JOINT BORDER ANALYTICS

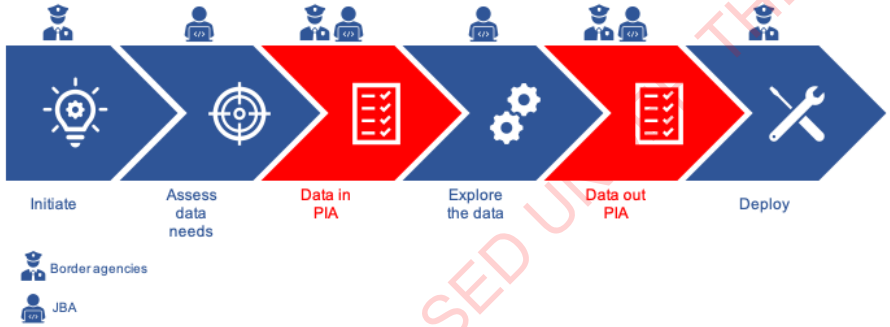
Single Agency Privacy Impact Assessment Template – DATA IN module

This module is for any new single agency analytics activity, conducted by the Joint Border Analytics Centre (JBAC) on behalf of a border agency, that requires the collection of new personal information from an external source. The module assists the requesting border agency to assess the lawfulness of the collection of new personal information. [1]

The objective of the JBAC PIA process and modules is to **enable single agency analytics, to better deliver border enforcement functions, in a way that is open, safe, and mindful of the people behind the data**.

Governance and accountability

Single agency analytics activities must be initiated by a border agency (the Requesting Agency). The Requesting Agency is responsible for assessing privacy or other risks raised by an activity and approving the activity. The Requesting Agency must involve its privacy and/or legal team as reviewers of this PIA. JBAC can assist involved border agencies to identify or develop analytics activities and manage associated privacy risks, but JBAC cannot approve analytics activities or outputs.



What the module covers

This is a DATA IN PIA module. A new module must be completed for each external dataset JBAC proposes to collect on behalf of the Requesting Agency for the purposes of the activity.

The process in brief

1. Requesting Agency initiates analytics activity with JBAC
2. JBAC completes sections 1 and 2 (in consultation with the Requesting Agency)
3. Requesting Agency completes section 3 (in consultation with JBAC)
4. JBAC completes section 4 to reflect outcome of section 3
5. Requesting Agency's privacy/legal representatives review completed PIA and add feedback
6. Subject to feedback, PIA is signed by Requesting Agency and privacy/legal reviewer
7. Activity may commence subject to actions or conditions identified in PIA

Section instructions, a glossary at Appendix 1, and explanatory notes at Appendix 2, provide more detail on completing the DATA IN PIA module. Tables are colour-coded (as above) to indicate who should complete them.

JOINT BORDER ANALYTICS

Single-Agency Privacy Impact Assessment – DATA IN module

Complete a separate DATA IN module for each external dataset required for the activity.

1. Governance and contact information

What's this for?	*This section records which border agency initiated the analytics activity and the contact details for key staff involved. Note, JBAC will always be involved as the analytics service provider.*
Who should complete this?	***JBAC** will complete this section on behalf of the Requesting Agency.*

Date PIA commenced	19/10/2021
JBAC contact person for this activity	s 9(2)(g)(ii) OIA
Requesting Agency	NZCS
Activity contact person for Requesting Agency	s 9(2)(g)(ii) OIA
Privacy/legal representative for Requesting Agency	s 9(2)(g)(ii) OIA

2. Overview of the activity

What's this for?	*This section explains the analytics activity, for the purpose of assisting the Requesting Agency to make the data collection assessment.*

JOINT BORDER ANALYTICS

Who should complete this?	***JBAC** will complete this section on behalf of the Requesting Agency.*

1. What is the name of this activity?	New Zealand Customs Sea Freight project					
2. Briefly describe the activity, including the problem/s it is seeking to address	This activity seeks to explore client behaviours in relation to the importation of sea freight to understand what is normal and identify what is not (i.e. anomaly detection). The goal is to attempt to identify other methods of targeting sea freight consignments to identify border risk					
3. How does this activity support the Requesting Agency's lawful purposes and deliver public benefit? [2]	NZCS	All New Zealander's benefit from an effective border security system. People, goods, and craft cross our border every day, potentially carrying prohibited or restricted items, such as drugs and weapons, or bio-security threats. These could damage our social wellbeing, primary and tourism industries, natural ecosystems, and international reputation. The sea freight project intends to model border risk specific to trade in the sea cargo environment to assist in the identification of drug risk for targeting purposes (via Intelligence evaluation and analysis). Further, the models will be utilised to identify and minimise interactions with compliant entities in the sea freight space.				
4. What external datasets are required for this activity? *[JBAC – add more rows as required before protecting the form]*	**Dataset**	**Data elements**	**Source**	**Time period**	**Relevance to activity**	
	s 6(c) OIA [redacted]					

					s 6(c) OIA
5. Where will the analytics dataset be stored and processed? [3]	s 6(c) OIA				
6. How long will the analytics dataset be retained?					
7. What are the intended outputs of this activity?	☒ Analytics models and forecasts (non-identifiable)		☒ Identifiable intelligence outputs		
8. Briefly describe the outputs	s 6(c) OIA				

		s 6(c) OIA [redacted]
9. Relevant attached documents		

3. External data collection assessment

What's this for?	*This section assesses the lawfulness of the collection of the **external** dataset required to build the analytics dataset for the activity. Where appropriate, explain your answers in the right-hand column.*
Who should complete this?	*The **Requesting Agency** identified at section 1 must complete this assessment for each dataset being collected to ensure that they are satisfied they have a lawful basis to collect it.*

A. Dataset: Company Office Bulk Data

Dataset	s 6(c) OIA [redacted]		
Data source			
1. Are you satisfied that you have a lawful basis to collect this dataset? *IPP 2* [4]	☐ No, we do not think there is a lawful basis		**Action required**
	☒ Our enabling legislation	Customs and Excise Act 2018 s303(2)	Proceed
	☒ Principle 2(2)(a) – publicly available [5]	s 6(c) OIA [redacted]	Proceed
	☐ Principle 2(2)(g)(ii) - research [6]	n/a	Proceed
	☐ Principle 2(2)(d)(i) – maintenance of the law [7]	n/a	Proceed
	☐ Principle 2(TBC – Privacy Bill) – serious threat [8]	n/a	Proceed
	☐ Other	n/a	Proceed

2. Are you satisfied that the personal information in this dataset – including data fields or time periods – is reasonably necessary for this activity? *IPP 1* [9]	☐ Not sure, we need more information		**Action required**
	☐ No, we need to refine the data requirements		**Action required**
	☒ Yes, the dataset is necessary		Proceed
3. Could the people this data relates to view this collection as unfair or unreasonably intrusive? *IPP 4* [10]	☒ No	s 6(c) OIA [redacted]	Proceed
			Proceed
	☐ Yes		**Action required**
4. Are there any statutory restrictions on the use or retention of some or all of the information in the dataset?	☒ No	N/A	Proceed
	☐ Yes		**Action required**
5. Do relevant JBAC and/or Requesting Agency staff have the correct security clearances to access this dataset?	☒ Yes	N/A	Proceed
	☐ No		**Action required**
5. Privacy/Legal team comments			
6. Can the collection and use of this dataset proceed?	☒ **Yes** - Approved by:		
	☐ **Yes, but**:	☐ We need more information to establish data relevance ☐ We need to refine the data requirements [populate R1] ☐ We need to address statutory restrictions [populate R2] ☐ This could be perceived as unfair or unreasonably intrusive [populate R4] ☐ We need to ensure correct security clearances are in place [populate R5] ☐ Other [populate other]	
	☐ **No - Because**:	☐ We have no lawful basis to collect [populate R3] ☐ Other [populate other]	

JOINT BORDER ANALYTICS

4. Privacy risks, mitigations and actions

What's this for?	*This section captures any risks generated by the outcome of section 3. JBA or the Requesting Agency can also add more risks and mitigations here. Some risks that cannot be mitigated will require an action (such as removing an external dataset) and others will require mitigations (such as refining data requirements, establishing data destruction rules or data refresh processes).*
Who should complete this?	***JBAC** will complete this section on behalf of the Requesting Agency but the **Requesting Agency** may also add content as required.*

Risk	Mitigation/Action	Responsible	Date complete
R1 ☐ We are collecting information that is not necessary for the purposes of the activity		N/A	
R2 ☐ There are statutory restrictions that must be met		N/A	
R3 ☐ The Requesting Agency has no lawful basis to collect a dataset		N/A	
R4 ☐ A dataset is being collected in a way that could be viewed as unfair or unreasonably intrusive		N/A	
R5 ☐ The Requesting Agency needs to ensure the correct security clearances are in place		N/A	
☐ Other		N/A	

JOINT BORDER ANALYTICS

5. Data collection sign off

What's this for?	*This section captures Requesting Agency approval for the collection of the external dataset and also records that this PIA has been reviewed by the Requesting Agency's Privacy Officer or team. An activity cannot proceed until this section has been completed.*
Who should complete this?	*Requesting Agency approval must be **manager level or above**.*

Requesting Agency	**New Zealand Customs Service**
Data collection approved by	**Privacy review by**
s 9(2)(g)(ii) OIA [redacted] **Date: 08/11/2021**	s 9(2)(g)(ii) OIA [redacted] **Date: 29/06/2022**

JBAC
PIA reviewed by
s 9(2)(g)(ii) OIA [redacted] **Date: 01/11/21**

JOINT BORDER ANALYTICS

Appendix 1: Glossary

This	Means
Activity	an agreed and authorised (by the Requesting Agency) use of data analytics to produce a set of outputs that may include analytics models, forecasts or identifiable intelligence outputs.
Adverse action	any action that may adversely affect the rights, benefits, privileges, obligations, or interests of any specific individual; including any decision: i. to make an assessment of the amount of any tax, levy, or other charge, or of any contribution, that is payable by any individual, or to alter any such assessment: ii. to investigate the possible commission of an offence: iii. to make a deportation order in relation to the individual, to serve the individual with a deportation liability notice, or to deport the individual from New Zealand.
Analytics forecasts	forecasts designed to look forward at possible future patterns of border risk using historical information. These products contain no personal information.
Analytics models	models that identify a class of goods, craft and/or people who present an increased or decreased risk at the border. The output of analytics models offers a score based on weighted predictors. These products contain no personal information but may be used by border agencies to create personal information (as a result of running the model).
Border agencies	DIA, DOC, MBIE, MPI or NZCS.
CRISP-DM	Cross Industry Standard Process for Data Science (CRISP-DM). CRISP-DM is an open standard process model that describes common approaches used by data mining experts. It has six stages – business understanding, data understanding, data preparation, modelling, evaluation, and deployment.
Data analytics	the discovery, interpretation, and communication of meaningful patterns in data.
Data exploration	the comparison of datasets and data fields through the use of analytical techniques, methods and modelling, in order to better understand the relationship between datasets or data fields for the purposes of generating analytics outputs.
Data refinement	the possible result of the data exploration process, where datasets or data fields found not to be relevant to desired outputs are purged from the analytics dataset.

Dataset	a distinct category of data held by the Requesting Agency, by a third-party agency or that is publicly available. Each dataset will include data fields that may relate to identifiable individuals.
DIA	Department of Internal Affairs.
DOC	Department of Conservation.
Enabling legislation	the legislation which sets out a border agency's statutory functions and powers and includes the Customs and Excise Act 2018, Biosecurity Act 1993 and Immigration Act 2009.
Identifiable intelligence outputs	the result of an analytical process which produces identifiable information. The output may identify previously unknown relationships or indicate a known or unknown level of risk for an individual.
JBAC	Joint Border Analytics Centre; MPI, NZCS and MBIE/Immigration analytics experts delivering technical solutions and insights at the request of border agencies. The team is operationally focused.
MBIE	Ministry of Business, Innovation and Employment, which includes Immigration New Zealand.
MPI	Ministry for Primary Industries.
NZCS	New Zealand Customs Service.
Personal information	any information about an identifiable individual (natural person), including but not limited to personal identifiers (like name and address) and any information linked to personal identifiers (like events or entities). By combining datasets and linking fields with certain individuals (for example using the IR Number or name and address), analytics activities may create new personal information about identifiable individuals.
Requesting Agency	the border agency that has initiated the activity, will provide the platform within which the activity will be completed, and will be the sole recipient of any identifiable intelligence outputs.
Unlawful discrimination	discrimination based on any grounds prohibited by the Human Rights Act 1993, including sex, martial status, religious belief, colour, race, ethnic origin, disability, age, political opinion, and sexual orientation.

JOINT BORDER ANALYTICS

Appendix 2: Explanatory Notes

[1] In the absence of specific legislation that permits border agencies to collect or disclose personal information, the Privacy Act and IPPs apply. The IPPs are a flexible set of principles intended to ensure that agencies can achieve their goals in a privacy protective way. In summary, they require an agency to:

1. **Scope** – Collect only the personal information it needs for a lawful purpose connected with its functions.
2. **Source** – Collect personal information directly from the person concerned, unless an exception applies.
3. **Notice** – Tell people certain things when collecting personal information directly from them.
4. **Manner** – Collect personal information in ways that are lawful and, in the circumstances, fair and not unreasonably intrusive.
5. **Security** – Take reasonable steps to protect personal information from harm.
6. **Subject access** – Give people access to the personal information it holds about them.
7. **Correction** – Let people correct personal information if it is incorrect.
8. **Accuracy** – Take reasonable steps to ensure personal information is accurate and up-to-date before using it.
9. **Retention** – Retain personal information for no longer than is required.
10. **Use** – Use personal information only for the purposes for which it was collected, unless an exception applies.
11. **Disclosure** – Not disclose personal information, unless an exception applies.
12. **Unique identifiers** – Take care when assigning or using unique identifiers.

Many IPPs – including principles 2 and 10 – contain exceptions that ensure legitimate information processing is possible. Thus, even where a border agency's enabling legislation is silent on the matter of collecting or using personal information for analytics activities, the Privacy Act is likely to permit it, provided that it is necessary and proportional and relates to the Requesting Agency's lawful functions.

The Privacy Commissioner and Government Chief Data Steward released a set of *principles for the safe and effective use of data and analytics* ('Analytics Principles'), intended to promote transparency and a best-practice approach to the use of data and analytics for supporting operational decision-making.

1. **Deliver clear public benefit** – it's essential government agencies consider, and can demonstrate, positive public benefits from collecting and using public data.
2. **Ensure data is fit for purpose** – using the right data in the right context can substantially improve decision-making and analytical models, and will avoid generating potentially harmful outcomes.
3. **Focus on people** – keep in mind the people behind the data and how to protect them against misuse of information.
4. **Maintain transparency** – transparency is essential for accountability. It supports collaboration, partnership, and shared responsibility.
5. **Understand the limitations** – while data is a powerful tool, all analytical processes have inherent limitations in their ability to predict and describe outcomes.
6. **Retain human oversight** – analytical processes are a tool to inform human decision-making and should never entirely replace human oversight.

[2] It is essential that the Requesting Agency consider, and can demonstrate, positive **public benefits** from collecting, analysing and using personal information. A clear link to Requesting Agency's lawful purposes (as set out in its enabling legislation) is also required to ensure that an activity is legitimate and necessary.

[3] Analytics datasets relating to single agency analytics activities will usually be **stored and processed** within the Requesting Agency's system, in accordance with the JBA single agency SOPs. Where JBAC proposes to store or process datasets on another platform, this must be stated in the PIA.

[4] The burden of establishing that an exception applies to permit a collection or use of personal information rests with the Requesting Agency seeking to rely on it. The Requesting Agency may seek further clarity from JBAC where this is required in order to establish whether an exception applies.

[5] Principle 2(2)(a) permits the collection of personal information if the information is contained in a publicly available publication. This exception is likely to permit the collection of personal information from publicly accessible online sources, including websites or social media platforms, or from the news media.

[6] Principle 2(2)(g)(ii) permits the collection of personal information if the information is to be used for statistical or research purposes and will not be published in an identifiable form. This exception is likely to permit the collection of relevant personal information for the purposes of generating analytics models and forecasts, but should not be applied where the Requesting Agency intends to generate identifiable intelligence outputs.

[7] Principle 2(2)(d)(i) permits the collection of personal information where this is necessary to avoid prejudice to the maintenance of the law, including the prevention, detection, investigation, and prosecution of offences. This exception is likely to permit the collection of relevant personal information for the purposes of generating targeted analytics forecasts (intended to detect or prevent offences) or identifiable intelligence outputs. Note, 'necessity' includes considerations of data minimisation and proportionality.

[8] Principle 2 will be amended by the Privacy Bill to include a serious threat exception. Once amended, this exception will permit the collection of personal information where this is necessary to prevent or lessen a serious threat to public health or safety or the life or health of an individual. This exception may permit the collection of relevant personal information for the purposes of generating or disseminating identifiable intelligence outputs to respond to an imminent threat.

[9] **Data minimisation** is an important element of the privacy framework. Agencies should collect and use only the minimum amount of personal information necessary to meet their lawful purposes. In the initial stages of an analytics activity, lawful purposes will include exploring and assessing datasets available to establish how useful each will be. Effort should be made initially to ensure that exploration datasets shared are broadly relevant to the activity and, later, to remove any datasets or data fields that are not found to be relevant to the activity.

[10] Principle 4 requires an agency to collect personal information in a manner that is not unlawful or, in the circumstances, unfair or unreasonably intrusive. This principle incorporates concepts of fairness and proportionality and will require the Requesting Agency to consider whether the collection of a dataset for the purposes of a particular analytics activity could be viewed as unfair or intruding into the personal affairs of affected individuals to a greater extent than the ends would justify.