

Traveller Journey Index

New Zealand Traveller Declaration

PRIVACY IMPACT ASSESSMENT

August 2023

Product owner: [REDACTED]

V1.1

PROACTIVELY RELEASED

Contents

Document management.....	2
Version history	2
Distribution list for external distribution.....	2
Glossary.....	3
1. Introduction and purpose	7
2. PIA scope.....	10
3. Executive risk summary	10
4. Openness and transparency	11
5. Personal information involved	11
6. Assessment of privacy impacts.....	12
6.1 Collection of personal information.....	12
6.2 Storage and security	17
6.3 Access, correction and accuracy.....	18
6.4 Retention, use and disclosure	21
6.5 Offshoring of information.....	24
6.6 Unique identifiers	25
7 Risk, consultation and signature.....	26
7.1 Consultation	26
7.2 Signatures	26
Appendix 1 – Information flow Traveller Journey Index	27
Appendix 2 – Project Risks and Controls table	28
Appendix 3 – Changes since version 1.0.....	31

PROACTIVELY RELEASED

Document management

Version history

Version	Date	Author and role	Description
0.1	20/10/23	[REDACTED] Business Analysis Lead	Initial draft
0.2	10/11/23	[REDACTED] Business Analysis Lead	Updated based on review comments
0.3	15/03/23	[REDACTED] privacy analyst	Redrafted following internal changes project team
0.4	15/03/23	[REDACTED] privacy analyst	Updated to reflect feedback from Business Analysis Lead
0.5	17/03/23	[REDACTED] privacy analyst	Updated to reflect feedback from Principal Privacy Advisor (ISP)
0.6	21/03/23	[REDACTED] privacy analyst	Updated to reflect feedback from Product Owner
0.7	23/03/23	[REDACTED] privacy analyst	Updated to reflect feedback from Product Owner
0.8	31/03/23	[REDACTED] privacy analyst	Updated to reflect feedback from partner agencies
0.9	03/05/23	[REDACTED] privacy analyst	Small editing changes
1	03/07/23	[REDACTED] privacy analyst	Final version
1.1	22/08/23	[REDACTED] privacy analyst	Small editing changes – see Appendix 3

Distribution list for external distribution

Version	Date	Recipient email address	Reason for sending
# sent	sent		
0.7	24/03/23	[REDACTED]	Feedback
0.7	24/03/23	[REDACTED]	Feedback

--	--	--	--

Disclaimer and assumptions

This PIA has been prepared by the New Zealand Customs Service - Te Mana Ārai o Aotearoa (Customs). Customs is the lead agency for the New Zealand Traveller Declaration and works closely with Ministry of Business, Innovation and Employment (MBIE) and Ministry for Primary Industries (MPI) to deliver the online system.

This PIA has been prepared to review the privacy implications of the Traveller Journey Index for the New Zealand Traveller Declaration (NZTD) and whether this complies with the Privacy Act and related Information Privacy Principles.

This PIA reflects the operation of the Traveller Journey Index as it is currently envisaged. It is intended to be a “living document” and will be regularly updated to reflect changes that arise as the NZTD is progressively rolled out and adapted to respond to changes in the broader environment.

Updating the PIA to reflect changes will be the responsibility of the product owner.

A version of this PIA will be made publicly available alongside the communication collateral deployed with the NZTD. This will support the public to understand the collection, storage, use and sharing of personal and third-party information. This is a transparency decision, intended to support public trust in the operation of the NZTD.

Glossary

Abbreviation	Meaning
ANA	Advance Notice of Arrival The person in charge of a craft that is en-route to New Zealand (from a point outside New Zealand) must, within the prescribed time, provide Customs with an advance notice of arrival, unless otherwise approved by the chief executive.
API	Advance Passenger Information For security reasons, most countries require airlines to provide details about their passengers before they travel. This is known as Advance Passenger Information (API).
APP	Advance Passenger Processing If notified of the requirement to do so, airlines must provide Advance Passenger Processing information to the Chief Executive of MBIE (Immigration NZ) about every passenger and crew member on their flights coming to or leaving New Zealand.
BDF	New Zealand Travel Declaration - Border Decision Framework

	<p>A framework that sets in motion a risk assessment of travellers to New Zealand. BDF is an assessment of a traveller declaration against rules; it does not do the actual risk assessing itself.</p>
Biometric information	<p>Biometric information, in relation to a person, means information that comprises—</p> <p>(a) 1 or more of the following kinds of personal information:</p> <p>(i) a photograph of all or any part of the person’s head and shoulders:</p> <p>(ii) impressions of the person’s fingerprints:</p> <p>(iii) a scan of the person’s irises; and</p> <p>(b) an electronic record of the personal information that is capable of being used for biometric matching</p>
Border agencies	<p>The border agencies are New Zealand Customs Service, Ministry for Primary Industries for Biosecurity New Zealand and the Ministry of Business, Innovation and Employment for Immigration New Zealand.</p>
Category of information	<p>Section 304 of the Customs and Excise Act 2018 defines two categories of information in regards to disclosures:</p> <p><i>Category 1 information</i> means any information held by Customs,—</p> <p>a) including information relating to—</p> <p>(i) persons:</p> <p>(ii) goods:</p> <p>(iii) craft; but</p> <p>b) excluding Category 2 information</p> <p><i>Category 2 information</i> means—</p> <p>a) the following information in relation to any person:</p> <p>(i) arrival and departure information:</p> <p>(ii) biometric information:</p> <p>(iii) passenger name record information; and</p> <p>b) intelligence assessments and reports generated by Customs</p> <p>Section 41A of the Biosecurity Act refers to the following definition of border information:</p> <p>border information—</p> <p>(a) means information—</p> <p>(i) that is required to be supplied to the Ministry or the Customs by or under this Act or the Customs and Excise Act 2018, or both, for a border protection purpose; or</p> <p>(ii) that is otherwise lawfully supplied or collected for a border protection purpose; and</p> <p>(b) includes, without limitation, information about—</p>

	<p>(i) goods, persons, or craft:</p> <p>(ii) import or export transactions:</p> <p>(iii) importers or exporters; and</p> <p>(c) also includes data or information that is derived from, or related to, any information referred to in paragraphs (a) and (b) or any analysis of that information</p>
Customs	New Zealand Customs Service - Te Mana Ārai o Aotearoa
CusMod	Customs' primary system for border management that records every movement of passengers, goods and craft across New Zealand's border. CusMod processes advanced passenger, goods and craft information to facilitate legitimate trade and travel.
DIA	Department of Internal Affairs - Te Tari Taiwhenua
DOB	Date of birth
INZ	Immigration New Zealand, a part of the Ministry of Business, Innovation, and Employment
IPP	Information privacy principle under section 22 of the Privacy Act
MBIE	Ministry of Business, Innovation and Employment - Hikina Whakatutuki
MoH	Ministry of Health, Manatū Hauora
MPI	Ministry for Primary Industries – Manatū Ahu Matua
NZeTA	<p>New Zealand Electronic Travel Authority</p> <p>An electronic visa waiver allowing eligible citizens to travel to New Zealand for tourism, business, or transit purposes.</p>
NZTD	New Zealand Traveller Declaration
Orchestration system	The harmonious coordination and arrangement of diverse components and processes within a complex system to achieve a desired outcome. It entails the integration and management of various interconnected elements, such as hardware, software, data, and human resources, in a synchronized manner, akin to a conductor skillfully directing a symphony orchestra.
Personal information	<p>Personal information</p> <p>(a) means information about an identifiable individual; and</p> <p>(b) includes information relating to a death that is maintained by the Registrar-General under the Births, Deaths, Marriages, and Relationships Registration Act 1995 or any former Act (as defined in section 2 of the Births, Deaths, Marriages, and Relationships Registration Act 1995)</p>

PIA	<p>Privacy Impact Assessment</p> <p>A tool used by agencies to help identify and assess the privacy risks arising from the collection, use or handling of personal information. A PIA will also evaluate ways to reduce privacy risks.</p>
PNR	<p>Passenger Name Record – generated at the time of the booking and consists of the passenger's personal and journey details.</p>
Pre-travel manifest	<p>A manifest is a document listing the cargo, passengers, and crew of a ship, or aircraft for the use of customs and other officials. Where such a list is limited to identifying passengers, it is a passenger manifest or passenger list.</p>
Primary line	<p>The primary line is the point in the arrivals hall where the traveller presents their passport to either an officer at the booth or an eGate. This is also the point where an application for a visa and/or entry permission may be made.</p>
Privacy Act	<p>Privacy Act 2020</p>
Rules engine	<p>A rules engine is a software system that manages business rules. A basic example of a business rule would be 'If A, then B, else if X, then do Y'.</p>
Secondary line	<p>A place where travellers may be directed for further interaction with a border official because an assessing officer considers further questioning or an inspection is required.</p>
SITA	<p>IT provider for the air transport industry, delivering solutions for airlines, airports, aircraft and governments.</p>
Third-party information	<p>Information collected by an entity that does not have a direct relationship with the user the data is being collected on.</p>
TJI	<p>New Zealand Traveller Declaration - Traveller Journey Index</p>
UI	<p>User Interface</p>

1. Introduction and purpose

This Privacy Impact Assessment (PIA) will assess the *Traveller Journey Index* for the New Zealand Traveller Declaration and whether this complies with the Privacy Act and related Information Privacy Principles (IPPs). It explains the process followed, the factors considered and the steps that will be taken to ensure the privacy of travellers to New Zealand will not be adversely affected by the use of this Traveller Journey Index (TJI).

The New Zealand Traveller Declaration (NZTD) is an online system for travellers to complete a declaration before they travel to New Zealand and answer questions for Customs, Immigration and Biosecurity¹². The NZTD will be an alternative to the paper-based passenger arrival card.

The aim is to modernise the border, help passengers move through airports more efficiently, and improve the safety and security of New Zealand by being able to assess passenger information earlier in their journey. This will support increased compliance by passengers and the ability to identify non-compliant passengers earlier.

It is estimated that by 2025, more than 18 million travellers will have used NZTD across air and maritime ports.

The Traveller Journey Index (TJI) is a centralised data orchestration system. The TJI records references to data stored in their proprietary systems. It captures the references for a journey record for a single unique journey made by a traveller. It is the core system component that orchestrates the validation of assertions made by the traveller and facilitates the BDF to complete a rules engine assessment to assist with processing at the Primary Line of the traveller upon reaching New Zealand.

TJI does not join journeys over time and is only used to facilitate a specific voyage, i.e. it does **not** create an explicit historical database of an individual's movements.

This PIA will assess the TJI for passengers arriving by airport and maritime port.

Initiative overview

Context

The TJI is the centralised data orchestration system that captures the references to a unique journey record for a single journey made by a traveller. This unique journey record is identified by the biographic details of a traveller along with the voyage details.

The TJI contains:

- Biographic details of a traveller.
 - name, DOB, sex
- passport details.
- Flight / voyage details.

¹ There are currently no Ministry of Health (MoH) requirements active in NZTD but the processes and systems have been established to enable the management of health requirements at the border to minimise health risks as we saw during the recent COVID-19 pandemic.

² The arrival card serves multiple purposes for multiple border agencies. For more information, please refer to the PIA on the Digital Traveller Declaration.

- References³ to other components that relate to a particular journey.
- Traveller Interactions at the border⁴.

Once a traveller declaration has been submitted by (or on behalf of) a traveller, the TJI will validate the information provided by the traveller about their eligibility to enter New Zealand by triggering the data enrichment service:

- *Non- New Zealand citizens* - If the traveller is a non-New Zealand citizen, the data enrichment service will query INZ visa services to gather the visa status of the traveller.
- *New Zealand citizens* - If the traveller has provided information that they are a NZ citizen travelling on a NZ passport, the data enrichment service will query Customs CusMod or DIA's citizenship services⁵.

TJI then triggers the Border Decision Framework (BDF)⁶ that sets in motion assessments from the border agency rules engines on a declaration once it is submitted by a traveller. The Rules Engines assessment results are stored by the BDF and enables sharing of the appropriate directives and notifications with the appropriate consuming systems.

The permission and access rights to TJI are governed by NZTD's data access policy. Border officers of appropriate agencies will only be able to see the relevant information necessary to perform their lawful functions or activities. The TJI does not enable access to an entire declaration and/or the directive outcomes from the rules engines. Instead, border officers will only be able to see the relevant information which will assist the different border agencies with processing and directing the traveller to the right pathway for processing on arrival.

The journey record will not include the rules engine assessments results. It will just include the assessment ID which is a unique reference number that identifies the assessment on that declaration in the BDF.

Draft/ unsubmitted declarations

Along with the submitted declarations, TJI creates a journey record for draft or unsubmitted declarations. These records are created to enable the contact centre agent to support the traveller⁷.

³ This includes the following information:

- Reference to the digital traveller declaration.
- Reference to border instructions (risk assessment results).
- Reference to interactions with passengers during processing (note: the NZTD only includes interaction meta-data to facilitate cross-agency coordination and traveller assistance; details of interactions are held in their respective systems).
- Results of verification checks with respect to claims made in the declaration (citizenship/visa status, credential authenticity).
- References to travel notifications for this specific journey (API, PNR, APP, ANA).
- Reference to the border-crossing movement.

⁴ Interactions that take place between a border officer and a traveller as part of Primary Line processing will be recorded in line with operational processes. They generally relate to concerns with the traveller's behaviour and/or comments made to an officer. These interactions capture details from the officer in terms of the concern and the recommended action to be taken by the operational agencies at the port. This will usually (but not always) result in subsequent secondary interventions for the traveller.

⁵ The functionality for Citizenship enrichment is yet to be built but it is anticipated that this will be completed in Aug – October timeframe.

⁶ The BDF is a mechanism where participating agencies will be able to operationalise rules and decision logic at the border. BDF is an assessment of a traveller declaration against rules; it does not do the actual risk accessing itself. For more information, please refer to PIA Border Decision Framework.

⁷ For more information, please refer to PIA Whare Āwhina.

There will be no enrichment data collection or rules engine assessments performed on these draft or unsubmitted declarations.

No declaration submitted by traveller

If the traveller does not submit a digital traveller declaration, there are other mechanisms by which the TJI will create a journey record, such as:

- If there is no declaration from the traveller at the point of check-in, data from Advanced Passenger Processing (APP) will create an orphan shell journey record based on the travel ticket the traveller has purchased. This record will then get linked to the declaration when a traveller creates a traveller declaration upon arrival.

If a traveller arrives at the Primary Line without having completed a digital traveller declaration, a paper-based passenger arrival card will be available. Border officers at the Primary Line may create an interaction, which will be stored in TJI. When TJI receives the movement record from the existing Customs application CusMod⁸, an orphan shell journey record will be created. There will be no enrichment or assessment performed on these orphaned declarations and these will be deleted according to the NZTD data retention policy.

The paper-based passenger arrival card will be digitised, ingested and stored in the Declaration Service. Once this action has been completed TJI will be notified to update its reference data.

Declaration submitted by traveller who does not come to New Zealand

Another way for an orphaned declaration to be created is if a traveller submits a declaration but does not end up travelling to New Zealand on the voyage entered into the declaration. As before, these orphaned declarations will be deleted according to the NZTD data retention policy.

TJI does **not** join journeys over time and is only used to facilitate a specific voyage. The TJI does not create an explicit historical database of an individual's movements.

Appendix 1 shows the data flow for TJI.

Issues this project will address:

- The TJI is an efficient way to ensure that the border agencies have access to the information they need to assess the risk of a traveller who has submitted a NZTD.

Benefits it will bring to the border agencies:

- A more efficient operational process for border officers upon arrival.
- Less risk to New Zealand's border⁹.
- A consolidated result by the border agencies of the rules assessment for a traveller's individual journey.

Benefits to others:

- A more efficient process for travellers.

⁸ Customs' primary system for border management that records every movement of passengers, goods and craft across New Zealand's border.

⁹ Border agencies work together to protect New Zealand by reducing risks from people, goods or craft arriving at the border.

Key privacy lessons learned from NZTD Trials

Before go-live, there have been several trials of NZTD processes. These trials tested NZTD systems, processes and functionality and provided an opportunity for border staff training. One lesson from the trial was a risk that traveller confusion would result in them completing both a Digital and Paper declaration. Communication and Operational based mitigations have been put in place to minimise this risk and TJI functionality has been revised to ensure the correct declaration retains primacy.

2. PIA scope

This PIA will focus on the Travel Journey Record (TJI) and how the information gathered from a traveller will be used across NZTD.

This PIA will not cover:

- The privacy impact of the broader NZTD programme, including the choice of strategic direction of the NZTD, the policy analysis or legislative settings that reflect that direction.
- The privacy impact of the digital traveller declaration¹⁰.
- The privacy impact of the Border Decisions Framework¹¹.
- The privacy impact of the enrichment service.
- The privacy impact of Whare Āwhina¹².
- The privacy practices of the participating agencies, e.g. MPI and INZ.

3. Executive risk summary

A risk-based approach to the use of TJI is being taken. We believe that TJI best meets NZTD's needs, in the most cost-effective way, while providing adequate privacy and security protections.

The following residual risks have been identified. Controls have been put in place or are still under development. A detailed description of risks and controls can be found in Appendix 2, Project Risks and Controls table.

¹⁰ Please refer to the PIA Digital Traveller Declaration.

¹¹ Please refer to the PIA Border Decisions Framework.

¹² Please refer to the PIA Whare Āwhina.

		Consequence				
		Insignificant	Minor	Moderate	Major	Severe
Likelihood	Certain					
	Likely					
	Possible		R4	R6		
	Unlikely	R5	R1, R2	R7		
	Rare					

* R3 - Risks in regard to IPP 5 - Storage and security of personal information - The NZTD cyber security team has assessed the security risks for TJI and is responsible for the Certification & Accreditation (C&A) process and security risk assessment. For more information on security risks, please refer to the security C&A.

4. Openness and transparency

IPP 3 of the Privacy Act requires agencies to be open and transparent about the way they manage personal information. To meet these openness and transparency obligations, we will:

- Make this PIA public.
- Have a NZTD privacy statement (<https://www.travellerdeclaration.govt.nz/privacy/>) that will explain how the border agencies will collect, use and disclose personal information travellers will provide through the NZTD online form.
- Engage where required and appropriate with anyone who has particular concerns with the operation of the TJI.
- Have a dedicated website for NZTD - <https://www.travellerdeclaration.govt.nz/>

5. Personal information involved

The personal information involved falls within the following categories:

- Biographic/ identity information.
 - name, DOB, sex
- Passport details.
- Flight / voyage details.
- References to other components that relate to a particular journey.
- Traveller Interactions at the border.

TJI does not capture any data on its own; nor does it process any data. Some of the data captured by the declaration service, APP, internal UI, Port Operations passenger processing systems and CusMod

passenger (PAX) movement data are shared with the TJI along with the enrichment service data¹³ and assessment data of the Border Decision Framework.

6. Assessment of privacy impacts

This section advises on the privacy impacts of NZTD's Traveller Journey Index in consideration of the IPPs of the Privacy Act.

6.1 Collection of personal information

IPP 1 - Purpose of collection of PI
<p>Personal information shall not be collected by any agency unless:</p> <ul style="list-style-type: none">• the information is collected for a lawful purpose connected with a function or activity of the agency; and• the collection of that information is necessary for that purpose. <p><i>Information sought should be necessary for the purpose of your project. It is not enough for the information to be merely helpful or nice to have.</i></p>

1. Describe how collection matches the functions or activities of the border agencies. If there are other agencies involved as the collecting agency, describe how their purposes are met.

TJI does not collect any information directly but acts as the centralised data orchestration system that controls the different components within NZTD involved with assessing traveller's risk. The data is collected or generated by:

- NZTD declaration service
- Cruise and Airline APPs (such as ANA, SITA APP, Cruise API, Pre-travel manifest matching)
- DIA (Citizenship)¹⁴
- INZ (Visa)
- NZeTA
- Customs' CusMod movements
- Agency Rules engine assessments (INZ, MPI, Customs, Health¹⁵)
- Interaction data (e.g data collected through the Primary Line web application)

There will be a privacy statement explaining what personal information is being collected, for what purpose, which agencies will have access to this information, etc. Travellers are asked to confirm they have understood how their information is being used before submitting their NZTD. The privacy statement is also available on the dedicated website for NZTD (<https://www.travellerdeclaration.govt.nz/privacy>).

The information that is being orchestrated by TJI is essential for the operations of NZTD. The agencies accessing the data have legal authority to access the data. Controls and restrictions have been built into the design of NZTD to ensure that the agencies will only have access to

¹³ The enrichment service data is the data that is being received from either DIA on citizenship status or INZ on visa status.

¹⁴ Expected to be build in Aug – October timeframe.

¹⁵ As noted before, there are currently no Ministry of Health (MoH) requirements active in NZTD but the processes and systems have been established to enable the management of health requirements at the border to minimise health risks as we saw during the recent COVID-19 pandemic.

the data they are legally authorised to have access to, i.e. Customs will only have access to relevant Customs data, MPI will only have access to relevant MPI data, INZ will only have access to relevant INZ data, etc. The NZTD data access policy controls which agencies have access to which data points.

Agencies are responsible for establishing their lawful purposes and, if needed, updating their legislation and/or information sharing arrangements to operate in the NZTD platform. The information each agency can collect, use, and disclose should be provided for under legislation and must be validated before any access is provided by NZTD's data access policy.

2. *Describe how collection is **necessary** for those purposes.*

The information that is being orchestrated in the TJI is essential for border control agencies to be able to process the travellers' arrival into New Zealand effectively and efficiently and is legally authorised under the agencies' legislation.

3. *Risks*

There is a risk that data will be accessed by an agency under the incorrect assumption that this agency has a legal authority to access this data.¹⁶

4. *State any policies / processes that exist, or may need to be developed, to achieve or maintain consistency with IPP 1 or to mitigate risks.*

Extensive work has been done by the project team assessing and validating the legal authority for all the information that will be collected by NZTD. If any of the agencies wants to have access to any of the other data points, they will need to establish their legal authority and submit a business case to request access.

Any sharing of information outside of the collection which is provided for by legislation and regulations of the core border agencies will be covered by an information sharing agreement. Information sharing agreements will:

- define the legal authority and lawful purposes for collecting the personal information,
- define the personal information necessary to fulfil the lawful authority and purpose, and
- require that adequate steps will be taken to ensure compliance.

Agencies are responsible for having the information sharing agreements in place.

The NZTD access policy controls which agencies have access to what data points.

Independent reviews and audits will ensure that the systems and processes for collecting the necessary personal information are adequate and operating satisfactory.

¹⁶ For initial trials we will be relying on a voluntary basis (openly collected through the privacy statement) and operational processes directing border officers on what they may access. For later trial and go-live, the authorisation model will be in place.

IPP 2 – Source of personal information

IPP 2 of the Privacy Act requires that an agency shall collect information directly from the individual concerned, unless an exception applies. Broadly, the exceptions under IPP2(2) are:

- (a) that non-compliance would not prejudice the interests of the individual concerned;
- (b) that compliance would prejudice the purposes of the collection;
- (c) that the individual concerned authorises collection of the information from someone else;
- (d) that the information is publicly available;
- (e) that non-compliance is necessary to avoid prejudice to maintenance of the law, for the enforcement of a pecuniary penalty law, for the protection of public revenue, for the conduct of court or tribunal proceedings, or to prevent or lessen a serious threat to the life or health of an individual; or
- (f) that compliance is not reasonably practicable in the circumstances of the particular case.
- (g) that the information will not be used in a form in which the individual concerned is identified or will be used for statistical/research purposes and not published in a form that could reasonably be expected to identify the individual concerned.

5. *Describe whether information will be collected directly from the individual.*

TJI does not collect any information directly, but processes data collected by:

- NZTD declaration service
- Cruise and Airline APP (such as ANA, SITA APP, Cruise API, Pre-travel manifest matching)
- DIA (Citizenship)¹⁷
- INZ (Visa)
- NZeTA
- Customs CusMod passenger movements
- Agency rules engine assessments (INZ, MPI, Customs)
- Interaction data

TJI does not join journeys over time and is only used to facilitate a specific voyage, i.e. it does not create an explicit historical database of an individual's movements.

The NZTD privacy statement will explain how the border agencies will collect, use and disclose personal information travellers will provide through the NZTD online form.

6. *Describe whether an exception applies etc.*

n/a

7. *State any risks.*

There is a risk that the data that is orchestrated by TJI is inaccurate and/or out of date which could mean that the traveller's risk profile could be incorrect.

8. *State any policies / processes that may need to be developed to achieve or maintain consistency and/or mitigate risks.*

¹⁷ Expected to be build in Aug – October timeframe.

- Many of the questions on the declaration relate to the conditions on arrival. The closer to arrival the declaration is completed, the less likely that the information is inaccurate. Controls will be in place to ensure a declaration cannot be submitted until 24 hours prior to beginning their journey¹⁸. This means that any inaccuracies or mistakes in the information will be minimised.
- The identity verification process, which occurs when the traveller crosses the Primary line, will ensure that the person providing the personal information is the correct individual. This process matches the passport to the individual and then to their declaration.
- The Primary Line is the point at which a digital traveller declaration is bound to a traveller's identity through association with their travel document. Travellers will be able to update their digital traveller declaration until they cross the Primary Line, mitigating the risk of inaccurate and/or out-of-date information. Once the traveller has crossed the Primary line, the declaration will be locked which ensures that no changes are made after the identity verification has occurred.¹⁹

IPP 3 – Collection of information from subject

IPP 3(1) of the Privacy Act requires that where an agency collects personal information directly from the individual concerned, the agency shall take reasonable steps to ensure that the individual knows:

- (a) the information is being collected;
- (b) the purpose of collection;
- (c) all intended recipients of the information;
- (d) name and address of the agency collecting the information and name and address of the agency holding the information;
- (e) whether collection is authorised or required by law – and the particular law, and whether it is mandatory or voluntary for the individual to supply the information;
- (f) consequences of not providing the information; and
- (g) their rights of access to (IPP6) and rights to correction (IPP7) of the personal information.

Under IPP 3(2) this should be done prior to collection, or as soon as practicable after collection.

Under IPP 3(3), agencies can forego notification of (a) to (g) above if the agency has recently communicated the same information to that individual in relation to collecting the same (or same type of) personal information from that individual. Please see the other exceptions under IPP 3(4), broadly:

- (a) that non-compliance would not prejudice the interests of the individual concerned;
- (b) that non-compliance is necessary to avoid prejudice to maintenance of the law, for the enforcement of a law imposing a pecuniary penalty, for the protection of public revenue, for the conduct of court or tribunal proceedings, or to prevent or lessen a serious threat to the life or health of an individual;
- (c) that compliance would prejudice the purposes of the collection;
- (d) that compliance is not reasonably practicable in the circumstances of the particular

¹⁸ Travellers arriving by small craft, commercial and specialist vessels will be able complete and submit their declaration no more than 24 hrs before departing from their last international port of departure.

¹⁹ A traveller can make verbal updates to a border officer after the Primary Line and the border officer can then make updates to the traveller's journey record.

case; or

- (e) that the information will not be used in a form in which the individual concerned is identified or will be used for statistical/research purposes and not published in a form that could reasonably be expected to identify the individual concerned.

9. *Describe how individuals will be notified of all the required information outlined in IPP3. Describe how individuals will be informed about the complete set of information to be collected.*

TJI will not collect any personal information directly.

There will be a privacy statement, explaining what personal information is being collected, for what purpose, which agencies will have access to this information, etc. Travellers are asked to confirm they have understood how their information is being used before submitting their NZTD. The privacy statement is also available on the dedicated website for NZTD.

Section 4 of this PIA provides more information on how NZTD will meet its openness and transparency obligations.

10. *Describe any exceptions.*

n/a

11. *State any risks (eg, only being able to advise on some of these elements, when there are no exceptions).*

n/a

12. *State any policies / processes that may need to be developed to achieve or maintain consistency and mitigate risks.*

n/a

IPP 4 – Manner of collection

Under IPP 4(1) Personal information shall only be collected by an agency

- (a) by lawful means; and
- (b) in the circumstances of this project, are by means that are
 - (i) fair, and
 - (ii) do not intrude unreasonably on the personal affairs of the individual concerned.

Particular care should be taken with regard to collection of personal information from children or young persons.

13. *Describe whether the collection is lawful, fair and not unreasonably intrusive (note - if an element is not met, it will be a risk).*

Extensive work has been done by the project team assessing the legal authority for the personal information that will be collected by NZTD. If any of the agencies wants to have access to any of the other data points, they will need to establish their legal authority and submit a business case to request access.

The NZTD privacy statement will explain how the NZ border agencies will collect, use and disclose personal information travellers will provide through the NZTD online form.

The NZTD will be available in English and te reo Māori²⁰ on go-live and static translations of the declaration for 29 other languages are available on the website. Work is being undertaken to determine the value of other languages being included in the future.

14. *State any risks (eg, if non-provision of information will result in the individual being unable to access the services – explain why this is not unfair in the circumstances).*

n/a

15. *State any policies / processes that may need to be developed to achieve or maintain consistency / mitigate risks.*

n/a

6.2 Storage and security

IPP 5 – Storage and security of personal information
<p>IPP 5(a) An agency holding personal information must ensure that information is protected by such security safeguards as are reasonable in the circumstances, against:</p> <ul style="list-style-type: none">• loss;• unauthorised access, use, modification or disclosure; and• other misuse. <p>IPP 5(b) This is also required when the information is transferred to a third party.</p>

16. *Describe security compliance including the security safeguards that will be in place.*

TJI does not store any data but orchestrates what component gets access to what NZTD data. The NZTD data access policy controls what agency will have access to what data. Agencies will only have access to the data they are legally authorised to access, e.g. Customs will only have access to relevant customs data, INZ will only have access to relevant immigration data, MPI will only have access to relevant biosecurity data.

The NZTD data access policy restricts an agency's access to only data required in the context of a specific purpose. They will only have access to the data they are legally authorised to access.

The NZTD cyber security team followed a 'secure by design' approach for NZTD, complemented by engaging an independent external third party to perform and complete penetration testing and configuration reviews.

17. *Describe how these are reasonable in the circumstances.*

The NZTD data access policy will allow the users and system of a particular agency to access only the data that is necessary for that agency to assess the travellers profile. i.e. MPI can only access answers to the questions that are relevant to MPI's role.

²⁰ Answers to the questions need to be provided in English, as per the current legislation.

A 'secure by design' approach is considered best practice.

18. *State any risks here (eg, 3rd party access, unsecured information etc).*

The NZTD cyber security team has assessed the security risks for TJI and is responsible for the Certification & Accreditation (C&A) process and security risk assessment. For more information on security risks, please refer to the security C&A.

19. *State any policies / processes that may need to be developed to achieve or maintain consistency and/or mitigate risks.*

Information sharing agreements will:

- define the legal authority and lawful purposes for collecting the personal information,
- define the personal information necessary to fulfil the lawful authority and purpose; and
- require that adequate steps will be taken to ensure compliance.

Agencies are responsible for having the correct information sharing agreements in place.

6.3 Access, correction and accuracy

IPP 6 – Access to personal information
<p>Where an agency holds personal information, the individual concerned shall be entitled</p> <ul style="list-style-type: none">• IPP 6(1)(a) to obtain confirmation of whether the agency holds personal information about them; and• IPP 6(1)(b) to have access to their personal information.
<p>Under IPP 6(2), if an individual is given access to their personal information, they must be advised that, under IPP 7, they may request correction of that information.</p>
<p>Under IPP 6(3), IPP 6 is subject to Part 4 (Access to and correction of personal information) of the Privacy Act.</p>

20. *Describe compliance elements – for example, can Customs (and other relevant agency) confirm the information exists and is held by Customs? Can Customs provide that information in a form requested by the individual concerned? How will the individual be advised of their right to request correction of the information?*

TJI is an orchestration system. The references stored in TJI do not contain personal information and any personal information processed by TJI is held in other systems. Access to this information is described in the PIAs of those systems.

21. *State any risks. (Note that IPP6 creates legally enforceable rights for the individual concerned.)*

n/a

22. *State any policies / processes that may need to be developed to achieve or maintain consistency and/or mitigate risks.*

n/a

IPP 7 – Correction of personal information

Under IPP 7(1), where an agency holds personal information, the individual concerned is entitled to request correction of that information.

Under IPP 7(2), the agency must then take such steps that are reasonable in the circumstances (considering the lawful purpose of use of the information) to ensure that the information is accurate, up to date, complete and not misleading.

Under IPP 7(2A), when making this request or at any later time, the individual may also provide the agency with a statement of the correction sought (**Statement of Correction**) and request that the Statement of Correction is attached to the information if the agency does not make the correction.

Under IPP 7(2B), where the agency is not willing to correct the information following a correction request, the agency must take reasonable steps to attach the Statement of Correction provided by the individual so that it will always be read alongside the information.

Under IPP 7(3), where the agency has corrected the information, or attached a Statement of Correction to the information, the agency must (if reasonably practicable) inform each person or agency to whom the information has been disclosed of those steps taken.

23. *Description of compliance – for example, can Customs correct that information? Can Customs **attach** a statement that the correction was sought, to the personal information itself? Can Customs inform the third parties it has disclosed the personal information to?*

TJI is an orchestration system. Any personal information processed by TJI is held in other systems and correction of this information is described in the privacy impact assessments of those systems.

24. *Description of compliance – if relevant, will 3rd party recipients (eg other agencies) be able to be advised.*

n/a

25. *State any risks.*

n/a

26. *State any policies / processes that may need to be developed to achieve or maintain consistency and/or mitigate risks.*

n/a

IPP 8 – Accuracy of personal information to be checked before use

An agency that holds personal information shall not use or disclose that information without taking steps that are (in the circumstances) reasonable to ensure that the information is accurate, up to date, complete, relevant and not misleading. These steps should be taken having regard to the purpose for which the information will be used (IPP1).

27. *Describe compliance with information accuracy – for example, will collection support accuracy? Will steps be taken to maintain accuracy over the project / information’s lifespan? Are these reasonable steps in the circumstances or could more be done?*

The TJI datastore contains:

- Biographic details of a traveller.
 - E.g. name, DOB, sex
- Passport details.
- Flight/ voyage details.
- References to other components that relate to a particular journey.

This data is collected by either the NZTD declaration service²¹ or other trusted sources such as check-in API, pre-travel manifest etc.

TJI’s role is to validate the assertions made on the digital traveller declaration. For this purpose, it uses trusted sources of data such as enrichments services, APP and CusMod Pax movements.

If there is no declaration at that time of arrival, TJI will use data from other trusted sources (such as APP or information collected at the check-in counter or at the Primary Line booth). When TJI uses data from other sources due to lack of a declaration, the TJI record will get updated with the declaration once it receives declaration data. If no declaration is received, the TJI record will be an orphan record and will be managed in accordance with NZTD data retention policy.

A key benefit of TJI is that it allows the gathering and matching of events from multiple sources of truth, will merge where it finds duplicate records for a traveller’s unique journey, and preserves the combined reference for each single unique journey record.

The TJI will use the following data matching rules:

- Minimise the chance of incorrectly joining two journey sources. It is better to have a declaration not match to a journey event (and be resolved via exception) than to allow a declaration to be incorrectly joined to a journey event from another traveller.
- Minimise duplication of data held elsewhere in the system.
- Allow for ‘loose’ matching in specific contexts where strict matching results in too many exceptions.

To minimise the chance of incorrectly joining two journey sources the inclusion of passport details is needed. Biographic details alone leave scope for false-positive mismatches (e.g. two John Smiths with the same DOB travelling on the same flight).

If a traveller uses the mobile app to fill out the digital traveller declaration, the traveller can scan their passport details. This limits the risk of mistakes made when manually entering these details and reduces data matching tolerances and/or mistakes (e.g. a traveller making a mistake while manually entering their passport details increases the risk of pulling the declaration of another traveller).

²¹ By having travellers fill out the digital traveller declaration.

28. *Describe how these steps are consistent with the purpose of collection/use under IPP1.*

The Primary Line is the point at which a traveller's digital traveller declaration is bound to their identity through association with their travel document. Travellers will be able to update their NZTD until they cross the Primary Line.

29. *State any risks.*

If there is no declaration at that time of arrival, TJI will use data from other trusted sources. This means that if a traveller does not submit an NZTD before reaching the Primary Line, TJI will not have all NZTD declaration information directly from the traveller. TJI will be updated progressively by Interactions from a Border Officer during arrival processing or notification from the declaration service that information from a paper card is available.

30. *State any policies / processes that may need to be developed to achieve or maintain consistency and/or mitigate risks.*

Many of the questions on the declaration relate to the conditions on arrival. The closer to arrival the declaration is completed, the less likely that the information is inaccurate. Controls will be in place to ensure a declaration cannot be submitted until 24 hours prior to beginning their journey. This means that any inaccuracies or mistakes in the information will be minimised.

The Primary Line is the point at which a digital traveller declaration is bound to the traveller's identity through association with their travel document. Travellers will be able to update their NZTD until they cross the Primary Line.

Identity verification processes (passport control) will ensure the person providing the personal information is identified as the individual (or another person lawfully permitted to provide the information).

6.4 Retention, use and disclosure

IPP 9 – Agency not to keep personal information for longer than necessary

An agency that holds personal information shall not keep that information for longer than is required for the purposes for which it may lawfully be used.

31. *Describe term of data retention - how long it is required to meet the lawful use under IPP 1.*

Once the traveller has arrived and has been processed, the journey will be deemed as closed. The record will need to be maintained for a minimum period for legal and operational purposes, then it will be deleted following the NZTD data retention policy²².

TJI captures the unique journey record for a single journey made by a traveller. It does not join journeys over time and is only used to facilitate a specific voyage, i.e. it does not create an explicit historical database of an individual's movements.

²² Disposal authority for NZTD is TBC.

32. *State any risks here.*

Keeping personal information longer than necessary may increase the risk of unauthorised and inappropriate access, use or disclosure.

33. *State any policies / processes that may need to be developed to achieve or maintain consistency and/or mitigate risks.*

Once personal information is no longer required to satisfy legal and operational requirements, it will be deleted from TJI²³.

Independent reviews and audits will ensure that TJI and the processes for the retention and deletion of personal information are adequate and operating satisfactorily.

IPP 10 – Limits on use of personal information

Personal information obtained in connection with one purpose, shall not be used for any other purpose unless the agency reasonably believes an exception applies. Exceptions are set out at IPP10(1), which broadly states:

- (a) that the purpose of use is directly related to the purpose of collection;
- (b) that the information will not be used in a form in which the individual concerned is identified or will be used for statistical/research purposes and not published in a form that could reasonably be expected to identify the individual concerned;
- (c) that the use for that other purpose is authorised by the individual concerned;
- (d) that the source is a publicly available publication, and it would not be unfair to use the information in the circumstances;
- (e) that the use for that other purpose is necessary to avoid prejudice to maintenance of the law, for the enforcement of a law imposing a pecuniary penalty, for the protection of public revenue, or for the conduct of court or tribunal proceedings; or
- (f) that the use for that other purpose is necessary to prevent or lessen a serious threat to public health or safety, or the life or health of any individual.

34. *Describe how use is consistent with collection purpose.*

The data that is being orchestrated in the TJI is essential for border control agencies to be able to process a traveller on arrival in New Zealand effectively and efficiently and will be an important component in enabling border control agencies to fulfil their statutory requirements.

Agencies will only have access to the data they are legally authorised to access, e.g. Customs will only have access to customs relevant data, INZ will only have access to immigration relevant data, MPI will only have access to biosecurity relevant data.

The NZTD privacy statement will explain how border agencies will collect, use and disclose personal information travellers will provide through the NZTD online form. The privacy statement is also available on the dedicated website for NZTD.

²³ Disposal authority for NZTD is TBC.

35. Describe any exceptions that may apply.

n/a

36. State any risks

Agencies could access the data for NZTD purposes (legally authorised) but use it for a different purpose (not legally authorised) as a result of those involved having an insufficient understanding or not applying the requirements of the Privacy Act and/or NZTD (and more specifically, TJI) policies.

37. State any policies / processes that may need to be developed to achieve or maintain consistency and/or mitigate risks.

NZTD's data access policy will specify role-based access components. Requiring validation of the legal authority at both an agency and role level will provide further mitigation for this risk. For example, a Customs officer who works in border processing at the airport will be able to access different information fields than an administrator of an agency's rules engine.

Privacy breach management processes will ensure that unauthorised and inappropriate access will be recorded, appropriately assessed, analysed and categorised, acted upon within agreed timeframes and result in improvements to privacy and security measures that will help prevent future breaches.

Independent reviews and audits will ensure TJI processes for dealing with unauthorised and inappropriate use are adequate and operating satisfactorily.

IPP 11– Limits on disclosure of personal information

An agency shall not disclose personal information to any other agency or person unless the agency believes, on reasonable grounds, that:

- (a) the disclosure purpose is in connection with (or directly related to) the purpose for which the information was obtained;
- (b) the disclosure is to the individual concerned;
- (c) the disclosure is authorised by the individual concerned;
- (d) the source of the information is a publicly available publication, and in the circumstances would not be unfair;
- (e) the disclosure is necessary to avoid prejudice to the maintenance of the law by any public sector agency; for enforcing a law imposing a pecuniary penalty; for the protection of the public revenue; or for the conduct of proceedings before any court or tribunal;
- (f) the disclosure of the information is necessary to prevent or lessen a serious threat to public health, or public safety, or the life or health of an individual;
- (g) the disclosure is necessary to enable an intelligence and security agency to perform any of its functions;
- (h) the information is to be used in a form in which the individual concerned is not identified, or for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
- (i) the disclosure is necessary to facilitate the sale or other disposition of a business as a going concern.

This principle is subject to IPP 12.

38. *Describe whether information will be disclosed to any other agency or person, in what circumstances, and, if so, which exception would apply to each disclosure.*

TJI will be accessed by the border agencies, i.e. Customs, INZ (through MBIE) and MPI²⁴. TJI will also be used to orchestrate the sharing of data to other government agencies where an appropriate statutory purpose and/or authorised information sharing agreement is in place. Agencies will only have access to the data they are legally authorised to access.

NZTD's data access policy will be used to allow access to TJI and to ensure that agencies will be able to access the NZTD data they are legally authorised to.

39. *State any risks.*

Personal information may be inappropriately disclosed as a result of those involved having an insufficient understanding of or not applying the requirements of the Privacy Act and TJI policies.

40. *State any policies / processes that may need to be developed to achieve or maintain consistency and/or mitigate risks.*

- The NZTD data access policy will be configured correctly to ensure only agencies that have a legal authority to access NZTD data will be able to access the data and only appropriate roles within the agency have access to TJI.
- The current Information Sharing Agreements have been reviewed and updated to ensure the participating agencies receive appropriate access to NZTD data.
- An independent review and audit will ensure that systems and processes for dealing with unauthorised and inappropriate disclosure are adequate and operating satisfactorily.

6.5 Offshoring of information

IPP 12 – Disclosure of personal information outside New Zealand

An agency may only disclose personal information to a foreign person or entity (recipient) in reliance on IPP11(a), (c), (e), (f), (h), or (i) if:

- (a) the individual concerned (whose personal information it is) authorises the disclosure after being informed that the recipient may not be required to protect the information in a way that, overall, is comparable to the Privacy Act;
- (b) the recipient is carrying on business in New Zealand and the agency believes the recipient is subject to the Privacy Act;
- (c) the agency believes on reasonable grounds that the recipient is subject to privacy laws that (overall) provide comparable safeguards to the Privacy Act;
- (d) the agency believes on reasonable grounds that the recipient is a participant in a prescribed binding scheme (as defined in [insert specific regulation] the Privacy Act);
- (e) the agency believes on reasonable grounds that the recipient is subject to the privacy laws of a prescribed country (as defined in [insert specific regulation]); or
- (f) the agency believes on reasonable grounds that the recipient is required to protect the information in a way that (overall) provides comparable safeguards to the Privacy Act – for example, under a contractual agreement between the agency and the recipient.

²⁴ As noted, MoH could also access the TJI if needed to (e.g. at the time of a pandemic or other health scare).

41. *State personal information storage location – some of this will, necessarily, be repetition of IPP5.*



42. *If overseas, state whether this is a disclosure.*
n/a

43. *State which exceptions will be relied on for disclosing.*
n/a

44. *State any risks.*
n/a

45. *State any policies / processes that may need to be developed to achieve or maintain consistency and/or mitigate risks.*
n/a

6.6 Unique identifiers

IPP 13 – Unique identifiers

Agencies shall not assign unique identifiers to individuals unless it is necessary for that agency to carry out its functions. Agencies shall not require individuals to disclose any unique identifier unless that disclosure is related to the purpose it was assigned.

46. *Describe whether unique identifiers will be assigned, and whether individuals will need to disclose them.*


No unique identifiers will be assigned to individuals in TJI. The journey record, which includes travellers' biographic details and voyage, will have a unique ID for that journey. The unique ID will be linked to the declaration answer for the specific journey, will only be used within the system, and won't be used anywhere else.

47. *State any risks.*
n/a

48. *State any policies / processes that may need to be developed to achieve or maintain consistency and/or mitigate risks.*
n/a

7 Risk, consultation and signature

7.1 Consultation

Consultation team	Team member	Date consulted	Advice given	Advice incorporated
ISP	 Principal Privacy Advisor	17/03/2023	Feedback on draft PIA	Yes

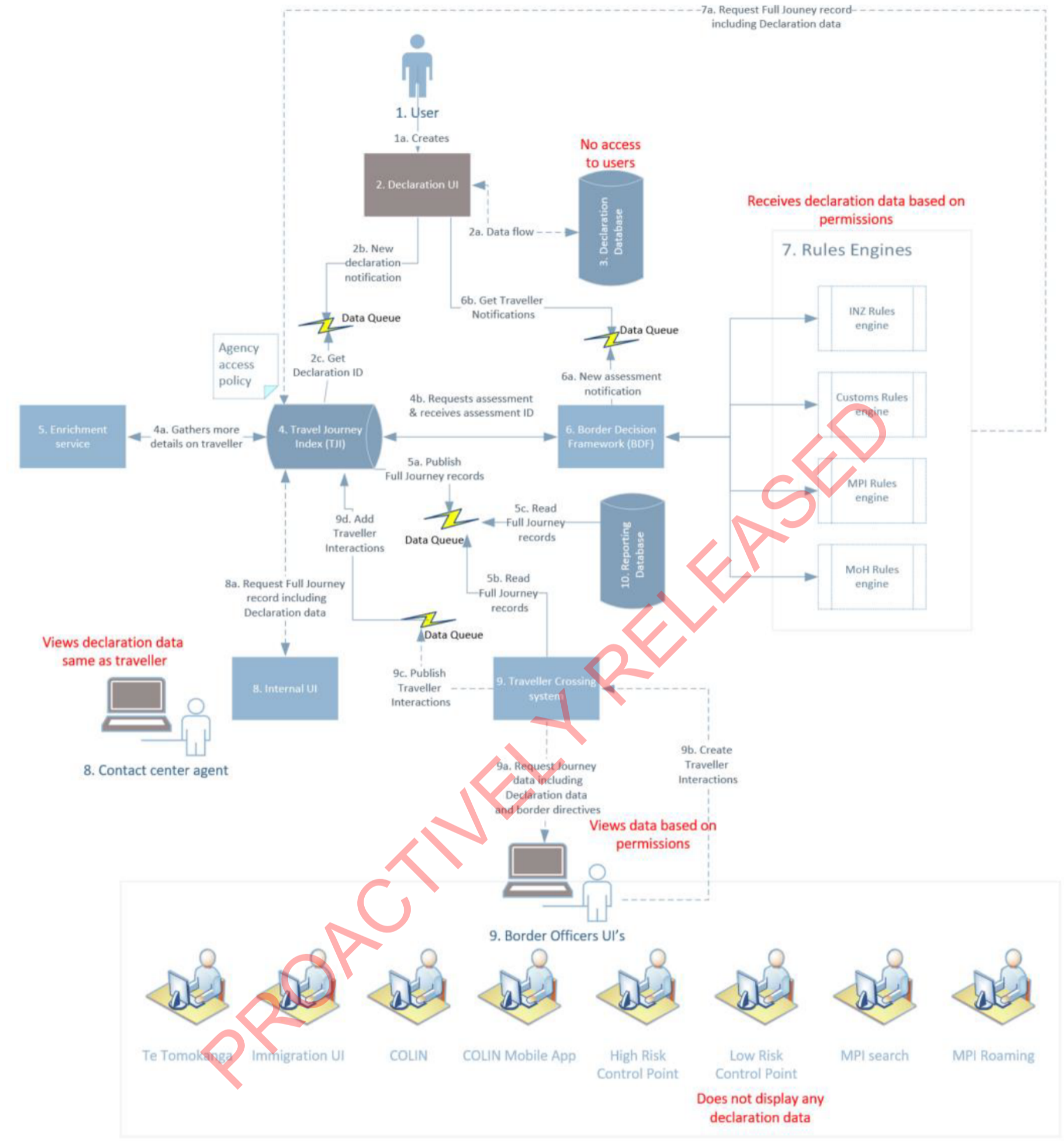
7.2 Signatures

Name and Position	Action	Signature	Date
Principal Pr			
Product Ow			
Product Ma			
Programme Director NZP			

Please refer to version 1.0 for the signed version.

PROACTIVELY RELEASED

Appendix 1 – Information flow Traveller Journey Index



Appendix 2 – Project Risks and Controls table

Risk #	Risk rating	IPP	Reasoning	Mitigations / Controls	Residual risk
R1	low	IPP1	There is a risk that data will be accessed by an agency under the incorrect assumption that this agency has a legal authority to access this data.	<ul style="list-style-type: none"> - Legal authority has been assessed. - If any of the agencies wants to have access to any of the other data points, they will need to establish their legal authority and submit a business case. - Agencies are responsible for updating their legislation and/or information sharing arrangements. - Independent reviews and audits will ensure that the systems and processes for collecting the necessary personal information are adequate and operating satisfactory. 	Very low
R2	low	IPP2	There is a risk that the data that is orchestrated by TJI is inaccurate and/or out of date.	<ul style="list-style-type: none"> - The closer to arrival the declaration is completed, the less likely that the information is inaccurate. Controls will be in place to ensure a declaration cannot be submitted until 24 hours prior to beginning their journey (or for maritime, 24hrs before departing from their last international port of departure). This means that any inaccuracies or mistakes in the information will be minimised. - The identity verification process will ensure that the person providing the personal information is the correct individual. - Travellers will be able to update their NZTD until they cross the Primary Line. 	Very low
		IPP3	n/a		
		IPP4	n/a		

R3		IPP5	The NZTD cyber security team has assessed the security risks for TJI and is responsible for the Certification & Accreditation (C&A) process and security risk assessment.	For more information on security risks, please refer to the security C&A.	
		IPP6	n/a		
		IPP7	n/a		
R4	medium	IPP8	If there is no declaration at that time of arrival, TJI will use data from other trusted sources. This means that if a traveller does not submit an NZTD before reaching the Primary Line, TJI would not receive all NZTD declaration information directly from the traveller.	<ul style="list-style-type: none"> - A declaration cannot be submitted until 24 hours prior to beginning their journey (or for maritime, 24hrs before departing from their last international port of departure). This means that any inaccuracies or mistakes in the information will be minimised. - Travellers will be able to update their NZTD until they cross the Primary Line. - Identity verification processes will ensure the person providing the personal information is identified as the individual. 	low
R5	low	IPP9	Keeping personal information longer than necessary may increase the risk of unauthorised and inappropriate access, use or disclosure.	<ul style="list-style-type: none"> - Once personal information is no longer required to satisfy legal and operational requirements, it will be deleted from TJI in a timely matter. - Independent reviews and audits will ensure that TJI and the processes for the retention and deletion of personal information are adequate and operating satisfactorily. 	Very low
R6	medium	IPP10	Agencies could access the data for NZTD purposes (legally authorised) but use it for a different purpose (not legally authorised) as a result	<ul style="list-style-type: none"> - NZTD's data access policy will specify role-based access components. - Privacy breach management processes will ensure that unauthorised and inappropriate access will be recorded, appropriately assessed, analysed and categorised, acted upon 	low

			of those involved having an insufficient understanding of or not applying the requirements of the Privacy Act and/or NZTD (and more specifically, TJI) policies.	<p>within agreed timeframes and result in improvements to privacy and security measures that will help prevent future breaches.</p> <ul style="list-style-type: none"> - Independent reviews and audits will ensure TJI processes for dealing with unauthorised and inappropriate use are adequate and operating satisfactorily. 	
R7	medium	IPP11	Personal information may be inappropriately disclosed as a result of those involved having an insufficient understanding of or not applying the requirements of the Privacy Act and/or NZTD (and more specifically, TJI) policies.	<ul style="list-style-type: none"> - The NZTD data access policy will be configured correctly to ensure only agencies that have a legal authority to access NZTD data will be able to access the data. - The current Information Sharing Agreements have been reviewed and updated to ensure the participating agencies receive appropriate access to NZTD data. - An independent review and audit will ensure that systems and processes for dealing with unauthorised and inappropriate disclosure are adequate and operating satisfactorily. 	low
		IPP12	n/a		
		IPP13	n/a		

PROACTIVELY RELEASED

Appendix 3 – Changes since version 1.0

- Version 1.1 (August 2023)
 - Section 7.2 (signatures) removed from version 1.0
 - Appendix 3 (Changes since version 1.0) added.
 - Page numbers added.
 - Footnote 17 added.
 - Amended traveller's declaration to traveller's journey record in footnote 19.
 - Removed footnote 25.
 - Amended the sentence that Information Sharing Agreements *will be reviewed* to Information Sharing Agreements *have been reviewed*.

PROACTIVELY RELEASED