (GDPR)

The Data Protection Act 2018 and Regulation 2016/679/EU apply to the processing of this data as data relating directly or indirectly to living individuals is being processed.

For the purposes of this analysis and the identification of applicable lawful processing conditions, we will break the application processing into three distinct phases:

---

3 http://www.irishstatutebook.ie/eli/1981/si/390/made/en/print?q=infectious+diseases+regulations&years=1981

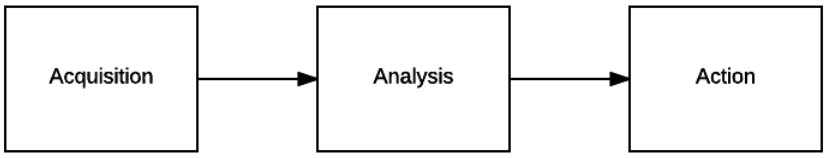


Figure 1: Generic Data Analytics life cycle - source: "Ethical Data & Information Management", O'Keefe & O Brien, Kogan Page 2018

Acquisition

This processing activity acquires data from an application that is downloaded and installed on a user's smartphone. The application interacts with the standard app permissions in the mobile device operating system.

The registration process for the application requires a mobile number and the associated app user identifier to be registered in a central database. The validity of the entered phone number is verified through the use of a one-time PIN code that is sent by SMS before data is processed to the central register.

Article 5(1)(d) Accuracy Principle control: Accuracy of phone number is verified before processing commences.

The application seeks consent for the processing of personal data, with two distinct purposes identified:

1) Recording of mobile number in a central register
2) The transfer of data from user devices to the health authority from users who are confirmed or suspected of being infected with the relevant infectious disease.

The requirement for consent in the original application would appear to derive from Section 13 of the Singapore Personal Data Protection Act 2012[4], which implements a narrower set of lawful processing conditions for personal data than Regulation 2016/679/EU.

Other potentially applicable grounds for processing data in this context are set out in the table below:

Applicable Article 6 basis	Rationale
Article 6(1)(d)	The purpose of contact tracing is to protect the vital interests of other parties who a data subject has come into contact with. While interview based contact tracing is possible (and is the traditional approach), the infection rate of Covid19 would suggest a faster and more

[4] https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P1IV-#pr13-

	accurate mechanism for logging of potential contacts is necessary to ensure an effective public health response.
Article 6(1)(e)	Contact tracing is a function which is carried out in the public interest and in pursuance of an official authority. The question of necessity arises in terms of the accuracy and timeliness of data that would be available for contact tracing purposes.

Consent is therefore not the only basis that may be relied on for the processing of this data and, as such, Article 8 of Regulation 2016/679/EU is not applicable.

The formulation of consent for the acquisition of data

The application has a single defined purpose. The downloading of the application is a voluntary act and the provision of data to the application is likewise voluntary.

The data that is being processed is specific (and communications of the processing purposes must be explicit and clear about the data that is being processed and why). The purposes of the processing are likewise specific and explicit.

Therefore, consent can be construed from the downloading of the application and the acknowledgement of the processing purposes and activities that are proposed. It is not necessary for an explicit consent to be obtained.

However, as the Controller is a public body, consent cannot be relied upon as the sole basis for processing.

Consent and Device OS permissions

To function, the application requires access to Bluetooth data on the smartphone device.

These permissions are controlled via the device operating system and are a toggled opt-in / opt-out permission. As such, for data to be logged, users have to provide device level consent to the application to access and process the relevant sensor data.

As location data is not needed, consent is not required for the processing of location data. However, Android operating systems on mobile link Bluetooth functionality to location data processing given the historic use of the technologies in tandem for user tracking for marketing analytics purposes. The location functionality in Android OS is not used by this application.

Does data at point of acquisition constitute "Special Category Data" under Art.9

No. The data that is being processed through the application does not constitute special category data as it reveals no information relating to health until such time as the data subject has had a positive test outcome and their data is require to notify other parties or until such time as a close contact has tested positive and the data subject needs to be contacted.

Therefore, at the point of acquisition, the data does not fall within the scope of Article 9.

Data Minimisation, Data Retention and On-Device Processing

A key feature of the application as described is that the logging of contacts is performed on-device using pseudonymous identifiers based on the duration of and proximity of contact.

As such, only the data necessary to identify a potential close contact is recorded. It is recorded on-device and is not accessible to users or any other party without the provision of a valid access code which permits the uploading of the data to the health authority database for analysis and action.

It is unclear from documentation if only data of users who have been both within a defined range and for a specific time period is recorded or if both data points are logged independently, however the potential risk of over-collection here is mitigated by the 21 day retention period that is applied to on-device data. Furthermore, the risk of overcollection is also mitigated by the potential benefit of counteracting any errors in logging of either variable over time.

Analysis

The analysis phase of the information processing life cycle applies to the use of the data for contact tracing. In this context there are two categories of data subject whose rights under DPA2018 and GDPR need to be considered:

- The application user who has tested positive for the infectious disease
- The application users who have been in close contact for a defined period of time.

In this context the personal data does fall within Article 9 of GDPR as it constitutes data relating to health of one or more data subjects. Furthermore, the argument for the necessity of contact tracing processing is more robust where a positive diagnosis or potential diagnosis exists.

Applicable Article 9 basis	Rationale
Article 9(2)(c)	The purpose of contact tracing is to protect the vital interests of other parties who a data subject has come into contact with. While interview based contact

	tracing is possible (and is the traditional approach), the infection rate of Covid19 would suggest a faster and more accurate mechanism for identifying of potential contacts is necessary to ensure an effective public health response.
Article 9(2) (g)	Contact tracing is a function which is carried out in the substantial public interest and based on Member State law. The question of necessity arises in terms of the accuracy and timeliness of data that would be available for contact tracing purposes.
Article 9(2)(i)	Contact tracing is necessary for reasons of public health and has a basis in Member State law.

Within the design of the application and its data processing controls, access to the data recorded on the device for the purposes of analysis to re-associate the pseudonymised identifiers with the identifiable phone numbers can only be executed once there is a verified basis related to a positive test result or diagnosis with the infectious disease.

Action

The "action" phase of this life cycle refers to the use of identified phone numbers that are linked to application users who have been within a defined contact radius of an infected person for more than a defined period of time based on the output of the analysis phase described above.

The action to be taken is the standard contact tracing communication and follow up action through a phone call to the data subject to advise them of their close contact with an infected person. This is an existing process and is not in the scope for this engagement. The lawful basis for this contact action is the Health Acts, and in particular Regulation 11 of SI390/1981.

Conclusion

There is a sound legal basis for this processing under the Health Acts and under the Data Protection Act 2018 and Regulation 2016/679/EU.

The provisions of SI336/2011 and the Communications (Retention of Data) Act 2011 do not apply in the context of the proposed processing mechanisms.

While the powers in the Health Acts and the associated Statutory Instruments are broad (reflecting to a degree the antiquity of the primary legislation in this area), they do establish a legal basis for processing. The application processes a minimal amount of information and does so primarily "on device" until such time as the data is specifically required for a public health purpose.

Information/Process Environment

The application information environment and process environments are relatively straightforward.

Process Environment Assessment

Users download the application and provide a phone number to the health authority. By keeping the application running the application broadcasts its identifier to other smartphones with Bluetooth enabled. When you are in range of another application user, the application logs an approximate proximity and duration of contact with that pseudonymous user. This data is held locally on the device.

When a user has a positive test for the infectious disease, the public health authority can provide a validation code that releases the pseudonymised data to the health authority who can then reidentify the other users who have been in close contact and perform follow up contact tracing.

Information Environment

Hosting and Data Transfer

The application operates as a "serverless" application building on the Firebase SDK, with data uploads handled through Firebase Storage. The application utilises the Google Firebase application development environment.

Data Storage

Data is hosted in an SQLite database. Proximity contact log data is stored on-device. The data stored includes:

- User ID
- Timestamp
- Model of users phone (hashed)
- Temporary User ID of the other device/app user (encrypted temporary ID, private key held by health authority)
- RSSI (used to measure proximity of a Bluetooth beacon)
- Measured power of Bluetooth beacon (other device) – used to make distance estimates.

Proximity and duration of contact data is derived from Bluetooth sensor data. This is logged locally on the user's device in the device local storage. Data is retained for a 21 day period. Note that code reviews have not identified the mechanism for enforcement of this retention period, however there is a timestamp record for each logged interaction so this functionality can be implemented relatively easily.

Data Encryption

Data is encrypted on device. User IDs exchanged between apps are also encrypted.

Identifiable User data.

Users register their phone number along with their device identifier in a central registry. No further data is processed centrally until there is a specific need for a contact tracing purpose.

Data is transferred to contact tracers securely and uploaded to the registry database to allow for reidentification of users for tracing purposes.

It is unclear from the provided documentation if data is transferred outside EU/EEA to Singapore or if the application would be installed locally in an EU-based data centre. The use of Google Cloud as the back-end environment for this application indicates that it would be prudent and possible to select an EU-based Google cloud region.

Controls and Governance Environment

There are two distinct aspects of the controls and governance environment to be considered with respect to this application.

1) Controls and governance of data "on-device"
2) Control and governance of access to data for analysis

On-device controls

There are a variety of data protection related controls in operation on-device/

- **Accuracy:** As noted earlier, the use of a One-time-Password sent by SMS ensures the accuracy of the mobile phone number entered to be associated with the application
- **Pseudonymised data:** no identifiable data is transferred. Only pseudonymous application user identifiers are shared and logged.
- **Encryption:** the application stores log data on-device in an encrypted format
- **Device OS controls:** The application must operate in line with device OS controls framework
- **Data Retention:** While it is stated that the data is retained on device for 21 days, it is not clear that that has actually been implemented in the currently available version of the code.

Access to Identifiable Data

The proposed method of implementation restricts the access to identifiable information. Data is held on the device in a pseudonymised form. Data can only be

accessed by transfer from device to a server once an authorisation code has been input. This is only available to public health contact tracing staff.

Once contact data is reidentified to a mobile phone number, the standard data protection and governance controls in the HSE public health departments will apply and are outside the scope of this RESEARCH PAPER.

Assessment of Data Protection Risks

In this section we address the risks to data protection rights and the potential risks to other fundamental rights and freedoms arising from the proposed processing activities. This section also considers the root causes of those risk factors as a precursor to the definition of remedial or mitigating actions to address those risks.

Assessment of Risks

On the following page we present the assessment of risks with a risk rating based on their *unmitigated* level of risk taking into account the currently proposed and currently existing controls and mitigations. Please note that the maximum score possible for a Weighted Risk Priority calculation is 500. The full analysis of the Probability and Impact of risks is set out in Appendix 2.

For the purposes of this RESEARCH PAPER we assigned a weighting of 60% to impacts on individuals and 40% on impacts to the organisation.

The risks are set out in the table below.

Issue	Title	Description	Impact on Individual	Impact on Organisation	Probability of Occurrence	Likelihood of Detection	Weighted Impact Individual	Weighted Impact Org	Risk Priority	Criticality
CT_001	Risk to data subject of fraudulent contact tracing	Data subjects will have provided their mobile number for contact tracing. There is a risk that they might be cold-called by fraudlent actors purporting to be contact tracers who could socially engineer data from them. This could deter co-operation with contact tracing	6	7	4	9	3.6	2.8	116	26
CT_004	Cross border data transfer	It is unclear from available documentation if data is to be hosted "locally" in EU or outside EEA. Appropriate basis for data transfer must be identified if data is being transferred	2	8	5	10	1.2	3.2	110	25
CT_003	Missed data on iOS devices	App must be running to record data. If iOS suspends an application logging of contact proximity data during the period of suspension may be reduced	2	8	9	5	1.2	3.2	99	45
CT_006	Excessive retention of register of users	User register data does not fall within the 21 data deletion process. There is a risk it could be retained indefinitely	2	6	5	10	1.2	2.4	90	20
CT_007	Application of retention period	Code does not appear to currently enforce 21 day retention period on-device.	2	7	9	5	1.2	2.8	90	41
CT_005	Withdrawal of consent	A data subject may withdraw consent for processing of data and delete the application leading to no contact tracing	5	7	4	2	3	2.8	24	24
CT_002	Unauthorised use of validation key	If a malicious actor obtained validation key used to unlock data on device for upload, they might have access to data of individuals proximity.	1	1	2	4	0.6	0.4	4	2

In addition, we would caution against over-reliance on the concept of consent as the basis for processing is much broader than exists in the legislation in other jurisdictions.

Root Cause Analysis

In this section we assess the root causes of any data protection and data privacy risks that arise so that appropriate mitigations can be recommended and implemented in a timely manner.

Risk ID	Root Cause Identified
CT_001	Malicious callers may take advantage of the overt use of mobile numbers as a contact tracing tool to conduct social engineering or fraud calls. This is identified as a risk in other jurisdictions. There is no easy mechanism to pre-validate that the caller is legitimately calling from contact tracing.
CT_004	Application is developed in a 3rd country. Unclear from available information how back-end data transfer will operate therefore risk that data will be transferred outside EEA.
CT_003	This is a function of the device for power saving purposes. Users can work around this if they are aware.
CT_002	Malicious actor risk needs to be factored in. However, the design of the application and the processing renders this vector largely impossible and of little value to a bad actor.
CT_005	The app as currently implemented appears to rely on consent. While the voluntary action involved in downloading the app suggests consent, broader grounds for processing exist. Therefore consent should not be the basis for processing and communication should focus on fair processing rather than soliciting consent. Data Subjects still have the right to opt-out and this should be permitted with a clear explanation of the implications of deleting the app/data.
CT_006	The root cause of excessive retention will be inertia and the absence of a defined retention period.
CT_007	Iterative development of application likely resulted in functionality not being deployed as not required within first 21 days of operation.
CT_008	Application originates in a jurisdiction with separate powers to permit government agencies to identify users of a particular mobile phone number. As such, the logging of information about the device user was probably not an immediate consideration.

Develop Improvement Plans

In this section of the we define actions which should be taken to address or mitigate the root causes of the risks and other deficiencies which have been identified in previous sections. This allows for a clear alignment to be defined between the risk and the associated mitigation.

Recommended Remediations

Risk ID	Root Cause Identified
CT_001	A randomly generated passphrase should be linked to the user in the master registry. This passphrase should be communicated to them either by SMS with instructions or should be displayed in the app. When a contact tracer phones a user they can provide the passphrase to validate they are calling from Public Health contact tracing. The existence of this security control should be clearly communicated as a deterrent to malicious actors.
CT_004	Ideally, on-shore all data storage to Ireland/EEA. If not possible, derogations under Article 49 can apply, subject to DPC approval.
CT_003	Ensure appropriate information is provided to users about how to avoid this issue. Consideration will need to be given also to the impact of screen-time application suspensions in IOS and Android.
CT_002	No mitigation possible to this potential risk, but impact is negligible
CT_005	• Make the applicable processing grounds clear in the application data protection notice and supporting material. • Remove reference to "consent" and replace with "acknowledgement" of processing • Provide clear information to data subjects re their right to object to processing and the implications to them of opt-ing out (no tracing contact if they are exposed, leading to risk to family and others)
CT_006	User register should be retained for 12 months from the date of registration or the date of last contact. The rationale for this is it allows for users to be recontacted to reinstall app if there is a resurgence of infections, but is not too long to present an excessive retention burden (baselined against SI336/2011 provisions re contacting customers).
CT_007	Localisation of the application should implement a 21-day cut off on retention of data. Pseudocode for query: "Select * from record_table where ((today)-(day(timestamp))>21"

Additional Recommendations

The benefit of this type of approach to contact tracing lies in the acceptance of the method by the data subjects. Unfortunately, State agencies have a significantly poor track record in the implementation of processes and systems that properly respect data protection obligations and there is inevitably a strong suspicion of government agencies engaged in new and innovative data processing.

Therefore, we strongly recommend a robust and clear communications process be implemented around this application to address the following key points:

1) The application does not process location data and, therefore, the State is not building a location tracking database for citizens.
2) Clearly communicating the purpose of the processing and how "herd tracing" (i.e. more people using the app) means faster response times for contact tracers responding to positive tests in individuals
3) Clearly communicating that people can change their minds about using the app at any time but explaining the consequences to them or others of doing so.
4) Clearly articulating that pseudonymised data is stored on people's devices, not centrally, until it is needed.
5) Clearly committing to deletion of any retained data once the purpose for its processing has expired.

Potential barriers to avoid

While it may be possible to argue that this processing falls within the scope of the exemptions to the Article 21 Right to Object, it is our recommendation that reliance on such exemptions would be counter-productive as it would lead to this being presented as a "mandatory but not compulsory" form of processing.

People should be allowed to opt-out of the processing (or to withdraw consent if there is an insistence on relying on consent), but they should be fully informed as to the implications of doing so for them and for others.

We would also strongly advise against the use of the word "anonymised" to describe the data that is processed. This is a factually incorrect classification of the data. It is pseudonymised as it can be reidentified by the health authorities when required. To describe it as "anonymised" when it is not will create confusion and invite unwarranted criticism and hostility to the processing.

Assessment of Residual Risk

The guidance notes on Data Protection Impact Assessments issued by various regulatory organisations are consistent in their identification that, despite every best effort to balance public interests with those of individual data subjects, not all risks to the fundamental rights and freedoms of individuals can be prevented or mitigated and some risks must simply be accepted within the risk appetite of the organisation.

In this section we perform an assessment of the residual risk inherent in the processing once all previously identified mitigating actions have been taken. This will also include a formal assessment of whether a referral to the Data Protection Commission for Prior Consultation under Regulation 2016/679/EU is required at this time, or if it would be a prudent consideration.

Residual Risk Assessment

Below we set out the risk assessment scoring assuming all remediation actions recommended are performed. Please note that the maximum scoring for a Risk Priority calculation is 500.

Residual Risks

Issue	Title	Recommended Mitigation	Residual Impact on Individual	Residual Impact on Org	Residual Probability of Occurrence	Residual Likelihood of Detection	Weighted Impact Individual	Weighted Impact Org	Residual Risk Priority	Residual Criticality
CT_003	Missed data on iOS devices	Ensure users are given clear instructions on how to minimise downtime in the app when running iOS	2	7	7	5	1.2	2.8	70	32
CT_004	Cross border data transfer	DPC can authorise transfer on the basis of Article 49(1)(d) or Article 49(1)(f) if necessary, but hosting in Ireland/EU is preferable. As app is hosted in Google Cloud, selection of GoogleCloud EU region mitigates this risk	2	8	1	10	1.2	3.2	22	5
CT_002	Unauthorised use of validation key	No mitigation required. Data on device is pseudonymised. If data was linked to user register, actual impact on fundamental rights nd freedoms is negligible.	5	6	4	2	3	2.4	22	22
CT_006	Excessive retention of register of users	Retention period should be set at 12 months since last communication with the data subject (baseline: SI336)	2	3	1	10	1.2	1.2	12	3
CT_001	Risk to data subject of fraudulent contact tracing	Include a "code phrase" in the app that is randomly generated as part of the registration process. Either generate on-device and record in central register or generate as part of the registration	2	2	1	10	1.2	0.8	10	2
CT_005	Withdrawal of consent	Consent is not the basis for processing in this context. Users should be advised of the implications of opt-ing out of processing and how to delete their data	1	1	2	4	0.6	0.4	4	2
CT_007	Application of retention period	Timestamp for each contact logged is recorded. Development of SQL statement and trigger to delete data is a required action. As retained data is not identifiable to 3rd parties, more substantial impact will be performance constraint on device.	1	1	1	1	0.6	0.4	1	1

Prior Consultation Recommendation

As the level of residual risk identified does not constitute a high risk to the fundamental rights and freedoms of data subjects, we do not believe a formal Prior Consultation procedure under Article 36 of Regulation 2016/679/EU is required at this time.

Summary Comment on Approach

Designing an app using an approach such as that of BlueTrace appears to meet criteria for Data Minimization and Privacy by Design and Default. It is likely that the specific focus for data processing using Bluetooth to record proximity and contacts will yield data that is more strongly fit for the purpose of supporting contact tracing than other approaches, while minimizing risks to the rights and freedoms of data subjects. Some implementation steps may be made to the approach taken by the reference app in order to better support local context and compliance requirements:

Recommended Steps to Implementation

We would recommend the implementation of the measures outlined above as part of a planned implementation.

This should address:

- Application customisation and functionality development
    - Implementation of data retention rule on device
    - Changes to text strings (replace “consent” with “acknowledge”)
    - Prepare a formal data protection statement for the app
    - Formally define retention schedule for user registration data
    - Add data and processing to HSE/HSPC Register of Processing Activities (Article 30 GDPR)
    - Implement EU-based hosting for database
    - Implement Contact Tracer Verification step
- Communications plan design and execution
    - Briefing on the application use
    - User guide
    - FAQ on how it works (localise content)
        - FAQ should specifically address how the application works and what data it accesses or doesn’t access.

Business Need #2 Symptom Tracking

This section examines the use of mobile location data and/or other mobile phone technologies to support the logging and tracking of symptoms. For the purposes of this research paper we have identified the Covid-19 symptom tracker deployed by Zoe Global Limited and Kings College London (https://covid.joinzoe.com/) as a reference model to conduct analysis against. We also looked at PatientSphere for Covid-19 by the Open Cancer Network in the United States.

Statement of Business Need and Approach

Proposed Processing Activity (What we propose to do)	To gather data about health symptoms from app users, whether they have tested positive for Covid-19 or not through a smartphone app
For the Purpose of	To develop a better knowledge of symptomatic progression and improve clinical case definitions to help differentiate Covid-19 from other seasonal respiratory infections (e.g. colds)
To achieve benefit (to the organisation)	• To improve clinical epidemiological information about Covid-19 • To support the identification of possible infection trends
To achieve benefit (to the data subject)	• To protect the vital interests of the data subject or others through more efficient use of public health resources

Analysis of Information Environment

This category of application can either process data as direct input into a remote database (Covid.Zoe approach) or it can log data locally on a device which can then be submitted to a public health official or doctor (PatientSphere approach).

Legal Environment (Basis for Processing)

As these categories of application would be processing special category data within the meaning of Article 9 of Regulation 2016/679/EU (GDPR), a higher standard of care is required in respect of the processing of this data.

Relevant Lawful Processing Conditions.

The relevant lawful processing conditions under GDPR are set out in the table below. It must be noted that *necessity* of the data to the processing purpose is a key requirement under the various provisions of Article 9.

Applicable Processing Condition	Rationale

Article 9(2)(a)	Individuals can be asked to give explicit consent. However, this must be explicit consent to each SPECIFIC processing activity that will be undertaken using the data.
Article 9(2)(g)	Processing is necessary for the purposes of Section 31(8) of the Health Act 1947, in particular Regulation 11 of SI390/1981
Article 9(2(i)	There is a public interest in the context of public health, subject to the provisions of the Health Act 1947

It is important to note, however, that these provisions carry with them a requirement to ensure appropriate safeguards for the processing of data.

Article 9(2)(c) does not apply in this context as:

1) The information processed is not *necessary* to protect the vital interests of the data subject (notwithstanding its helpfulness)
2) The data subject is capable of providing consent.

Processing of Location Data

Location data processed from the device such as GPS co-ordinates will require consent. This is a requirement under SI336/2011 and also a practical constraint of the permissions model of mobile operating systems.

Process Environment (Description of Processing Activities)

Both Covid.Zoe and the Planetsphere Covid Symptom tracker record data relating to:

- Personal profile (name, contact number, age)
- Symptoms (current symptoms, symptom history)
- Whether user or a co-habiting person has tested positive (Planetsphere only)
- Medications being taken (Planetsphere)
- Hospital treatments received (Covid.Zoe)

Screenshots of each of the applications from the Apple app store are provided in an appendix to this document.

The PlanetSphere application logs data locally on-device and allows it to be shared by email with a third party. The Covid.Zoe application logs entries directly to a backend database. It is not clear from the available documentation whether local logging of data takes place.

Users are identified primarily by their mobile phone number in both applications and mobile phone numbers are validated using a One-time-password code (similar to the TraceTogether implementation).

Necessity of Processing

For the purpose identified in the statement of business need and approach, it is necessary for public health officials to:

1) Identify and contact the data subject (name, mobile number)
2) Identify the data subject's general location
3) Identify self-reported symptoms
4) Identify medications being taken or medical interventions that have been undertaken in hospital

In the context of applications that are being deployed by Public Health authorities, there is no requirement for the application to record that the data subject or a person connected to them has tested positive for Covid-19 (this is functionality in the PlanetSphere app) as this information should already be available to the Public Health Authority.

Adequacy / Accuracy of Data

A limitation of "crowd-sourced" data gathering applications of this kind is that the quality of self-reported symptoms can be variable. Also, this kind of data gathering requires users to continue to log data in order for it to be useful for analytics purposes.

This may be easier to control for in the context of application users who have tested positive for Covid-19 or are identified close contacts of persons who have tested positive as part of a case-management approach.

In addition, the use of mobile phone location data to register the user's location may not provide appropriate level of data quality for accuracy in analysis.

Security of Processing

The Covid.Zoe implementation of symptom tracker logs data and uploads to a central server. The PlanetSphere implementation logs data locally on-device and allows for reports to be emailed off device to a user-input email address.

Any local storage on-device must be secure and encrypted.

It is our view that, in the context of a public health authority deploying an app to support symptom tracking, the app should not require the need to send data to a third party by email.

The exception to this would be if the symptom tracker information was required by a medical professional outside the public health environment. In such cases, the

application should be capable of uploading the symptom tracking report to a secure location which can be accessed by authorised healthcare professionals.

Technical Environment

Mobile Network

The use of smartphone applications assumes a consistent and reliable mobile phone network connection that can support upload of data to remote servers. While the headline coverage for mobile phone networks in Ireland is good, there are a large number of areas where operator coverage can be weak to non-existent due to local topographical issues or as a result of operator decisions re: investment in masts in a given area.

On-Device

The application can record a variety of items of data from mobile devices. If a user's location is required, their location can be derived from GPS data on the device. This will require consent and this should be clearly sought in the user registration process for the application.

Alternatively, users can be asked to provide their Eircode. Again, the purpose for this information needs to be made explicitly clear.

Risks and Root Cause Analysis

We have identified a number of risks in relation to the proposed use of symptom tracing applications modelled on the Covid.Zoe and PlanetSphere reference applications.

Issue	Title	Description	Risk Priority	Criticality	Category
ST_005	Retention of data	The retention of symptom and medication data linked to an identifiable individual is not necessary once the public health emergency has ended. Data may be relevant for research.	160	36	Governance
ST_001	Quanity of low quality data	Mass roll out of the symptom tracking application capability could result in excessive data of variable quality of self-reported symptoms which could reduce quality of analysis and actions	158	39	Governance
ST_003	Unauthorised access to symptom data in transfer	Special category data from symptom tracker needs to be transferred securely.	111	23	Technology
ST_002	Mobile network access may impede use of app	The use of an app to upload symptom data assumes existence of an "always on" data capability and reliable mobile network. This may exclude people in certain areas from the use of this app.	88	25	Governance
ST_004	Inaccurate Location Data	Users registering the app at a location that is not their home address may be mis-identified as being based in the other location leading to inaccuracy in any analysis	52	24	Process

The root causes for the identified issues are as follows:

Issue	Root Cause
ST_005	Storage limitation is a requirement under GDPR. Clarity on retention period/purpose is an essential element of ensuring user trust.
ST_001	Individual perception of symptoms can be subjective. Submission of irrelevant symptom data from a large population can result in symptoms correlated to a link to a diagnosed case being missed/overlooked.
ST_003	Email is an insecure data transfer mechanism. Unless app supports an encrypted email client internally, potential breach of Article 32 obligations to ensure security of data.
ST_002	This is a function of mobile networks and is outside the scope of an app to address. An alternative mechanism needs to exist for individuals to log their symptoms where necessary
ST_004	People may download app at GP surgery or at a location not their home. Also, mobile network location data can be inaccurate.

Recommended Mitigations

Based on our analysis, we would make the following recommendations for mitigation, which we believe will reduce the residual risks involved in processing.

Issue	Title	Recommended Mitigation	Residual Risk Priority	Residual Criticality
ST_005	Retention of data	A defined retention schedule is required BEFORE the application is deployed to define how long de-identified symptom and medication data will be retained and for what purpose. There is no basis to retain this in an indentifiable format	17	4
ST_001	Quanity of low quality data	Recommend targetting roll out of symptom tracker to close contacts of positive test subjects	92	20
ST_003	Unauthorised access to symptom data in transfer	For app implementations that communicate directly with server, HTTPS protocol must be applied, data should be encrypted in transit. Where data is stored locally, email should not be used for data transfer off app, use an upload process similar to TraceTogether data upload.	50	10
ST_002	Mobile network access may impede use of app	Need to consider alternative mechanisms for symptom tracking for people with low/no mobile coverage or access to internet	84	25
ST_004	Inaccurate Location Data	Request home eircode for the purposes of mapping symptoms. This should be an OPTIONAL field and should NOT be used for any other purpose	36	16

Summary Comment on Approach

The Business Needs and Approach, and Information Environment of an app for symptom tracking is significantly different to the goals, contexts, and purposes for processing of the previously reviewed app to support contact tracing, requiring completely different datasets for different purposes, and presenting a different risk profile.

The quality and fitness for purpose of data collected may vary significantly with implementation decisions in developing the app in addition to the variable quality of crowd-sourced symptom data. The processing of location data presents compliance and privacy risks which may not be adequately answered by benefit of quality data for analysis.

In addition, as the data gathered in such an app would be self-reported, design of the data flow and analysis must take into consideration data quality for information collected from people who become too unwell to self-report using the app.

Furthermore, our analysis presumes a “self-hosted” application, not a rebadged version of an externally provided application which would introduce additional risks.

Business Need #3: Push Notification of Contacts

This section examines the use of mobile location data and/or other mobile phone technologies to support the push notification through an app of alerts regarding close contact with an infected person. For the purposes of this research paper we have identified a Covid-19 close contact tracking application from the EU which provides this functionality as a reference model for assessment.

Statement of Business Need and Approach

Proposed Processing Activity (What we propose to do)	To send a push notification alert to an application user when they are identified as having been in close contact with another individual who has tested positive for Covid-19
For the Purpose of	• Advising the individual as to the required public health actions (self-isolation etc.) • Advising individual re: testing or symptom tracking requirements
To achieve benefit (to the organisation)	• Reduces human involvement in contact tracing process • Improved efficiency of contact tracing and follow up
To achieve benefit (to the data subject)	• To protect the vital interests of the data subject or others through more efficient use of public health resources

Analysis of Information Environment

Legal Environment (Basis for Processing)

As these categories of application would be processing special category data within the meaning of Article 9 of Regulation 2016/679/EU (GDPR), a higher standard of care is required in respect of the processing of this data.

Relevant Lawful Processing Conditions.

The relevant lawful processing conditions under GDPR are set out in the table below. It must be noted that *necessity* of the data to the processing purpose is a key requirement under the various provisions of Article 9.

Applicable Processing Condition	Rationale
Article 9(2)(a)	Individuals can be asked to give explicit consent. However, this must be explicit consent to each SPECIFIC processing activity that will be undertaken using the data.
Article 9(2(i)	There is a public interest in the context of public health, subject to the provisions of the Health Act 1947

It is important to note, however, that these provisions carry with them a requirement to ensure appropriate safeguards for the processing of data.

Article 9(2)(c) does not apply in this context as:

1) The information processed is not *necessary* to protect the vital interests of the data subject (notwithstanding its helpfulness)
2) The data subject is capable of providing consent.

Article 9(2)(g) does not apply in this context as:

1) The sending of a push notification is not NECESSARY given the existing and established processes for contact tracing and follow-up that exist.

Application of SI336/2011 and the ePrivacy Directives

As the communication in this context will not be for the purposes of marketing, the provisions of Regulation 13 of SI336/2011 do not apply.

Process Environment (Description of Processing Activities)

The reference application identified which triggers push notifications to users is primarily a contact tracing application that, once a close proximity contact of a user is confirmed as having tested positive for Covid-19 generates a push notification to any app user who has been in contact with the positive test subject.

Therefore, the operative processing mechanism is similar to the "Action" phase of the contact tracing scenario examined earlier in this report, with the outbound calling from a contact tracer being replaced with a push notification delivered to the app.

Adequacy / Accuracy of Data

In this context, the key driver of the trigger to send notification is the identification of a close proximity contact between two users of the application. This will be accurate within the following constraints:

- Accuracy of Bluetooth range estimation and contact logging
- Uptake and adoption of the contact tracing application
- Functionality constraints in iOS environment

Security of Processing

The security of processing of the data will be dependent on the security of the mobile app and associated back-end database.

There is a risk that push notifications could be accessed by 3rd parties (e.g. family members). This could lead to distress, particularly if the 3rd party is a related child or person with reduced intellectual capacity to understand the nature of any message.

Potential for Unintended Consequences

It should be borne in mind that there is a significant risk of unintended consequences from the use of push notifications in this context.

There is a risk that a push notification without supporting context information could cause unwarranted distress to a data subject or another (e.g. a child). This is particularly the case in vulnerable persons (e.g. people with depression, mental illness, or intellectual disability, or cognitive impairment).

There is also a risk that in circumstances where a data subject has a small social group or lives in a sparsely populated area that a push notification of close contact could provoke a negative reaction and create a risk of harm to a 3rd party. While this is a low probability risk, it would be damaging to trust in the application if it was to occur.

Therefore, the reliance on push notifications as a primary method of communicating close contact events to data subjects should be treated with caution to ensure appropriate social and clinical responses are delivered.

Risks and Root Cause Analysis

We have identified a number of risks in relation to the proposed use of push notifications for communication of close proximity contact with infected persons.

Issue	Title	Description	Risk Priority	Criticality	Category
PN_001	GPs swamped with inbound calls, affecting delivery of care	The provision of a push notification of close contact may result in an increase in calls inbound to GPs or health clinics, impacting on operations and delivery of care	175	39	Process
PN_005	Push notification to children in error	Unless application captures year of birth, there is a risk that push notifications will be issued to children, who have downloaded a contact tracing app	160	33	Process
PN_003	Distress to data subject	The impersonal nature of push notifications means that this may cause distress to data subjects who receive a message and do not understand the message or who are vulnerable to negative interpretations	158	35	Process
PN_002	Unauthorised disclosure of contact with infected person via 3rd party accessing phone	If a 3rd party acesses a users phone they will be able to see any push notifications received. This may include children using a parent's device	88	35	Governance
PN_004	Injury to a 3rd party	If push notification received by a person in a small social group/small population area, it may give rise to aggressive response (driven by fear/lack of understanding)	70	14	Process

The root causes we have determined for these risks are identified below.

Issue	Root Cause
PN_001	Human reaction on receipt of a push notification of close contact with positive case will be to seek further information or take further action. This will result in calls to primary healthcare provider.
PN_005	If children register for apps without any check to verify age/identify age, push notification will be issued to children
PN_003	Lack of human touch and absence of immediate response to queries that might arise will lead to distress
PN_002	Nature of phones and push notifications. User may expose data themselves
PN_004	Lack of “human touch” and absent immediate response to queries and information in context could result in a negative emotional response (anger) towards a small/identifiable population set.

Recommended Mitigations

Our recommended mitigations for the risks identified above are summarised below, along with our estimation of the residual risk inherent in the proposed processing as a result of applying these mitigations.

Issue	Title	Recommended Mitigation	Residual Risk Priority	Residual Criticality
PN_001	GPs swamped with inbound calls, affecting delivery of care	An existing process for contact tracing follow up exists. Push notification should supplement not replace this process. Recommend use of push notifications AFTER contact attempt by contact tracer. Message sent needs to have clear and specific call to action. Alternatively: establish dedicated INBOUND call line for queries but must ensure capacity.	100	23
PN_005	Push notification to children in error	Contact tracing apps should capture year of birth as part of registration. Children (<18, or potentially <16) should be excluded from push notification contact	32	7
PN_003	Distress to data subject	Push notifications should support/supplement standard human-driven contact tracing follow up processes. Messaging must be exceptionally clear to minimise distress	87	20
PN_002	Unauthorised disclosure of contact with infected person via 3rd party accessing phone	This is outside the direct control of the health authority to mitigate. Users should be advised of the risk of push notifications if this is to be deployed	88	35
PN_004	Injury to a 3rd party	Push notifications should support/supplement standard human-driven contact tracing follow up processes. Messaging must be exceptionally clear to minimise distress	44	9

As a general principle, push notifications should be used to supplement not replace standard public health tracing and follow up processes.

The communication and "call to action" in any push notification should be extremely clear for individuals and need to ensure that people with literacy or language issues will be capable of understanding the message and what their next action should be.

Summary Comment on Approach

This approach presents numerous risks of unintended consequences. Reliance on push notifications as a primary method of communicating close contact events to data subjects should be treated with caution to ensure appropriate social and clinical responses are delivered.

Business Need #4: Population Movement

This section examines the use of mobile location data and/or other mobile phone technologies to support tracking of population movements. For the purposes of this research paper we have referenced against the use of mobile phone location data during the most Ebola outbreak to inform our assessment.

Statement of Business Need and Approach

Proposed Processing Activity (What we propose to do)	To use mobile network CDR (call data record) or network location data to develop statistical analysis of population movements
For the Purpose of	• To support statistical analysis of the effectiveness of restrictions on movement. • To identify higher risk areas for community transfer due to statistical non-compliance with movement restrictions
To achieve benefit (to the organisation)	• To assist in infection trend prediction • To inform of effectiveness of public health controls
To achieve benefit (to the data subject)	• To protect the vital interests of the data subject or others through more efficient use of public health resources

Analysis of Information Environment

The primary source for data for the purposes of this type of tracking would be the mobile phone networks. The location data from CDRs (Call Data Records) in the network allows for the identification of an approximate location of an individual based on the mobile phone mast that their device has connected with to connect to the network.

Legal Environment (Analysis of Legal Basis)

The processing of location data from devices connected to a public communications network is governed by the ePrivacy Directives 2002-2009, as enacted in Ireland through SI336/201. The ePrivacy Directives are *lex specialis* and therefore need to be considered outside the parameters of GDPR.

Regulation 9 of SI336 addresses the use of location data and requires data to be either made anonymous or be processed solely on the basis of consent "to the extent and duration necessary for the provision of the value added service" (which in this context we will interpret as mobile operator assisted infectious disease control, but normally this relates to value added services in a mobile network).

Anonymisation and Reidentification

The term "anonymised data" is often misused to refer to data that has had the directly identifiable portions removed or truncated. However, if there is the possibility for an individual to be identified *indirectly* from data it still falls within the definition of personal data under Regulation 2016/679/EU and should be more accurately described as pseudonymised data.

Therefore, for any processing of location data derived from the telecommunications network to be used without having to obtain freely given, specific, unambiguous, and informed consent from each data subject, the data must be aggregated such that an individual user cannot be reidentified from the data. However, it must be noted that granular location data has a very high risk of reidentification, to the point that location pattern information derived from CDR data is functionally impossible to truly anonymise under the EU Data Protection legislation.

Technical Environment (Summarised)

Mobile phone networks record both CDR data for the purposes of billing. In this data is the Home Location Register data which records which network mast a device was connected to when making a call. The network records the number of devices connected to a Home Location as part of its network logging data.

It is therefore possible to identify for a given subscriber what HLR they were connected to at a specific time, which is a traditional use of CDR data in law enforcement applications. It is also possible to report on the number of mobile phones connected to a given Home Location at particular times, allowing for statistical comparisons of network usage and device movement over time.

The granularity of location data derived from the network is down to the Home Location / Mast level and within the signal radius of a given network mast. It is not sufficiently granular for close proximity contact tracing but could be relevant for statistical analysis of population movements.

FlowMindr has published information on the approaches taken to processing mobile network data for epidemiological analysis based on their work supporting mobile operators using data to assist in the response to the Ebola outbreak in 2014. They recommend the following approaches to minimise data protection, privacy, and security risks:

1) MISISDN and IMEI numbers should be hashed and stretched using SHA-3
2) Anonymised data should be retained within operator's environments and not be shared. Analysis should take place in the Operator's environment with access via VPN

Process Environment

The general processing approach to processing this data is to perform statistical analysis of population movements between locations defined by network locations. The analysis would show a percentage increase or decrease of devices connecting to the network in particular locations.

This data can be used to evaluate the level of changing population mobility as a measure of effectiveness of restrictions on movement in the society as part of disease control measures.

Risks and Root Cause Analysis

We have identified the following risks.

Issue	Title	Description	Risk Priority	Criticality	Category
PT_001	Mass Surveillance risk	Where users consent to the use for mobile location data, it constitutes a mass surveillance risk	350	70	Governance
PT_003	Excessive retention of data	Data may be retained for longer than is needed	171	39	Governance
PT_002	Disclosure of individual calling patterns	If a malicious actor knows the cell tower a person is calling from, they can potentially identify calling patterns that would identify an individual	132	33	Governance

These risks assume that consent has been obtained for processing or that the processing is being undertaken in a manner that aggregates and effectively anonymises data using appropriate clustering.

The root cause for these risks is that they arise from the volume of data and the potential desire of organisations to retain data for research or analytical purposes.

We set out a number of mitigations to these risks.

Recommended Mitigations

Issue	Title	Recommended Mitigation	Residual Risk Priority	Residual Criticality
PT_001	Mass Surveillance risk	Appropriate safeguards need to be implemented to mitigate riskof mass surveillance. This includes deletion of data once public health emergency has abated, restriction on use of data to purely statistical analysis, and limitation on the access to data by individuals	175	35
PT_003	Excessive retention of data	Need to have a defined retention period for any data that is not aggregated statistical data. Retained data should be aggregated using K-anonymity approach to cluster data and remove data where group sizes are small	30	7
PT_002	Disclosure of individual calling patterns	Limit access to data to specifc persons. Retain data within operator environments to reduce risk of reidentification	53	13

Key controls that are recommended in respect of the use of mobile network data include:

- The mobile phone numbers of subscribers making and receiving calls or text messages will be anonymised by mobile operators inside their premises and on their equipment. This is achieved by replacing the mobile phone numbers with an anonymous code before being analysed. This is done through a hashing process using the secure SHA-3 algorithm.
- Anonymised CDR data will not be transferred outside of the operator's system/premises: The anonymised data will be kept secure and encrypted within the operator's premises. Access to the data will be controlled and given only to pre-approved and authorised personnel. A record of access will be maintained and auditable. Access to the algorithm and the ability to decrypt the data will be further protected by also limiting access to pre-approved and authorised personnel.
- All analysis will take place on mobile operator's systems, in their premises and under operator supervision. Once anonymised by the mobile operator, the data will be analysed on-site by approved research entities that agree to abide by strict ethical standards on the use of data.
- No analysis will be undertaken that singles out identifiable individuals. No attempts will be made to link the data to other data about an individual and which may impact on their privacy or otherwise cause harm.
- Only the output of the analysis (i.e. the resulting non-sensitive data on population mobility estimates, aggregate statistics, indicators, etc.) will be made available to relevant and approved aid agencies, government or research agencies that can use these inputs in their modelling and planning efforts. No sensitive data will be shared with or made available to any third parties.

In addition to these mitigations, we would recommend the consideration of pure statistical analysis of device connections to different Home Locations in the HLR data set. Analysis of this data over time, using hashed data, would allow for a statistical analysis of movement between locations without the call data associated to a CDR that could potentially allow for reidentification.

This data could be prepared for analysis by operators and aggregated by a small area statistical code to further cluster mobile network masts into defined geographical areas not directly linked to individuals.

Summary Comment on Approach

The use of CDR data, in particular location data, is complicated by the Legal Environment and the difficulty of truly anonymising granular location and CDR data, as it carries high risk of reidentification. Mitigations must be taken to ensure that individuals cannot be singled out from a crowd in analysis.

Business Need #5: Push Notification of Updates

This section examines the use of mobile location data and/or other mobile phone technologies to support the logging and tracking of symptoms. For the purposes of this research paper we have referenced against the use of mobile phone location data during the most Ebola outbreak to inform our assessment.

Statement of Business Need and Approach

Proposed Processing Activity (What we propose to do)	Push notifications to be sent to app users to provide information to data subjects about infection control measures or other public health measures.
For the Purpose of	• Supporting public health communications and updates on social control measures in effect in an area
To achieve benefit (to the organisation)	• Improved targeting of communication • Improve efficiency of communication
To achieve benefit (to the data subject)	• More timely provision of targeted information relating to their specific situation.

Legal Environment (Analysis of Legal Basis)

Assuming push notifications would be of a general nature and would not be relating to the health of an identified data subject, the legal basis for processing would need to be found under Article 6 of GDPR.

Consent under the ePrivacy Directives/SI336 would not be required so long as the messages did not contain a direct marketing call to action (e.g. requesting people purchase an app or subscribe to a service).

Applicable Processing Condition	Rationale
Article 6(1)(a)	Data subjects can "opt-in" to receive push notifications
Article 6(1)(e)	The processing may be necessary to provide updates and information necessary to the public health function but not necessary to the protection of vital interests

Process Environment

The processing environment for push notifications of this kind is that a message is formulated and then submitted for broadcast via the application.

However, this is dependent on network coverage and an active data connection and may discriminate against persons who have poor network coverage, particularly for data services.

Risks and Root Cause Analysis

We identify few risks associated with this proposed processing activity, assuming the purpose of processing to distribute push notifications is clearly explained and disclosed to data subjects.

Issue	Title	Description	Risk Priority	Criticality	Category
PN2_001	Push notification to children in error	Notification messages may be sent inappropriately to children. Less significant impact than contact trace push notifications but may cause upset/distress	90	20	Governance
PN2_002	Retention of contact information	A defined retention period would be required for retention of subscriber lists	144	32	Governance

The root causes here are related to the potentially open nature of the applications to download.

Recommended Mitigations

Issue	Title	Recommended Mitigation	Residual Risk Priority	Residual Criticality
PN2_001	Push notification to children in error	Implement appropriate safeguards to ensure age appropriate messaging is used	28	6
PN2_002	Retention of contact information	Recommend a retention period of 12 months after date of last message, benchmarked against SI336	26	6

The above mitigations substantively address the risks identified, however we would also recommend an alternative strategy be considered.

Summary Comment on Approach

Rather than pursuing the strategy of a push notification via an application, we would recommend the creation of a subscription SMS service where individuals can subscribe using their County and receive updates at a County level by SMS.

This reduces the reliance on push notification, and removes any dependence on mobile network data services.

Conclusion and Recommendations

The development of contact tracing and symptom tracking applications has a clear benefit in the context of public health responses to infectious diseases, not just in the immediate context. However, the convenience and capability of smartphone application based technologies needs to be balanced against the fundamental rights of individuals, particularly given the *de facto* introduction of a mass surveillance capability in response to a public health emergency.

The need to strike an appropriate balance has been recognised by the WHO, the EU Commission, and other key stakeholders. With great power comes great responsibility.

We recommend that a graduated response would be appropriate in respect of applications, with the temptation to build a "one-size fits all" application being avoided in favour of specific apps for specific purpose.

We further recommend that:

1) General notifications and updates are best served through an SMS update list rather than an app-based mechanism as this would widen the pool of potential recipients beyond smartphone users or people with good data connectivity.
2) Push notifications to alert to close proximity contact with persons who have tested positive should be approached with caution for a variety of reasons. This technology should be implemented in a manner that supports but does not replace or supplant existing well practiced processes that have a strong "human touch" component.
3) Mobile network data analysis has a potential application in assessing population movements en masse and in assessing the effectiveness of population movement controls to limit spread, but they require substantial safeguards to be put in place to limit their impact on fundamental rights and freedoms
4) Bluetooth sensor based contact tracing applications strike an appropriate balance between functionality and privacy, notwithstanding the functional limitations that have been identified in certain mobile operating systems.
5) Symptom tracking applications should be used in tandem with contact tracing and should be deployed with people who have been identified as a close contact to support monitoring of disease progression (or not) while these close contacts self-isolate. Wide spread public deployment risks creating a large volume of data but a low value of information due to data

quality issues in self-reporting of symptoms and variances in self-reporting discipline among individuals.

6) Public Authorities should avoid the temptation to build all features into a single app, particularly when deadlines are tight and there is a need for the delivered software to function with minimal error. There are (at least) two applications to consider:
    a. **Contact tracing** – a *de minimis* app should allow for identification of close proximity contacts and communication with them
    b. **Symptom tracking <u>for close contacts</u>**: - a *de minimis* application in this context should allow for the close proximity contacts of infected persons to record their symptoms and for that data to be accessible by public health officials.
7) Data should be retained in an identifiable form for no longer than is necessary for the management of response to the public health emergency
    a. Mobile network data should be anonymised at all times
    b. Identifiable user registration data should be retained for 12 months after date of last contact
    c. Symptom tracker data should be retained in an identifiable form for 30 days after date of last entry. Aggregated and deidentified data may be retained for research purposes for longer.

We further recommend an excessive focus on transparency and communication of what is being done with people's data to ensure that data subjects can trust the processing. This extends to robust clarity on retention periods for identifiable data and the methods that will be used to aggregate data for research purposes which may arise subsequent to the initial response periods.

The importance of trust in this process cannot be understated to ensure that the right information is obtained in the right way to inform appropriate public health actions to support recovery and promote health. If any concept is to be adopted from the software development world into this process it should be the concept of the **minimum viable product**.

Ultimately, as Dr. Michael Ryan has pointed out, "The perfect is the enemy of the good" in pandemic response.

References

de Hert, P., & Wright, D. (2012). *Privacy Impact Assessment.* Brussels: Springer.

DPC. (2018, November). *List of Types of Data Processing Operations which require a Data Protection Impact Assessment.*

DPC. (2019, September). *Guide to Data Protection Impact Assessments (DPIAs).* Retrieved from Data Protection Commission: https://www.dataprotection.ie/sites/default/files/uploads/2019-09/190926%20Guide%20to%20Data%20Protection%20Impact%20Assessments%20%28DPIAs%29.pdf

EDPB. (2017, October 4). *Guidelines on Data Protection Impact Assessment (DPIA) and determining whetherprocessing is "likely to result in a high risk" for the purposes of Regulation 2016/679.* Retrieved from European Data Protection Board: https://ec.europa.eu/newsroom/document.cfm?doc_id=47711

Finneran-Dennedy, M., Dennedy, T., & Fox, J. (2014). *The Privacy Engineer's Manifesto.* Apress.

Justice, A., Rabeneck, L., Hays, R., Wu, A., & Rozzette, S. (1999). Sensitivity, specificity, reliability, and clinical validity of provider-reported symptoms: a comparison with self-reported symptoms. . *Outcomes Committee of the AIDS Clinical Trials Group*.

McDonald, S. (2016). *Ebola: A Big Data Disaster.* Dehli: The Centre for Internet and Society.

O'Keefe, K., & O Brien, D. (2018). *Ethical Data & Information Management: Concepts, Tools, and Methods.* Kogan Page.

Vokel, F. (2020, 03 23). *TraceTogether - Under the Hood.* Retrieved from Medium.com: https://medium.com/@frankvolkel/tracetogether-under-the-hood-7d5e509aeb5d

Appendices

Appendix 1: Mapping Castlebridge Framework to EDPB/DPC Guidance

Description of Methodology and Approach

The Castlebridge DPIA Framework

The analysis in this report has been carried out using the Castlebridge DPIA Framework. This methodology has been developed based on a proven quality management system for information management, which we have adapted to meet the requirements of a structured Data Protection Impact Assessment methodology. This assessment addresses the first six steps in this framework.

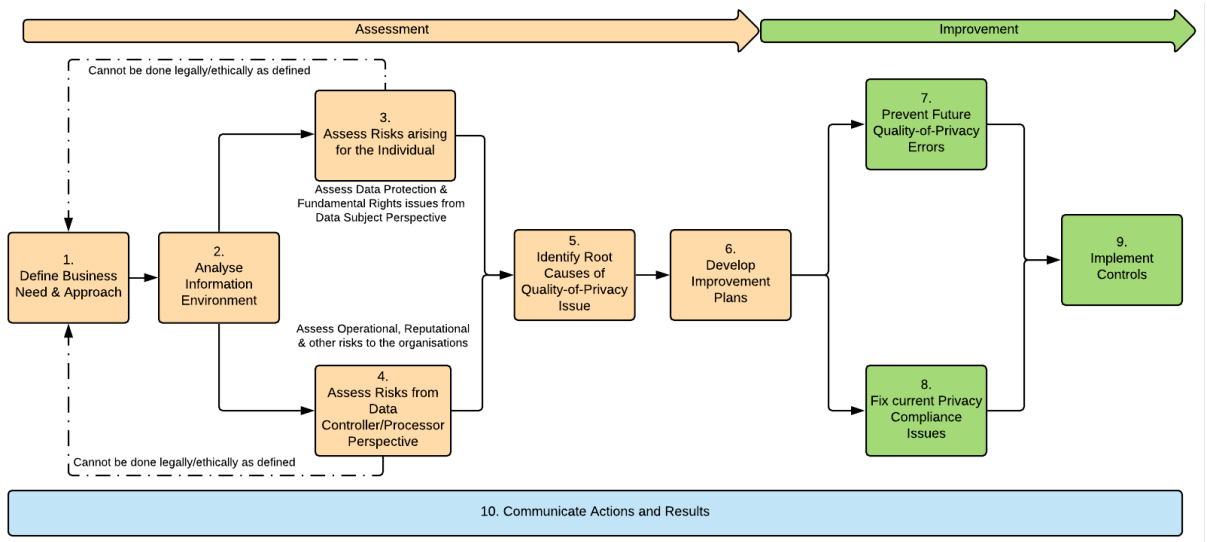


Figure 2: The Castlebridge DPIA Framework

The Castlebridge Ethical Impact Assessment Framework builds on the DPIA framework and extends it to consider wider ethical issues as appropriate. The full Ethical Impact Assessment model is described in (O'Keefe & O Brien, 2018)

Step	Summary Description
1	This step defines the processing purposes and seeks to break out the description of processing into discrete goals. It is also where an assessment of whether a DPIA is required is undertaken.
2	In this step we assess the broad information environment of the processing environment from different perspectives, including legal basis, necessity, proportionality, technology etc.
3	In these steps we conduct an assessment of the impacts on data protection rights, fundamental rights and freedoms, and organisation objectives to establish risks.
4	
5	In this step we determine the root cause of the issues /risks identified
6	In this step we develop remediation and mitigation plans to address the root causes of the risks identified in steps 3 to 5.

Data Protection Impact Assessments are intended to "identify and mitigate against any data protection related risks arising from a new project, which may affect your organisation or the individuals it engages with[i]". The primary concern at all times has to be the impact on data subjects. All impacts on data subjects, regardless of relative criticality or priority, have to be mitigated or addressed.

The Castlebridge DPIA methodology used in this Research Paper is a proprietary methodology developed to take account of the requirements under Recital 75 of GPDR and Recital 58 of the Law Enforcement Directive for organisations to assess risks from the perspective of the impact on the fundamental rights and freedoms of data subjects, while at the same time taking account of the c7ompeting interests of Data Controllers, to ensure that informed decisions are made regarding safeguards and other mechanisms envisaged to protect personal data, minimise the impact on fundamental rights and freedoms, and to demonstrate compliance with relevant legislation.

The methodology is adapted from a proven risk assessment methodology in quality management systems, Failure Modes and Effects Analysis[ii], and it explicitly recognises the impact of identified issues and risks to both the individual and to the organisation. These impacts are ranked on a 1 to 10 scale to allow for granularity of assessment. The likelihood of occurrence is also ranked on a scale of 1 to 10 and the likelihood of detecting the risk event (i.e. recognising that it is occurring) is also scored on a scale of 1 to 10. A composite "Risk Criticality" score is calculated based on the Impact on Individuals, Impact on the Organisation, and the Likelihood of Occurrence. A "Risk Priority" score is calculated by including the Likelihood of Detection. Therefore, highly critical risks which would be easy to detect and mitigate are given a higher priority score.

These scores are assigned to both the inherent risk assessment (before mitigations and controls are applied) and the residual risk assessment (after mitigations and

controls are implemented). Mitigations usually focus on reducing the impact of the risk or its likelihood of occurrence.

Further information about the Castlebridge Risk Assessment Methodology can be obtained directly from Castlebridge.

The European Data Protection Board (EDPB) and Ireland's Data Protection Commission (DPC) have both published guidance on the conduct of Data Protection Impact Assessments. Our methodology maps to the high-level framework recommendations of both the EDPB guidance of 2017 (EDPB, 2017) and the guidance note from the DPC in September 2019 (DPC, 2019).

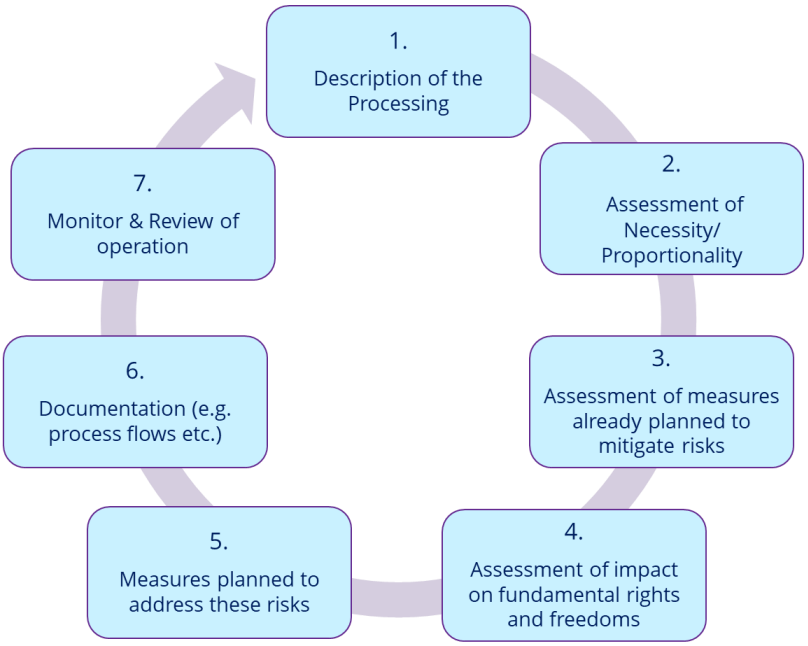


Figure 3 EDPB Data Protection Impact Assessment Process (source: WP248, rev.01, October 2017)

EDBP Step	Castlebridge Mapping	Comment
Step 1	Step 1- Business Need & Approach Definition	This is essential for the correct scoping and framing of the DPIA process.
Step 2	Step 2 – Assess Information Environment	Castlebridge Methodology breaks these activities into different task clusters from the EDPB generic format but the same activities are performed.
Step 3	Step 2 – Assess Information Environment Step 3 – Assess Data Subject Privacy Impact Step 4 – Assess Business Risk	
Step 4	Step 3 – Assess Data Subject Privacy Impact Step 5 – Identify Root cause	
Step 5	Step 2 – Assess Information Environment Step 5 – Identify Root Causes Step 6 – Develop Improvement plans	
Step 6	Step 2 – Assess Information Environment Step 10 – Communicate Step 7 - Fix current issues Step 8 - Prevent future issues	Documentation is provided for review as part of Step 2, documentation would be updated as part of implementation of PIA recommendations
Step 7	Step 9 – Implement Controls	PIA will recommend controls as part of improvement plans

Table 1: Mapping Castlebridge Methodology to EDPB Guidance

Risk Assessment Methodology

The Risk Assessment Methodology applied by Castlebridge is a proprietary risk assessment approach we have developed for Data Protection/Privacy Impact Assessments. It takes account of the clear requirement under Recital 75 of Regulation 2016/679/EU and the implied requirement in Recital 58 of Directive 2016/680/EU for organisations to assess risks from the perspective of the impact on the fundamental rights and freedoms of data subjects. The methodology applied also takes account of the competing rights and interests of Data Controllers for the purposes of informing decisions regarding safeguards and other mechanisms envisaged to ensure the protection of personal data and to demonstrate compliance with relevant legislation.

We apply a variant of the Failure Mode Effects Analysis[iii] methodology that is commonly applied in quality management systems. Within this analysis, we rank the following variables to calculate a risk criticality score. The variables we rank are set out in the table below. Rankings are performed on a 1 to 10 scale. The rubric and process for calculating risk criticality is also described below.

Variable	Definition

Impact on Individual (**IoI**)	An assessment of the impact on the fundamental rights and freedoms or choice/agency of individuals arising from or as an outcome of the proposed processing activity
Impact on Organisation (**IoO**)	An assessment of the impact on objectives of the organisation or on the brand or operations of the organisation in the event that this risk materialises
Likelihood of Detection (**LD**)	An assessment of how likely it is, in the normal course of operations and in light of the identified controls and mitigations that have been or will be implemented, that the occurrence of a risk would be identified in a timely manner sufficient to minimise impact on individuals or organisations
Probability of Occurrence (**PO**)	An assessment of the probability that a given risk would manifest itself as an actual event impacting individuals or the organisation.
Weighted Impact on Individual (WIOI)	Where a Risk weighting bias is included in the calculation to reflect a priority to the Individual or organisation this is calculated as (IoI * Risk Bias)
Weighted Impact on Organisation (WIOO)	Where a Risk weighting bias is included in the calculation to reflect a priority to the Individual or organisation this is calculated as (IoO * Risk Bias)
Criticality of Risk (**CoR**)	A calculation of the severity of the risk without consideration of ease of detection. ***COR=(Average(WIoI:WIoO)*PO***
Risk Priority (**RP**)	A calculation of the relative priority of a risk taking into account of the likelihood of detection. It is calculated as follows: ***RP=(Average (WIoI:WIoO)*LD*PO)***

Table 2 Risk Calculation and Assessment Variable

Presentation of Risk Assessment

The Risk Assessment is presented in a standard grid format that allows for summarisation by Risk Priority Score or Risk Criticality score. For the purposes of colour coding risks, the maximum and minimum risk scores are calculated as hidden values to ensure an appropriate Red/Amber/Green coding across all values. The maximum Risk Priority Score is 1000 and the minimum is 1. The maximum Risk Criticality is 100.

The Risk Bias value allows for a weighting between the right of the individual and the interests of the organisation to be explicitly applied. This bias is on a scale of 0 to 100 and results in the calculation of a Weighted Impact score for Individuals and Organisations which is used as the basis for Risk Priority and Criticality calculation.

The template also captures the recommended remediation for the specific risk and the Residual Risk Priority and Risk Criticality scores based on the recommended remediations being applied.

Risk Bias	Individual	Organisation																		
	60	40																		
Issue	**Title**	**Description**	**Impact on Individual**	**Impact on Organisation**	**Probability of Occurrence**	**Likelihood of Detection**	**Weighted Impact Individual**	**Weighted Impact Org**	**Risk Priority**	**Criticality**	**Category**	**Recommended Mitigation**	**Residual Impact on Individual**	**Residual Impact on Organisation**	**Residual Probability of Occurrence**	**Residual Likelihood of Detection**	**Weighted Impact Individual**	**Weighted Impact Org**	**Residual Risk Priority**	**Residual Criticality**
Unique ID	**Failure mode / Risk**	**Failure mode / Risk description**	**1- 10 Score**	**1 -10 score**	**1 -10 score**	**1 - 10 Score**	Individual score * Weighting	Organisation score * Weighting	RPN Score	Criticality Sore	**Categorisation of Root Cause Type**	**Recommended Mitigation**	**1- 10 Score**	**1 -10 score**	**1 -10 score**	**1 - 10 Score**	Individual score * Weighting	Organisation score * Weighting	RPN Score	Criticality Sore

Figure 4: Example of Risk Assessment Template

Appendix 2: Alignment of TraceTogether with Irish Standards

As part of our analysis of TraceTogether application, Castlebridge mapped the functions of the application to HIQA Safer Better Patient Care and also to a general statement of fundamental data protection principles.

HIQA Safer Better Patient Care

Any healthcare processing in the Republic of Ireland should comply with HIQA's "Better Safer Patient Care" standards. While not strictly a component of data protection compliance, compliance with these standards as they apply to the protection of personal data does form a component of the assessment of stakeholder expectations. The most relevant standard statements are contained in Theme 8 of Better Safer Patient Care.

HIQA Standard	How Met
8.1 Information Quality	The data from this app would be more accurate than mobile mast-based data as it is working in a closer range communications protocol. It would also have more accurate information about duration of close contact as it would not be dependent on operative range of mobile cell. Contact information would be as volunteered
8.2 Good Governance arrangements	The app only requires the sharing of data with the Public Health departments once a positive test has been recorded. Data about close contacts is only identifiable to the HSE once it has been uploaded and linked to the registered users of the app
8.3 Effective arrangement for management of healthcare records	The storage of data on the device means it is not processed or retained by the HSE until such time as it would need to be part of a healthcare record – e.g. the initiation of contact tracing following a positive diagnosis. The use of a security key to activate the file transfer to the HSE is a control against unauthorised access

In addition, the trigger event for the disclosure of information to the HSE once it is required allows for a timely sharing of data in a privacy respectful manner.

Alignment with Data Protection Principles

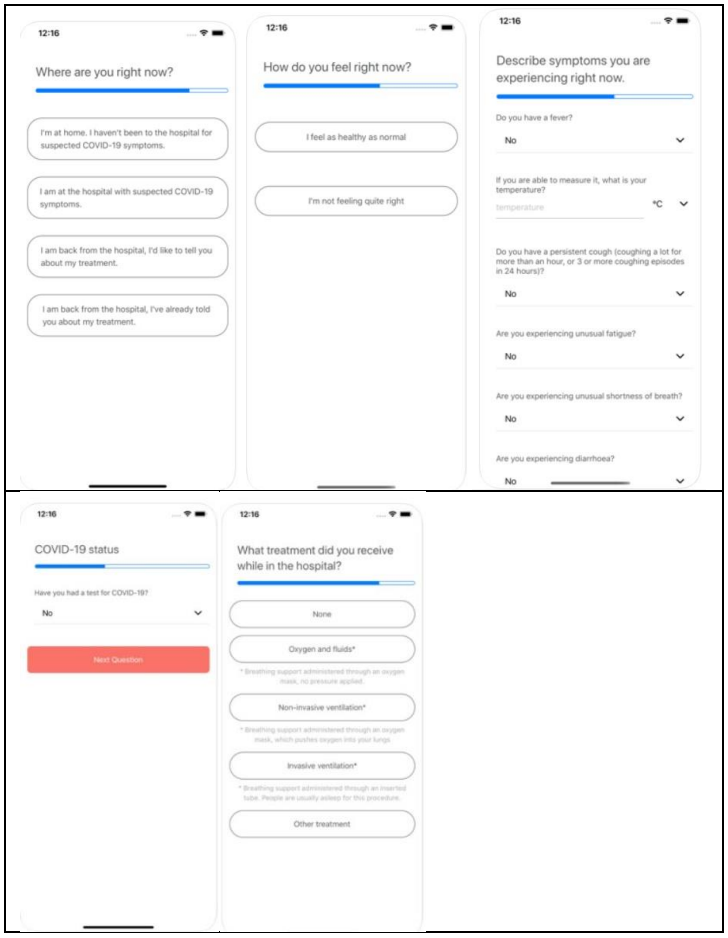
The application, as described, addresses the core data protection principles as follows:

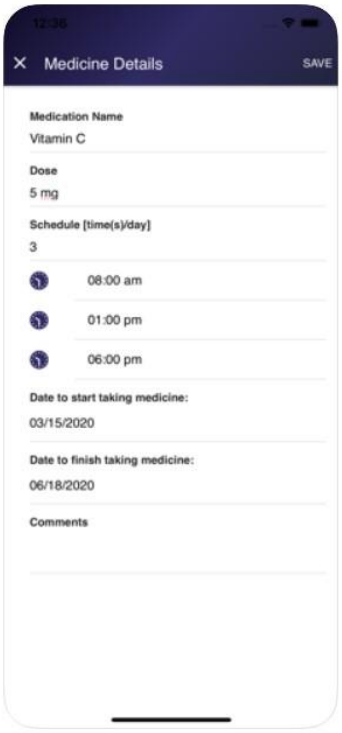
Fair, Lawful, Transparent	• Purpose of application is clearly communicated • Data cannot be obtained without data subject being aware through use of app • Clear lawful basis for processing (other than just consent) exists
Purpose Specification	• Application can only be used for one purpose • Once data has been linked for contact tracing, continued use of data for internal public health purposes would be compatible purposes
Adequate, relevant, limited to what is necessary	• Only data that approximates proximity of contact and duration of contact is processed • Only mobile phone number is registered against a pseudonymous identifier
Accurate and, where necessary, kept up to date	• The app logs data in real-time when active. • If user changes phone or phone number, they are treated as a new registrant and historic data is deleted from old device after 21 days.
Kept in a form that identifies data subjects for no longer than is necessary	• Logging data is recorded in a pseudonymous format • User registration data (mobile phone and identification key) are retained for as long as is deemed necessary – this requires a formal retention period to be defined. • 21 day retention period for on-device data is claimed but not implemented • Once linked and reidentified for contact tracing, retention is defined by HSE data retention schedule.
Integrity and Confidentiality	• Data is stored in encrypted form on-device • A verification code is required to allow data to be transferred to public health authority • Once data is processed for contact tracing, HSE data security and confidentiality controls apply as data is off-device and out of the application.

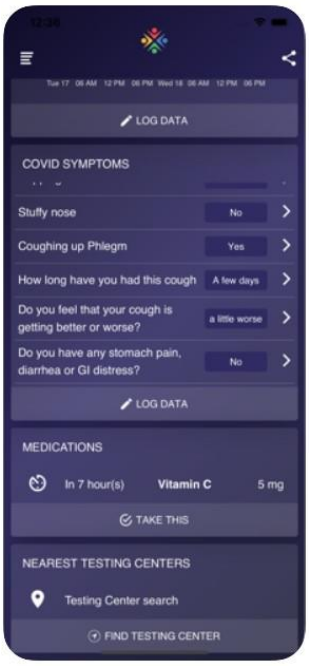
Appendix 3: Screenshots from Symptom Tracing Apps

Castlebridge reviewed two Symptom Tracking applications as part of this research review. These screenshots are sourced either from the application itself or from the Apple Appstore page for the application. It must be noted that there is a substantial transparency deficit in many of the Covid-19 symptom tracker applications.

Covid19.Zoe







[i] Source: Data Protection Commissioner Guidance on DPIAs: https://dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments

[ii] Failure Mode and Effects Analysis is a standard process analysis tool used in quality management systems initially developed by the US military in the 1940s and forming the basis of quality management systems such as Total Quality Management and Six Sigma. The objective of an FMEA analysis is to support a cross-functional assessment of the things that might go wrong in a proposed process (Failure Modes) and the likely impacts or consequences of these failures (Effects). Failure modes are prioritised based on the severity of their impact, the likelihood of their occurrence, and the likelihood that they can be detected (and therefore prevented or mitigated). Further information on the FMEA methodology can be found at the American Society for Quality (ASQ.org).

Castlebridge has adapted the FMEA approach from quality systems to apply to the objective assessment of issues arising in data protection assessments. This adapted methodology explicitly recognises impacts on individuals and on the organisation in respect of an identified risk materialising. This allows for risks to be prioritised accordingly for treatment in any remediation plan or preventative definition of controls as part of a DPIA. This methodology is proprietary to Castlebridge and has used in a number of DPIAs for public sector projects since 2012. Training in the methodology has also been delivered extensively to Public Sector organisations and government departments either in-house or through Public Affairs Ireland. The methodology is also taught on the Law Society Certificate in Data Protection Practice since 2013 and in the UCD Sutherland School of Law Diploma in Data Protection and Governance

[iii]