Privacy Impact Assessment Questionnaire

Human mobility insights

This checklist is to be completed by the responsible Business Owner or Project Manager. This must be done as early as possible in the planning process, for:
1.   All new IT systems or key business processes
2.   Any changes to IT systems or key business processes.
Note, for the purposes of this assessment, personal information is any information that relates to an identifiable individual. It does not have to include their name or contact details to be personal information.
If you do not believe that the change you are assessing involves or impacts on any personal information, then please provide your rationale for this in the summary of change section below.

Business Unit	Service Strategy & Partnerships
Sponsor	Justine Haves
Date Completed	10 Aug 2022

Summary of Change

Service Strategy and Partnerships is seeking insights about our customers based on anonymised mobile-application data, to address gaps and inconsistencies in our current evidence based for community investment advice. Two potential providers have been identified, both providing Software as a Service products (i.e. websites on which the information can be accessed).

There is no desire, intention or need to pass any information about customers to these providers. The only Council information they would store are geospatial files describing the boundary of publicly known facilities (e.g. Tepid Baths) and parks.

The company 'Pathzz' is the preferred vendor based on functional requirements and does not provide any personal information. All information products provided by Pathzz through their service are aggregate statistics and can not be used to identify an individual. This includes: 1) Estimated number of visits and unique visitors for specific locations and times 2) Broad geographic areas (SA1) those visitors are estimated to live in 3) Estimated aggregate demographics of visitors to those locations 4) Popular places frequented by visitors to those locations.

Pathzz data is being tested for accuracy. If this is unsatisfactory, a back-up vendor is Near Intelligence. This vendor provides both aggregate data and mobile-device level information about the location and time of devices. The business unit considers this is not personal information, but advice is sought on this matter. A point of comparison is survey-based insights, which Council obtains for similar purposes to the data under consideration here. In some survey data paid for by Council, details such as age, gender, ethnicity and home suburb are collected from individuals, are connected to one another for the same individual and supplied to Council (but without contact details). By way of contrast, no details about individuals other than the time and location of a device and any analysis of this, would be obtainable through Near.

Assessment Questions

What personal information will be involved?

Existing information

Provide a summary of any personal information we already hold that will be used in the change. This could be about customers, staff, stakeholders or other individuals. Confirm the original purpose that this information was collected for.

None – no personal information will be used.

New information

Provide a summary of any new personal information we will be collecting about individuals as a result of the change. Provide reasons why we need this new information for this change.

None – no personal information will be used.

Is any of the information likely to be sensitive?

Provide details of any information involved in the change that is likely to be viewed as sensitive by the individuals that it relates to.

For the preferred vendor Pathzz, no individual information will be accessible by Council. Some information may be deemed commercially sensitive such as the level of foot traffic at our leisure facilities.

For the back-up vendor Near, no personally identifiable information is accessible by Council. This vendor does provide mobile-device level information about the location and time of that device however that could potentially be viewed as sensitive as if combined with specific information from other sources (e.g. home and work address an individual), an individual could theoretically be identified. There are no other details about specific devices or the device owners available to Council through this vendor other than what can be deducted from the timestamped location of devices.

Where did we get the information from?

Individual
What information are we collecting directly from the individual involved? For this information, how have we made sure that the individual understands what we are collecting and the purpose that we are collecting it for?

None.

Direct third party
What information are you collecting from a direct third party about individuals? Outline why it is being collected from them and what consent/authorisation you have to do so.

Information collected

1. Current preferred vendor Pathzz None – information is aggregate only, not at an individual level, e.g. tables with the estimated number of visitors to a specified location over a specified time, estimated proportion that are male, female etc. Data accessed by Council comes from mobile application publishers. Pathzz privacy policy can be accessed below however note that information they hold referenced in this statement 'precise geographic location of a device at a certain

time' is not accessible to customers using their SaaS product: https://www.pathzz.com/privacy-policy

2. Alternative vendor Near.com Geographic location of mobile devices over time. Based on these data, where possible the vendor additionally estimates the SA1 within which is the home location of the device owner as well as the common day-time location (SA1s are typically home to 100-200 people and up to 500). No details about the device operator or owner are attached such as names, email, addresses, phone numbers, age, gender or any other personal attributes. Other information provided by this vendor is aggregate only, not at an individual level, and not linkable to mobile devices e.g. tables with the estimated number of visitors to a specified location over a specified time, estimated proportion that are aged over 65 years etc.

Near privacy policy: https://near.com/privacy-policy/#business-policy

Why it is being collected

See Strategic Assessment

Consent/authorisation

Consent is granted by the device operator within mobile applications via terms and conditions and additionally opting in to share their location – if refused the device is not included in the data. Both providers claim data is obtained via consumer consent at source in this way, however there are many different mobile applications (claimed to be in excess of 250,000 from one provider) supplying the data through commercial arrangements with the vendors and we are not privy to which apps these are.

Other third party

What information are we collecting from other third-party sources? List the source(s) and outline why it is being collected from the source and what consent/authorisation we have to do so.

As noted above, some data comes to the vendor through commercial agreements we are not privy to.

Where are we storing the information?	*Provide details of the system/location where information will be stored, including whether it will be hosted in the cloud. If the information will be stored outside our environment, provide details of where and what contractual arrangements are in place.*

1. Pathzz

The vendors website which we would access is hosted on a server in Australia. The vendor has signed a Data Sharing Agreement regarding geospatial files we have supplied to them, though these geospatial files are not sensitive information. No other Council data will be stored on their application.

Once data is downloaded by Auckland Council staff, it will be stored in the general folder structure as it is non-sensitive.

2. Near

The vendors website which we would access is hosted by Amazon Web Services in the USA. The vendor has signed a modified Data Sharing Agreement regarding geospatial files we have supplied to them which is being reviewed by our legal

services, though these geospatial files are not sensitive information. No other Council data will be stored on their application.

Auckland Council ICT to advise on storage however its proposed device-level data is stored securely with access restricted to a small number of analysts who would read and sign an agreement about the handling of this information.

How are we keeping the information safe?	*Provide details of security controls that are in place to protect the information. If a security risk assessment or penetration testing has been completed, provide a summary of the outcomes here.* As we are not storing sensitive Council information via this application, it is proposed the main security requirements are around appropriate access to the information stored at Auckland Council.
How will people be able to access and correct their information?	*Provide details of how individuals will be able to access and correct their information. Will it be through standard/existing processes or will additional steps need to be put in place?* They will not be able to access and correct their information because even in the case of our back-up vendor 'Near' there are no personal details in the data (e.g. no name, email address nor phone number) that could be used to link a specific device to a person.
How do we know personal information is accurate before we use it?	*Provide a summary of any validation/accuracy controls that are being put in place to check personal information is accurate before it is used or disclosed* Not applicable – no personal details are included.
How will the information be used?	*Provide a summary of how personal information will be used in the change. For example, if we are using information to assess an individual's eligibility for a service and then delivering it, outline what information is being used for assessing the eligibility and what is required to deliver the service.* Not applicable
	Will there be any areas where we use algorithms or automated decision making? No
	If the information is being used for research/analysis, will individuals be identifiable during the analysis or in the outputs? Individuals will not be identifiable in any planned outputs, however an analyst could derive an individuals identity in the analysis if they combine this with other information such as an individuals home and work address.
Do we have the right permission or basis to use it for this?	*Do we have consent/authority or a legal basis to use the information in this way? If so, provide the details here.* See above 'Where did we get the information from?' on the topic of consent.
	How have we communicated to individuals how we will be using their information?

We have no way of contacting individuals from whom the data is derived.

Are we going to be sharing the information with anyone else?	*If so, list all parties who will have access to information, what information they will have access to and why they need to have it?*
	Non-sensitive summary information – tables, charts, commentary – will be available to a wide range of Council staff and elected members. If contracting Near, only a small set of analysts would have access to the data. Currently:
	- Insights & Strategy Lead – Customer & Community - Customer & Community Insights Specialist - Principal Asset Spatial Advisor - Senior Asset Spatial Advisor (1-2 of 3 roles)
	Do we have consent/authority or a legal basis to share the information in this way? If so, provide the details here.
	See above 'Where did we get the information from?' on the topic of consent.
	Provide details on what safeguards have been put in place to provide us with assurance that the information will be protected by the people/organisations we are sharing it with.
	Pathzz and anlaysis outputs – no additional safeguards required beyond principals and processes set out in [We Keep Our Information Safe](#). If Near is contracted, downloaded data files to be password protected and proposed that analysts that are given access to this read and sign an agreement about handling this information, including not providing access to unauthorised parties (authority to be specified in document), where and how files must be stored.
What will we do when we don't need the information any longer?	*Do we know how long we will need to retain the information for? Why is it for this period?*
	Pathzz data downloaded to Council and any summary outputs to be subject to ordinary [Council record keeping procedures](#). If Near is contracted, device-level data downloaded could be deleted after 12 months to provide sufficient time for analysis and any re-analysis to be conducted.
	How will the information be disposed of when it is no longer required?
	TBC
Are we using unique identifiers?	*Are we using any specific unique identifiers for individuals as a part of this change (i.e. Passport, Driver Licence)? If so, provide details of what and why we are using them.*
	No

Auckland Council, Private Bag 92300, Victoria Street West, Auckland 1142 — Tel: 09 301 0101 — www.aucklandcouncil.govt.nz

Privacy Impact Assessment Questionnaire   5