DIGITAL CONTACT TRACING PRIVACY IMPACT ASSESSMENT REPORT

11 May 2020

Absolutely Positively Wellington City Council
Me Heke Ki Pōneke

DIGITAL CONTACT TRACING
PRIVACY IMPACT ASSESSMENT
CONTENTS

DOCUMENT SIGNOFF

Name	Role	Signature	Date
Sean Audain	City Innovation Lead	S.	11 May 2020
James Roberts	Chief Digital Officer	JR	12 May 2020

DOCUMENT HISTORY

Version	Date	Author	Revision Description
0.1	11 May 2020	Sean Audain	Initial Draft
0.9	12 May 2020	Sean Audain	Submitted
1	12 May 2020	James Roberts	Recommendations agreed

REFERENCE DOCUMENTATION

Ref.Doc N.	Title	Version	Date	Author
1	RIPPL Presentation to MOH	For S A	6 May 2020	RIPPL
2	Memo 30 April		30 April	Sean Audain
3	Memo 6 May		6 May	Sean Audain
4				
5				
6				
7				
8				
9				
10				

1 DIGITAL CONTACT TRACING

1.1 Purpose

With the move to Level Two Pandemic Alert the focus of the New Zealand Governments COVID19 Eradication Strategy has moved to contact tracing. The activity of contact tracing is carried out by the Ministry of Health and teams within regional public health. The role of Council is to support these agencies with their tracing efforts by providing access to a record of those who have visited Council's sites and facilities. The basis of this tracing system is a manual registration system. Any Digital Contact Tracing application or system sits alongside this as an option for those who wish to use it. As can be seen from the approach to the technology (memorandum 30 April – attached) and options assessment (memorandum 6 May) privacy is core to the success of this project. In order to maintain effectiveness, confidence and trust in any digital tracing system, the two core outcomes must be privacy by design and effectiveness for contact tracers.

This privacy assessment has been conducted on the selected option as an assurance that Wellingtonians that choose to use Council's selected Contact Tracing System can be connected to public health contact tracers knowing that their data will not be used for any other private or public purpose. Because of the whole of city approach to this project this assessment will evaluate Rippl based on use across a number of organisations, contexts and environments

2 SCOPE OF THE PIA

2.1 Scope

This PIA covers:

1. The proposed Digital Solution Rippl
2. The use of RIPPL across Council Facilities
3. The use of RIPPL across Community Organizations
4. The Use of RIPPL across businesses and visitor attractions in Wellington.
5. This assessment does not cover the use of manual registration systems or any other data systems used by council
6. This assessment does not cover the systems used by Health Authorities once the data is transmitted to them from users.

2.2 The process

This PIA was completed using information provided by Rippl and sourced from the Office of the Privacy Commissioner. This information was accessed Saturday 9 May.

2.3 2.3 Explain the scope and process

The rational for the whole of city scope of this PIA was that people in Wellington were likely to encounter a digital tracing solution in a number of places across Wellington. Because of the number of organisations involved in managing these different environments it was determined that a single frame of reference was needed so that people could understand that their information was meeting clear and protected privacy expectations.

3 PERSONAL INFORMATION

Rippl works by a user scanning a QR code which creates a record of a time and place in a person's phone. When the person leaves the place they check out giving the duration. These three pieces of data are assembled into a record which is kept on the person's phone. Should that person test positive for COVID 19 they can then provide this record of places, times and duration to Contact Tracing in Public Health. If this data is of interest to the public health tracer they then send a push notification with a key which will notify all those who were in the same place at the time of interest. These people then provide their contact details to contact tracers assisting them to do their work. This creates a data relationship directly between the user and the contact tracer, with the place as common entry allowing registers to be made by place, without those facility owners having to develop systems and training for sensitive information during a time of pressure.

During day to day operation there is no personal contact data stored in Rippl. The location times, and durations could be used to identify someone if combined with other data that might be present on the phone. The protection of this data relies on the cyber and physical security of the phone to protect it.

During Contact Tracing the user gives public health their name, contact phone number, email address and any other data the contact tracer might request. This is transmitted with encryption and with the explicit consent of the person. This data is not stored in the app, but is stored in a receiving database for use by contact tracers. The protection of this data relies on transmission encryption. By collecting the data at the time it is required it mitigates the security risk of storing data, and ensures it is up to date, and the reason for collection is clear to users.

If a Premises of interest is generated by contact tracing a notification is sent to the contact for the business/facility/venue concerned to assist them in gathering manual and other records for assisting contact tracing. These contact details are held secure by PaperKite and are not in the user app.

The information that is held in the app is held by the user for as long as they wish. The information transmitted to contact tracers is held according to the Ministry of Health guidelines and rules for contact tracing.

4 PRIVACY ASSESSMENT

The principles in the Privacy Act provide the legal framework that your organisation has to consider. This section lets the decision-makers see at a glance whether the policy or proposal will comply with the law.

Each row in the following table summarises the key requirements of each of the privacy principles and outlines some key questions or considerations you should address. A risk assessment table can help you identify the privacy risks relevant to your initiative.

The accompanying Risk and Mitigation Table (see Appendix B) provides a more detailed explanation of how the project fits with the privacy principles. Either cut and paste from the Risk and Mitigation Table into this section of the PIA Report (and then omit those details from the "Risk assessment" section of this report, to save repetition), or provide a brief overview here and then expand on it in the "Risk assessment" section.

It is still useful to consider the privacy principles even if your agency is one of the few that doesn't have to comply with the Privacy Act (for instance, if you're a news agency collecting, using or publishing information for news purposes; or you're a court or tribunal exercising judicial functions). Your activity may be legally compliant, but understanding how the Privacy Act deals with a matter can better inform you as to the likely privacy impacts of your proposal, and how privacy concerns can best be accommodated.

#	**Description of the privacy principle** *(These can be deleted from your final report if they're not relevant to your project – but you should at least consider each principle)*	**Summary of personal information involved, use and process to manage**	**Assessment of compliance**
1	Principle 1 - Purpose of the collection of personal information Only collect personal information if you really need it	*The purpose of the information is to assist public health contact tracing. The information is required under level 2 contact tracing requirements. The requests for information come directly from contact tracers minimising and targeting data collection*	*The project is compliant* *By creating a direct data relationship between the user and public health at the time it is needed this reinforces the purpose for collection.*

2	Principle 2 – Source of personal information Get it directly from the people concerned wherever possible	*The information is collected directly from the individual. The information is transmitted, on request and consent, directly to Public Health Contact Tracing. This minimises the exposure of the data to businesses, other public servants and community groups*	*The project is compliant* *By restricting the data relationship to those providing the information to those having the need and purpose for the information it protects against misuse both within Council, but also other organisations such as retailers, venues and attractions.*
3	Principle 3 – Collection of information from subject Tell them what information you are collecting, what you're going to do with it, whether it's voluntary, and the consequences if they don't provide it.	*The collection of location information is explained in the apps Privacy Policy. It is clear that it does not store personal information, use location services or use GPS data. The act of scanning qr codes means the user should be conscious of data collection. The user can also see this data themselves. Council has also been certain to include that the app is voluntary in all communications to make people aware that they do not have to use this service.* *The consequences and nature of data provision are made clear by contact tracers in their requests for information from people.*	*The Project is compliant* *The conditions are available in the app and on the website. The technology and support systems are agile enough to change should the requirements or consequences for information change.*
4	Principle 4 – Manner of collection of personal information Be fair and not overly intrusive in how you collect the information	*The information is collected in a proportionate way, requiring only location and time data under ordinary operation. If this proves of interest to contact tracers then further data is requested. This minimises data collection and means data is collected at the time it is most needed*	*The Project is compliant* *The data is collected under clear expectations that act to minimise collection and exposure of data.*

5	Principle 5 – Storage and security of personal information Take care of it once you've got it and protect it against loss, unauthorised access, use, modification or disclosure and other misuse.	*Under day to day operation the only data stored within the phone is the time, duration and location of check ins. This data is protected by the physical security of built into the telephone and the digital security encryption built into the app. Further encryption keys are used in the creation of the QR codes to protect against people producing spoof codes to access peoples data.* *Contact details are protected by not being collected until needed, and when needed they are transmitted to Regional Public Health using encrypted data transfers, protecting the information against interdiction* *The storage of the data within Regional Public Health is protected by the security and policies of the Ministry of Health and District Health boards* *The security of the information, and protection of the information within the organisations using Rippl is mitigated by creating a direct relationship between user and contact tracer, meaning the information is not accessible to other organisations.*	*The Project is compliant* *By keeping peoples data with them and targeting input and transmission to Contact Tracers when it is required, the potential for misuse or loss of data by third parties is minimised.*

6	Principle 6 – Access to personal information People can see their personal information if they want to	*By keeping a person's information with them and under their control this means this information is always visible and transparent to them. By seeking active consent to transmit data to contact tracing this creates a clear hand over from one system and governance set to another.*	*The Project is compliant*
7	Principle 7 – Correction of personal information They can correct it if it's wrong, or have a statement of correction attached	*A person provides their personal information to contact tracing at the time it is requested. If this needs to be amended it would be done under the processes of the Health Agency.* *The location data can be corrected/added to during the Contact Tracing Interview process.*	*The Project is compliant*
8	Principle 8 – Accuracy etc. of personal information to be checked before use Make sure personal information is correct, relevant and up to date before you use it	*By transmitting the information at time of use it will be up to date and relevant to time of use. If the information provided is incorrect this can be addressed by users at the time with Contact Tracing.*	*The Project is compliant*
9	Principle 9 – Not to keep personal information for longer than necessary Get rid of it once you're done with it	*The app keeps location and check in data for the duration the user chooses. The collection of personal contact details is minimised to a situation when they are required, and are not stored once transmitted to Contact Tracing in the app. Contact Tracing will hold the information according to their policies and procedures.*	*The Project is compliant*
10	Principle 10 – Limits on use of personal information Use it for the purpose you collected it for, unless one of the exceptions applies	*This system is designed to minimise the potential uses of information by ensuring that the user provides it directly to Regional Public Health. By collecting contact details at the time they are required the purpose and need is clear.*	*The Project is compliant*

11	Principle 11 – Limits on disclosure of personal information Only disclose it if you've got a good reason, unless one of the exceptions applies	*Council, or another premises cannot disclose the information as it is not held by us. Disclosure to Contact Tracing is by the user, further disclosure is managed by Contact Tracing.*	*The Project is compliant*

4.1 Summary / Conclusions

In summary the project complies with the principles of the Privacy Act. Given this is novel use of technology, in a pandemic emergency and contact tracing apps have faced criticism in other nations it is recommended that:

- A copy of the approved Privacy Assessment is made available proactively on the Council's website
- A further independent security review is undertaken
- That should this situation continue beyond three months, or changes to app functionality be proposed that a further PIA process take place
- That a plain English summary of how the app works be made available to the public.

5 RISK ASSESSMENT

The major risk is that the lack of definition of digital contact tracing, the technologies that underpin it and the very different privacy implications of systems and methods make this a difficult thing to explain to the public and generate informed use. This risk is further compounded by criticism of tracing apps in other jurisdictions and a burgeoning market for digital solutions. Whilst privacy techniques like collection minimisation show the commitment of this solution to privacy by design there is still a residual cybersecurity risk due to the transmission of data.

6 RECOMMENDATIONS TO MINIMISE IMPACT ON PRIVACY

Ref	Recommendation	Agreed Y/N
R-001	- A copy of the approved Privacy Assessment is made available proactively on the Council's website	Y
R-002	- A further independent security review is undertaken	Y
R-003	- That a plain English summary of how the app works be made available to the public.	Y
R-004	- That should this situation continue beyond three months, or changes to app functionality be proposed that a further PIA process take place	Y

7 ACTION PLAN

Ref	Agreed action	Who is responsible	Completion Date
A-001	- A copy of the approved Privacy Assessment is made available proactively on the Council's website	Smart Council	
A-002	- A further independent security review is undertaken	Smart Council	
A-003	- That a plain English summary of how the app works be made available to the public.	Communications	
A-004	- That should this situation continue beyond three months, or changes to app functionality be proposed that a further PIA process take place	Smart Council	