



12 August 2022

ref 2122-2328

Will O'Brien

fyi-request-19661-107b5a4f@requests.fyi.org.nz

Tēnā koe Will

Thank you for your Official Information Act (OIA) request of 14 June 2022 to the Ministry of Business, Innovation and Employment (MBIE), for copies of our risk templates. On 3 July, you advised you were interested in the following material:

- *a copy of the template MBIE uses for its information security risk assessments*
- *a copy of the template MBIE uses for its privacy impact assessments*

Information security templates

There is one template in scope of your request.

Due to its content, I am withholding the template in full under the following sections of the OIA:

- s6(b), to avoid prejudice to information entrusted to the government on a basis of confidence
- s6(c), to avoid prejudice to the maintenance of the law, including the detection and prevention of offences; and
- s9(2)(k), to prevent the use of official information for improper gain or advantage

The templates you have requested, if released into the public domain, would provide a level of information about MBIE's approach to managing information security issues that would put our systems and security at real and measurable risk.

In line with section 9(1) of the OIA, I have also considered whether there is a countervailing public interest strong enough to override our decision to withhold this template in full in the grounds in section 9(2) of the OIA. In this instance, I believe the greater public interest is in ensuring the safety of MBIE's information security systems.

MBIE's IT templates are based on, and consistent with, the protective security requirements for government agencies, as outlined by the Government Chief Digital Officer (GDCO). You can read more about these requirements on the GDCO's website, at:

<https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/security/>

Privacy Impact Assessment templates

I am releasing to you the documents listed in the table overleaf. No information has been redacted from these documents.

Number	Title/description
1	Privacy and Security Threshold Assessment web form
2	Privacy Impact Assessment Workflow chart
3	<i>Privacy Impact Assessment Report</i> Template document
4	<i>Privacy Impact Assessment Guidance</i> Internal document

A copy of the spreadsheet containing our Privacy Impact Assessment Tool is also attached to the same email as this letter.

These documents supplement our publicly available advice regarding the collection of information under the Privacy Act 2020, as contained on our website at <https://www.mbie.govt.nz/privacy/>.

Thank you again for your request. Under section 28(3) of the OIA, you have the right to refer our response to an Ombudsman for review. You can find more information about this by emailing info@ombudsman.govt.nz or by calling 0800 802 602.

Nāku noa, nā



David Habershon
Chief Information Security Officer, Digital, Data and Insights

Privacy Threshold Assessment

Start new assessment

Recent

Privacy and Security Threshold Assessment

The Privacy Team and Cyber Security may both be in touch with you if any further information is required.

Overview

Project/initiative name* and project code number (if applicable)

Business group project/initiative being delivered for *

Business owner *

Project manager *

PMO manager (if applicable)

Submitter name

Submitter role

Has a privacy impact assessment previously been completed? *

Briefly describe the initiative/project and the business purpose/need. Outline what's new or changing and if you require personal information to meet that change *

Characters left 500

Which answer/s best describe the project/initiative? *

What is the budget for this work? *

What stage is the project in? *

What is the go live date on this project/change? *

Unsure of date

Select the categories of information that may be collected, stored, used, impacted or disclosed as a result of this change *

:

Information Collection

How will this information be classified? *

How many people will this work collect personal information about? *

Fewer than 5,000 individuals More than 5,000 individuals

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Information about:	
Will any collection of personal information for the project/initiative be mandatory? *	<input type="radio"/> Mandatory <input type="radio"/> Not mandatory
How will you collect any personal information for this work? *	<input type="text"/>
How will any personal information collected be used? *	<input type="text"/>
If this work is going to modify an existing project/initiative, which sentence best describes the change? *	<input type="text"/>
Is the collected personal information going to be matched or linked with other sources of information? *	<input type="text"/>
Who is personal information being used by, shared with or disclosed to? *	<input type="text"/>
Is any of the personal information that you are collecting going to be disclosed to a person or entity outside of New Zealand? *	<input type="text"/>
Technology Impact	
Which sentence best describes the technology to be used? *	<input type="text"/>
Where will the personal information be stored? *	<input type="text"/>
Are other business critical MBIE systems or processes, internal or external, are dependent on this system? *	<input type="text"/>
If the system is a website is it "transactional" (providing for any exchange of information including contact details), or is it "static", meaning it will simply publish information? *	<input type="text"/>
Does the system introduce any of the following?	Check all boxes that apply or might apply don't worry if you're not sure
Self-Analysis and Third Parties	
What does your team consider the impact of this work on information privacy? *	<input type="text"/>
Will any third parties be involved in this work (outside MBIE) that legal and/or commercial agreements will be required for? *	<input type="text"/>

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Submitter comment

NAVIGATION

[Services - Ratonga](#)
[IT - Hangarau](#)
[HR - Tiaki tāngata](#)
[Belong - Nō Konei](#)
[News - Pānui](#)
[About us - Mō mātau](#)

USEFUL LINKS

[Internal policies](#)
[Report an event](#)
[Report an emergency](#)
[Update your profile](#)
[Facilities support](#)

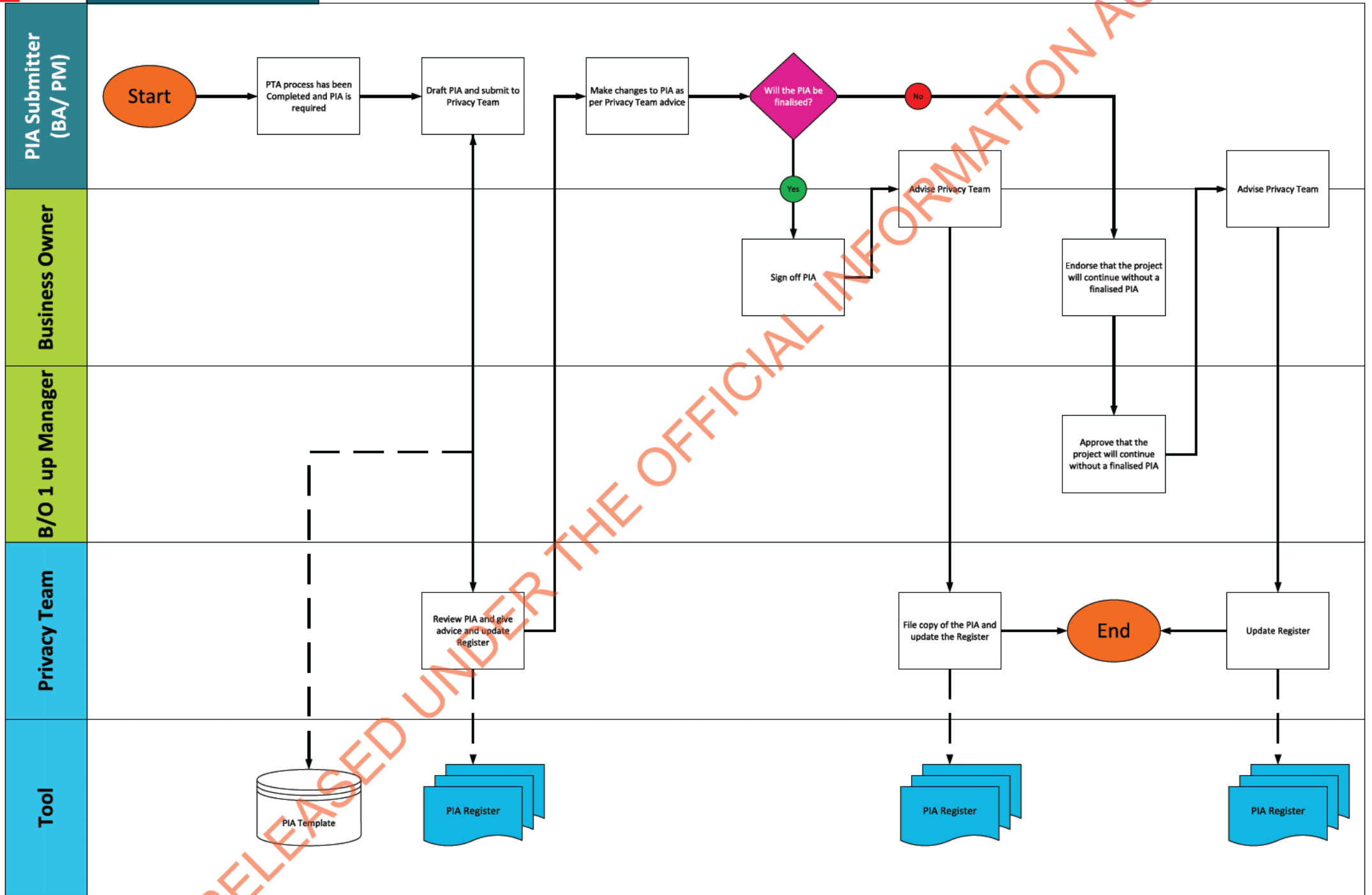
[People leaders](#)
[FlexiPurchase](#)
[Te Taura sub sites](#)
[Team sites](#)
[News on the MBIE website](#)
[Public Sector Intranet](#)

CONNECT

[LinkedIn](#)
[Twitter](#)
[Facebook](#)

RELEASED UNDER THE OFFICIAL INFORMATION ACT

PIA Process



RELEASED UNDER THE OFFICIAL INFORMATION ACT



CLASSIFICATION TEXT



[Initiative name]

Privacy Impact Assessment Report

[Date]

RELEASED UNDER THE OFFICIAL INFORMATION ACT

CLASSIFICATION TEXT

Version control


Version	Author	Description of change	Date

Consultation

Date	Reviewer	Comments

Review and sign-off

Name	Role	Date	Signature

Drafting note: Click Show/Hide  to display hidden guidance text.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Contents

Executive Summary..... 4

Initiative summary 5

PIA methodology..... 6

 Scope..... 6

 The process 6

 Explain the scope and process 6

Personal information 7

Privacy analysis 8

Risk assessment 9

Actions to enhance or minimise impact on privacy..... 10

Conclusion..... 11

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Executive Summary

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Initiative summary

The initial Privacy Threshold Assessment (PTA) identified that this initiative had a high risk of potentially impacting personal information and individuals' privacy.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

PIA methodology

Scope

The process

This PIA was undertaken in accordance with the MBIE PIA Framework. The initial PTA was completed , and MBIE's standard Data Flow and Impact Analysis templates were approved .

Explain the scope and process

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Personal information

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Privacy analysis

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Risk assessment

Ref	Risk description	Existing controls	Options considered

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Actions to enhance or minimise impact on privacy

Ref	Treatment / Action	Owner	Status	Comment

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Conclusion

RELEASED UNDER THE OFFICIAL INFORMATION ACT



Privacy Impact Assessment Guidance

Planning and completing a successful assessment

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Preface

This guide is here to help you complete a privacy impact assessment. In the spirit of help, here is the first suggestion: don't read this guide cover-to-cover. Most of this guide is probably not relevant to your specific privacy impact assessment, so dip in-and-out. The information is chunked up into sections so find the section relevant to your question, but don't worry about knowing or reading every word.

This guide is broken into three chapters.

Chapter One: Introduction to privacy impact assessment, the process, and why you should consider privacy impact.

Chapter Two: Key Concepts looks deeper at concepts- this chapter is entirely new and is in response to those of you that want to know more about the underlying principles.

Chapter Three: Question-by-question guide to the Privacy Impact Assessment tool's questions. You can use the index to find the section relevant to you. There is also a list of common risk and mitigations for each principle.

This guide does not cover the business processes or rules. For that information, see [here](#).

The guidance includes these symbols:



Important information



Key question



Trip hazard: this is an area where people often hit issues or problems.



Stories and examples from other PIAs.

Contents

Preface..... 2

Part One: Introduction to the Privacy Impact Assessment..... 4

Part Two: Key concepts..... 7

Part Three: Question-by-question 11

Principle 1..... 12

Principle 2..... 15

Principle 3..... 17

Principle 4..... 20

Principle 5..... 22

Principle 6..... 26

Principle 7..... 28

Principle 8..... 30

Principle 9..... 32

Principle 10..... 33

Principle 11..... 36

Principle 12..... 38

Principle 13..... 38

Governance & assurance issues..... 39

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Part One: Introduction to the Privacy Impact Assessment

A Privacy Impact Assessment is a process for assessing how something will affect people's privacy, both positively and negatively. You could use a PIA in a project, policy, service, product, or research. A PIA will be useful where a change involves personal information or information used to target people (e.g. targeted advertising).

The purpose isn't only to note the privacy impact but also to introduce privacy enhancing changes to the design. For this to work, start early. By getting privacy right early you will could avoid rework and issues. A PIA isn't a compliance check, it isn't for approval; it is about mitigating risk and improving design.



In some instances a PIA can completed in a few lines and in others it may be a 60 page report. The important thing is the privacy risks are considered and that the privacy impacts are justified.

The basic requirements of a PIA are that it must include a description of the existing state, the change (including the justification), the effect, and the outcome.

Why do a Privacy Impact Assessment

PIAs improve MBIE's ability to manage privacy, which is critical to us meeting our objectives. Some reasons to do a PIA include:

Required by law

MBIE is required to complete a PIA in some situations. For example, the Immigration Act requires it for some biometric data uses.

Manage risk

To help MBIE manage privacy risk. Privacy risk is the risk of harm or distress to a person through dealing with their information or otherwise intruding.

Identify privacy enhancing features

Privacy enhancing features often emerge through the PIA process.

Identify privacy vulnerabilities before they become issues

By identifying vulnerabilities before they become issues you can avoid rework, harm, costs, and complaints.

Meet your obligations

PIA's also support you and your business managers to meet your obligations for your business areas to respect privacy.

Finally and most importantly, privacy is about people. People care about how we deal with their information. People feel a close connection to their personal information. Treating it well is treating them well.

When should you do a PIA?

You should do a PIA whenever you change any aspect of how you collect, store, use, share, or dispose of personal information. You should do a PIA when you can still change the initiative; otherwise, it is effectively a compliance check.

The process can be iterative. You can start by reviewing the themes your initiative is likely to engage. Once that is done, you might develop a policy paper and refine your assessment. Then when you decide to go ahead with an operational product, you can consider privacy in that design. Each iteration enhances the product and the analysis. You don't have to have the full picture from the start.

Is it necessary?

MBIE has a tool called a [Privacy Threshold Assessment](#). A business owner is required to complete a threshold assessment when change or initiative will affect personal information. If the tool calculates a medium or high risk a privacy impact assessment must be completed.

I am getting advice to do a PIA but the initiative is existing practice



This may be a great opportunity to review your existing practice. From time-to-time things come about which may have slipped through the cracks, or may be undocumented accepted risks. When these arise, it is worth considering whether there is an issue and whether the situation remains acceptable.



Example: The Incorrect Address Form

A company rolled out new software for customer enquiries. Soon after, it was identified that there was an increase in privacy breaches. But it wasn't until a significant complaint required settlement that the issue was investigated.

Initially the mistakes were attributed to human error. The error was that customer service staff were sending information to the wrong addresses. On further analysis it was identified that the system often displayed the address of the previous files on screen in a history tab. This was so that staff could click through to their previous work easily. It also meant staff were sending information with the incorrect address presented on the screen.

The solution was to remove addresses from the history tab. The software was updated and the issues went away. Problem solved, but the complaints, settlement and cost of customising the software could have been avoided had privacy been considered in the design.

Your PIA Team

All PIA's require a range of expertise. This could include security, privacy, process and project expertise. Sometimes you can find this expertise in one person, other times you can't. It is all about ensuring your PIA is the right-size.

The Privacy Team are available as a form of assurance and expertise, they can review your drafts and advise on where to focus, but they cannot complete the PIA for you.

When should you get external help?

In some instances external help is useful. First, when the initiative does not have internal resource capable of completing the PIA. Second, when the initiative requires external expertise. Third, when the initiative has privacy implications that suit a robust independent opinion.

The first situation is the clearest cut. If you do not have the resources internally then there is no alternative. The remaining two situations are more difficult and it would be worth consulting with the [Privacy Team](#). It is also worth remembering the advantages of keeping PIA's in-house. These include subject matter expertise, less time taken to learn MBIE's context, and maintaining a close proximity to the change programme.

When should you consult with the Privacy Commissioner?

Sometimes it is worth consulting with Office of the Privacy Commissioner—or the law requires it. They can review documents and provide guidance. If you think this is appropriate, talk with the [Privacy Team](#).

Keep in mind, turnaround for consultation with the OPC ranges between 2 - 8 weeks.



Does the Office of the Privacy Commissioner Approve PIA?

No. While they may review a document, they will not approve a PIA and we do not ask him to.

Part Two: Key concepts

Privacy is about people’s reasonable expectation of inaccessibility and control of information about themselves.


New Zealand has a Privacy Act. It contains 13 Information Privacy Principles that establish how people’s information should be collected, used, disclosed, and stored. It also says that people should generally have access to their own information.

The Act appoints a Privacy Commissioner. The Privacy Commissioner’s function isn’t just to enforce compliance with the Privacy Act, it is also to promote privacy.

The Act is not everything the law has to say about privacy. There are also privacy protections contained in other statutes such as the Crimes Act, the Harmful Digital Communications Act, and the Electoral Act. When it goes wrong, there is a risk of breaking the customer’s trust and confidence and even the possibility of litigation. For this reason, MBIE’s [Privacy Policy](#) states that we take a broad interpretation of privacy.


Personal Information

The Privacy Act regulates ‘personal information’. Personal information is something that tells us something about an individual. The information does not need to name the person, as long as they are identifiable.



Personal information is “Information about an identifiable individual”. The person does not need to be identified, secret, or particularly private.


It must be ‘about’ the individual, so just because a person is named doesn’t mean the information is about them, for instance it could be about a company. In this way, what is personal information is contextual.



New Zealand does not regulate privacy based on Personally Identifiable Information (or PII) or Sensitive Personal Information (SPI). These terms are frequently used overseas. If you see these terms in a document, watch out, as this may mean the document you are reading is not relevant to New Zealand.

Collection

Collection is about gathering information. It can be done in many ways. For instance, it can include a form or an electronic application programming interface (API).

	<p>Many times people do not think of searches as a collection. Another example commonly missed is when moving a storage device from one agency to another, the information on that storage is both collected and disclosed.</p>
---	---

Collection involves an active step. So, sometimes information we do not collect may end up in our possession. For example, a customer could send MBIE an unsolicited letter of complaint detailing sensitive information. This is not collection but it is still personal information and the other information privacy principles still apply.

While collection involves an active step, this does not have to be for the particular information received, just the broad class of information sought. For example, a CCTV camera captures a broad range of information, and all of that is considered as collected, regardless of whether it is the particular information sought.

Use

The Privacy Act does not define use, but in practice, its definition is a broad one that covers all handling of information for any purpose. It includes automated decision-making, data manipulation, and combination. For instance, if MBIE takes one database and matches it with another, then that is use.

Disclosure

Disclosure is also a broad concept. It covers sharing, trading, and matching information.

Contracting Outside MBIE

The Privacy Act applies to MBIE, the services we provide, and how we go about providing those services. We are responsible for the delivery even if we ask others to do something for us. For this reason, it is important that we consider privacy in procurement, and ensure that outsourced services are delivered with care and concern for personal information.

Consent

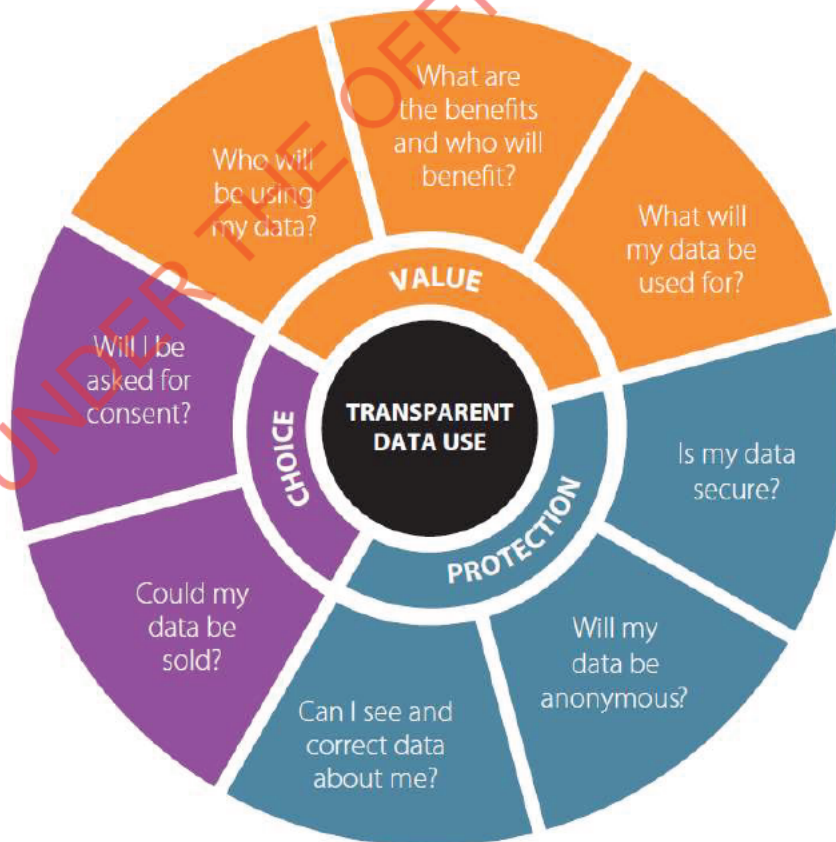
Consent has a broad part to play in privacy. A customer's free and informed consent is perhaps the most significant risk reduction for the use of their personal information. The Privacy Act also includes a range of exceptions when an agency has a person's authorisation, and consent helps with that authorisation.

In order to gain consent, ensure that your collection statement:

- Presents a real choice with options
- Requires an opt-in or positive action, rather than opt out
- Is clear, concise, and separates consent from other terms and conditions
- Avoids making consent a precondition for service unless necessary

Positive consent is best for customers. It is also best for us as it creates positive evidence that we can rely on.

The Data Futures Partnership produced the following tool for consent and transparent data use. Their research found that customers expected the following questions to be answered.



Information sharing

Considering privacy for information sharing is unique. This is because there is a particularly focused purpose, and there will be another agency involved. For this reason, we have the following tips:

1. Start with a broad optimistic view of what will be included in the sharing. It is easier to take information out of the analysis than to put it in. So start broad and refine the PIA as the negotiations progress.
2. Information sharing is highly regulated. Start discussions with Legal Branch early on to understand any hard limits to your information sharing.
3. Consider the technical implications. Often software incompatibility and classification differences cause issues late in projects.

Publishing the Privacy Impact Report

Sometimes there are questions about whether to proactively publish a Privacy Impact Report. Publishing a privacy impact report can have benefits, such as transparency and demonstrating a commitment to privacy. Still a PIA must contain a fair analysis of privacy risk; not a sales pitch. The business unit with ownership of the initiative should decide whether to proactively publish the report.

Part Three: Question-by-question

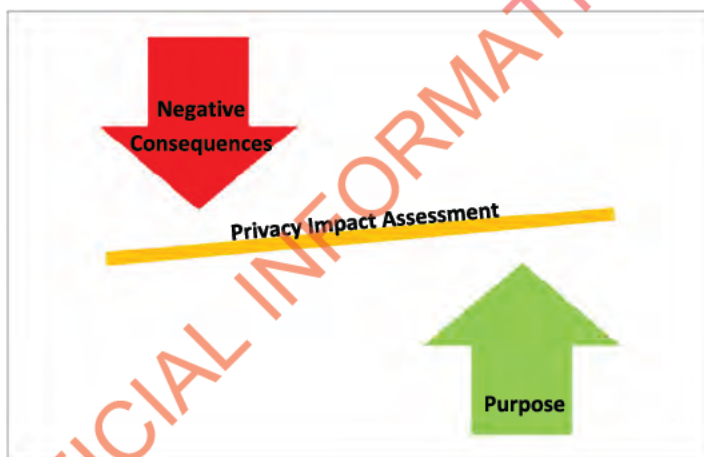
This section goes through the PIA tool question-by-question. Don't feel obliged to read it all, jump to the section that applies to you, or flick through it as you complete the PIA.

Initiative Overview

The first section of the PIA focuses on purpose. This is a time to consider why you are doing what you are doing. Later you will be balancing your information processing against this interest.

This question shows the contextual nature of privacy. For example, the justification of saving lives will legitimise information processing further than user experience will. For this reason, it is important to define the purpose clearly, because everything else flows from it.

This is also the stage you can start thinking about your data flows— this is how your data will be handled, stored, and transferred. You can create data flows using sophisticated software like Visio, or you could use a pen and paper.



Question– Description

What is it your initiative is doing, is it a project to build houses, or a research proposal to investigate the genetic makeup of New Zealand?

What will be the secondary consequences?

Question– what is the reason for the change?

As above, this is the beginning of understanding your purpose. This is important, as this is what the negative consequences and risks will be balanced against.

Question– Will this change how personal information is dealt with, if so how?

This is an opportunity to think about how the initiative will change how MBIE deals with personal information. Are you going to collect more or less personal information? Will it be more secure or less secure? Will information traditionally stored in New Zealand be outsourced overseas?

Keep this high level, as you will consider the specifics further on. If necessary, you could come back to this question once you have completed the following sections.

Question– Attach any diagrams which show how the information will be stored and transferred.

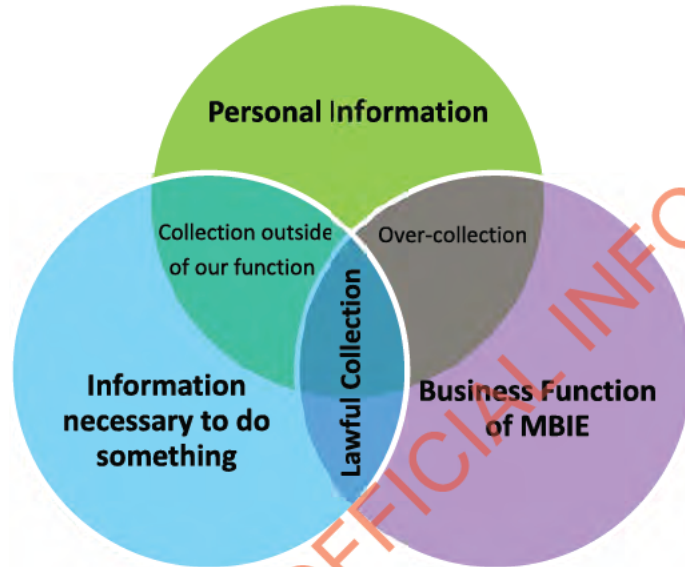
Attach here any diagrams or data flow diagrams that show how information will be handled in your process. As mentioned above, these could be Visio mock-ups, or they could be pen and paper drawings.

Principle 1

Principle one is about how, what, and why your initiative collects information. The flipside of principle one is the irrelevant, unnecessary, or excessive collection of information.



The guiding questions are: is the collection lawful, is it connected with our business functions, and is the collection necessary for that function.



There are no exceptions to the principle. That means that a customer cannot authorise an agency to collect more information than is necessary for a legitimate business purpose, this is particularly important in research and investigations.

For example, a customer authorised an insurance company to speak to her doctor about a medical claim. The insurance company got her to sign an “anything” authorisation, that granted them access to any information. The insurance company then requested the customer’s full medical file. This was a breach of the customer’s rights, because the insurance company had no need for the full file; it was not necessary for the processing of the medical claim. The insurance company therefore had to settle the complaint.

<i>Identifying issues for Principle One</i>	<i>Common mitigations</i>
<ul style="list-style-type: none"> • Personal information is collected without a clear purpose or authority. • The information is unnecessary for the purpose it was collected. • Decisions affecting the individual use irrelevant information. • The individual feels a loss of control over what information is collected. • Sensitive information is not identified as requiring special consideration. 	<ul style="list-style-type: none"> • Limit the information collected to what is truly necessary to achieve the purpose of collection • Clearly state the purpose for collecting the information. • Make it opt-in. • Only have room for that information which you require.

Question 1.1 – What categories of personal information will be collected?

Think about the categories of information that will be collected. Categories of information are useful to start thinking about the privacy cost or sensitivity of information. For instance, generally, health information is more sensitive than political preferences and employment information is more sensitive than purchase history.

Information categories are useful as a shortcut to consider a reasonable expectation of privacy, but are not conclusive, as there is not a strict hierarchy and the sensitivity of information is still contextual. For example, health information could be someone's HIV status, or that someone had a cold last week (one is highly sensitive, the other less so).

Question 1.2– List the personal information in these categories and highlight personal information that may be considered particularly sensitive

List the information in the categories above. Keep in mind some information may not be asked for directly, but is created by combining other information (such as eligibility for a benefit).

Part of this question is noting sensitive information, which is information that people would generally consider being more private such as ethnic origin, religious affiliation, finances, medical records, or information about children or other vulnerable people.

Sensitive information includes information that if released could cause harm, significant stress or inconvenience. The key question is harm. Information is sensitive if it is possible or likely that it will result in harm. By identifying the data items that may require special care, it will be easier to consider other requirements later in the process.

If in doubt, ask the [Privacy Team](#) to help identify data items that may be sensitive.

Question 1.3 – What is the primary purpose for collecting this information?

Consider the purposes for which you are collecting personal information.

If the purpose is defined too narrowly, you may be unable to use information in the way that you might want to in the future. If defined too broadly, the purposes may be meaningless and MBIE could be over-collecting information. This section will be helpful when you write your privacy statement. A clear purpose creates trust and shows you know what you are doing.

Describe whether you believe each data field is necessary for the initiative. Note any fields that could be unnecessary because the purpose of the initiative can be achieved without them.

Include any legislative or regulatory purposes.

Question 1.4 – How else will this information be used?

Please consider evaluation, quality assurance, and investigations.

Question 1.5 – Is this information MBIE has not collected before?

Question 1.6 – Will any of this information collected be mandatory?

Consider if this information will be collected either for the provision of a service or collected under compulsion regardless of the authorisation of the person the information is about.



Privacy Impact Assessment Guide

Question 1.7 – Conclusion: All information collected will be necessary for a lawful business purpose.

True/False

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Principle 2

The best source of information is usually the person the information is about. Requesting the information directly from the person also helps them to feel engaged with the process. In some circumstances, it is detrimental to collect information from the person so principle two has some exceptions.

Exceptions to Principle 2

The information is publically available

There is no single answer to what is publically available; it means anything the general public could access. This includes papers, magazines, public registers, books, or newspapers.

What about websites? Generally accessible websites with no content restrictions such as sign up and logins have previously been considered publically available. Websites that have restricted access, such as social media are more complicated and require case-by-case consideration. That consideration should consider the level of accessibility. For example, a social media profile with highly limited access may not be publically available. If in doubt consult with the Privacy Team.



Publically available information is exempted from Principle 2. This often causes issues because people mistakenly believe publically available information is exempted from the whole Privacy Act. This is not the case.

Collection is authorised by the individual

Another exception is where the individual authorises the collection. Authorisation requires some active step of the person allowing the collection. It is usually best practise that any authorisation is in writing as this creates evidence.

Collection is for the maintenance of the law

To enforce the law sometimes an agency needs to collect information from other sources.



It is difficult to claim this exception unless there is an ongoing investigation of the specific individual. Other evidence should also support the collection. For example, this exception would not allow MBIE to collect the employment records of all New Zealanders in order to assess compliance and prosecute offenders.

Better information that wouldn't prejudice the individual

Sometimes other people have clearly better information than the person it is about. For example, a parent may know more about a child's medical condition than the patient. Here, you can collect information from the person with better information but only if the information that could not possibly prejudice the individual.

Other Exceptions



Other exceptions exist (see Questions 2.3). If you believe that your initiative would be better if it collected information from a source other than the individual then discuss this with the Privacy Team or investigate additional exceptions.

Question 2.1 – Who are you collecting this information from?

For each data category, consider who the information is being collected from. Keep in mind that in some circumstances information can be about multiple parties.

Question 2.2 – Will the personal information be collected directly from the individual, If you are not collecting the information from the individual directly, what is the justification for this?

If you are not planning to collect information directly from the individual then document the source. For example a spreadsheet, a public register, a person or business unit within MBIE, or an informant or witness.

If you have listed sources above that are not the individual discuss the justification and whether any exceptions are apply. Exceptions include:

- The individual concerned has authorised the collection from someone else
- The information is already publicly available
- If collection from another source won't prejudice the interests of the individual
- The information won't be used in a manner that identifies the individual concerned (e.g. for statistical or research purposes)
- Collecting from another source is necessary to maintain or enforce the law, or for court proceedings, or to protect public revenue
- Collecting information from the individual concerned isn't reasonably practicable in the circumstances



If you want to rely on an exception you must have evidence and a reasonable basis for believing an exception applies. Remember to include any verification process, if completed.

Identifying issues for Principle Two

- Individuals may not be aware that information is being collected, who will use it or what it's being used for. If they become aware later, they may be surprised or upset
- Collecting information from a third party could perpetuate and compound any errors that are already in the data
- Information may be out of date or irrelevant for the intended purposes if it is used outside the original context in which it was collected
- Individuals won't be able to update their information if they don't know we have it

Common Mitigations

- Ensure information is only collected directly from the individual unless there is a good reason not to do so
- If information is collected from a third party, make sure the individual knows that you are going to do that unless there is a good reason not to tell them
- Have a clear privacy statement saying where personal information will be collected from
- Provide people with a way to see the information you hold about them (like a dashboard) and give them an opportunity to correct it if it is wrong

Principle 3

When collecting information from an individual agencies must be open about what is going to be done with it.

With limited exceptions, MBIE must take reasonable steps to ensure that a person is aware:

- That the information is collected by MBIE
- The purpose
- The intended recipients
- MBIE's address and the name and address of any other agency that will hold the information.
- Whether the collection is authorised or required by law.
- Any consequences of not providing the information.
- Their right to access and correct the information.

One way to think of this is as the no-surprises rule. People should not be surprised by how we are handling their information. This leaves them in an empowered position to control their own information and reduces the risk of a complaint.

The Department of Internal Affairs publish [additional guidance for New Zealand Government websites](#) that reflect the requirements of the Web Usability Standards.

What does it mean to take "reasonable steps"?

This depends on the initiative; including considering what is being collected, the potential prejudice to the individual, and who will receive the information.

Good Practice

It is good practice that collection statements are in writing. The statement should be separate from other terms and conditions and freely available prior to the collection of information. The statement should be Plain English and in a clear legible font. In some situations a sign will be effective and reasonable, for instance with CCTV.

Better practice

Privacy Impact Assessment Guide

Best practise is to provide inline layered privacy statements. These involve breaking up the privacy statement and placing these in line with the actual collection form.

The Contextual Form	
For instance you could have a form that tells the user why each field is relevant and what happens if they don't provide it. For instance, your complaint form could say:	
Contact details	
We collect your contact details to contact you, you can complete this form without providing contact details but we will not be able to progress your complaint.	
Name	<input type="text"/>
Email or phone number	<input type="text"/>
Some people may want to note a concern without being identified. So the form allows the user to decide how their information is used. They may choose not to provide the information if the outcome is not one that they want.	

Question 3.1 – What will you tell individuals about the collection of their information?

This question will assist you to draft your privacy statement. Consider first, whether people have already been told that we are collecting their information, if so, is the current privacy statement sufficient?

Second, consider if an existing MBIE process already collects similar information, if so, could this be used or adapted for your initiative? If you are stuck, the [Privacy Team](#) will be able to assist.

Question 3.2 – How will you tell individuals about your privacy statement?

Keep in mind the best practice discussed above on page 16. It is worth considering the cost of the solution and the practical implications.



Example: The Call Campaign

An agency was designing a call centre campaign. A collection statement was required. There were two options: a recorded message or a call script. The company was concerned that quality assurance showed only 80% compliance with a similar call script, so chose the recorded message. The recorded message took longer to set up but once implemented ensured consistency. It was also found that the recorded message took less time to deliver than the call script, so improved call efficiency metrics. In this way, the best practice privacy solution also saved costs.

Question 3.3 – What steps will you take to ensure that people read and understand the privacy statement?

When an agency collects personal information directly from the individual concerned, it must take steps to make sure that person knows details such as:

- Why the agency is collecting the information
- Who will have access to the information
- Whether they must give the information or whether this is voluntary
- What will happen if they don't provide the information

Identifying issues for Principle Three	Common Mitigations
<ul style="list-style-type: none"> • The statement isn't accessible. • People often don't read the statement. • Individuals may be surprised by new collection • The individual may lose trust in us, leading to a lack of engagement which may affect our ability to achieve our objectives 	<ul style="list-style-type: none"> • Make sure the privacy statement is in plain language • Explain the benefits of providing information. • Make it clear if there is a legal authority for collecting the information • Ensure changes are reflected in the privacy statement.

Principle 4

Principle Four is perhaps the simplest requirement but also the one with the biggest ramifications. It requires that we do not collect information unlawfully, intrusively, or in an unfair way.

What is intrusive or unfair is highly connected with what is considered 'normal'. This requires consideration of social norms and standard practice. What is intrusive is not the information collected, but the information in the context of the particular collection. For example, what is intrusive for a co-worker to ask may be very different for a doctor.

Law enforcement activity and searches

This principle is particularly important in the context of involuntary law enforcement activity. If your initiative involves developing an investigation process then you need to consider whether your investigation involves searches. Just because the collection is permissible under the Privacy Act does not mean that the collection is not a search. The test is whether the information you are seeking is something over which there is a reasonable expectation of privacy. A reasonable expectation of privacy means, if a reasonable person plucked from Lambton Quay and put into the situation would consider the situation private— for example bank records or searching someone's home.

If there is a reasonable expectation of privacy over information and you require that information then you need to consider whether that search is reasonably justified. It is important that you consult with the Legal Team.

Accidentally intrusive collection

People rarely intend to intrude; often it is a mistake. A common example is that there is a justifiable reason why a CCTV camera is necessary, but improper placement means that it collects a lot of information that is not justifiable and is potentially intrusive.



A question to ask is— would people consider this creepy?

Identifying issues for Principle Four	Common Mitigations
<ul style="list-style-type: none"> • Recording equipment is badly located or improperly adjusted resulting in an over- 	<ul style="list-style-type: none"> • Think carefully about the different options available for collecting information and

Part Three:
Question-by-Question

Privacy Impact Assessment Guide

<p>collection of information or an unjustified intrusion</p> <ul style="list-style-type: none">• Information is collected unfairly by the use of duress, coercion, or deception• Information is collected from an individual who mistakenly believes they have to provide it because of a false representation	<p>choose the least intrusive option that fulfils the purpose</p> <ul style="list-style-type: none">• Check that every field on a form is necessary• If providing information is optional, make this clear• Provide a written document for investigation interviews detailing the process and the purpose
---	---

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Question 4.1– Describe how the information will be collected

Discuss how the initiative intends to collect information. Consider if this is a form and manner of collection that people expect in their day-to-day life. If not, is it something a reasonable person would consider natural or expected. This isn't a question of whether they want it to occur, just would they expect it to occur.

If your initiative involves the covert collection of information explain why.

Is it unlawful?

Any collection of information contrary to the law will also be a breach of principle 4.



Example: The Flat Inspection

A Property Manager entered a flat without providing the tenant adequate notice. There, they found the flat to be messy and unventilated. They took photos of the flat and left intending to take the matter to the tenancy tribunal.

The tenants complained. The Privacy Commissioner found that the entry to the flat was unlawful and therefore the associated collection of information was a breach of principle 4.

Is it unreasonably intrusive?

Intrusive collection usually involves covert or disguised surveillance. Things that raise concerns are long-range photography, the use of shotgun or remote microphones, or information capture in particularly sensitive areas, such as bathrooms, or changing areas.

Is it unfair?

Unfairness usually arises when there is coercive, manipulative, or threatening behaviour.

You need to take particular care to consider if your collection practices are fair and reasonable if you are collecting personal information from children and young people.



Example: Misleading Conduct

Misleading conduct is sometimes not unfair, especially in investigations. For example, in one case, an investigator posed as a customer, misleading the individual as to the purpose. This was not a breach of principle 4. Law enforcement will also often not disclose that they have received a tip-off or independent corroboration when interviewing a person. In such circumstances, the Privacy Commissioner will consider:

- The purpose of the collection
- The extent the person was misled
- The duration of the deception
- The advantage the agency received

Question 4.2 – Is any of the information, not collected directly from the individual it is about, information over which there is a reasonable expectation of privacy?

Examples may include:

- The contents of a person's phone
- Photos of a person's house
- Medical information

Please talk with the Privacy Team if you have any doubt about the answer to this question.

Question 4.3 – If you are using any analytic information, how will you tell people that this is happening, and why?

For example, do you have a cookie policy on your website?

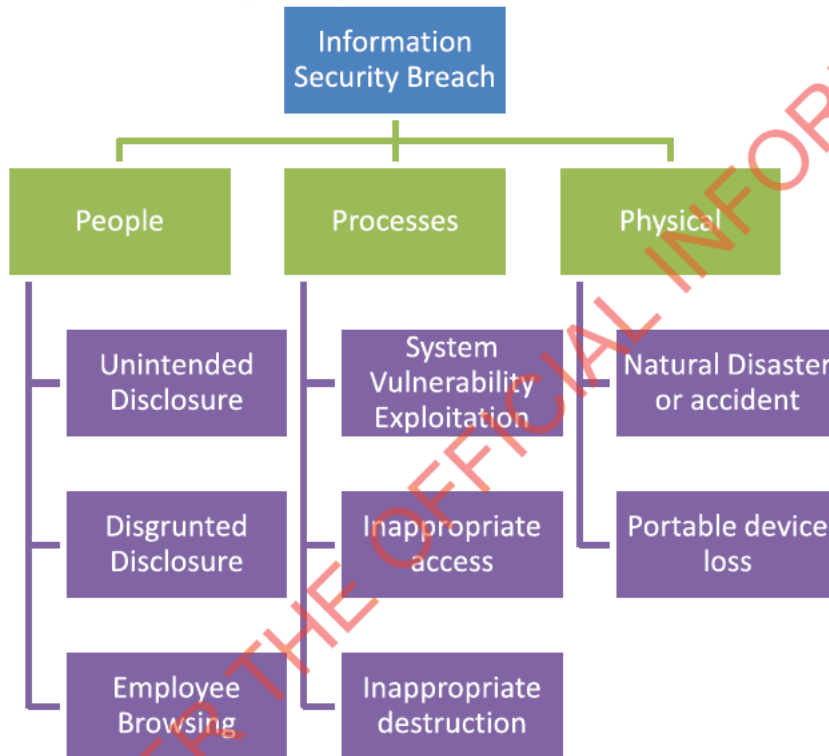
RELEASED UNDER THE OFFICIAL INFORMATION ACT

Principle 5

This principle requires us to look after information. This includes protecting it from the full range of risks that come from storing and transferring personal information.

The [Information and Data](#), [ICT Security](#), [Protective Security](#), and the Privacy Team can help you to ensure that your solution adequately protects information.

Common breaches of principle 5



Identifying issues for Principle Five	Common Mitigations
<ul style="list-style-type: none"> • Failing to limit edit-access to data. • Not monitoring access • Shared workspaces leading to inappropriate permissions • Staff inappropriately accessing information (employee browsing) • Testing and training environments may expose personal information • Hacking, system failures, data compromise or breaches are not properly managed • Personal information being stored in a country with inadequate protections 	<ul style="list-style-type: none"> • Encrypted file transfers • Prohibiting the use of unauthorised removable devices, like USB sticks <ul style="list-style-type: none"> ▪ Documented user access controls ▪ Penetration and other security testing ▪ Internal audit, investigations and/or compliance staff who audit information

Question 5.1 – Where will personal information be stored? For example, MAKO, or the Cloud?

Describe how personal information will be stored. Work with subject matter experts on storage if necessary. It is worth considering the cost and security controls of the solution. Also, consider what would happen if people bypass safeguards and skip controls.

Question 5.2 – Who will be responsible for keeping it safe during storage?

Consider and discuss the responsibility for ensuring that information is safe and secure. How will the responsible person be enabled to maintain safe storage?

Ensure the safeguards are right for the risk. For example, in one high-risk process the relevant manager must approve all information accesses, individually one-by-one. In another, a low risk process, that could be completely excessive. It all depends on the context.

Question 5.3 – Describe your engagement with ICT Security and whether a C&A process is being undertaken?

Indicate whether you have completed the Certification and Accreditation (C&A) process with IT Security. If you have, attach the documentation. You do not need to repeat the technical controls in this assessment.

Question 5.4 – Who will have access to the information?

Consider who needs access to do their job, including 3rd parties, and how you will limit access.

Question 5.5 – How will inappropriate access to be identified and reviewed?

For example, spot-check quality assurance, regular audit, and contractual monitoring.

Question 5.6 – If an initiative/project involves third parties, how will you make sure that any privacy issues are reported to us?

Note any legal or commercial safeguards that apply. For instance, if you have a contract with a third party provided, does it contain agreed privacy standards? Do you have a Memorandum of understanding that details how MBIE and our partners interpret the law? If not, would these be useful or necessary?

The other reason for detailing these now is so that, if anything goes wrong, there is a record of mitigations and safeguards that you can refer to in that moment without having to gather the information.



Are you using new technology or systems? Often these pose unique issues that haven't been considered before.

Principle 6

People generally have the right to access information about them. Having the right to access means having the ability to know, see, or hear what information an agency holds about them. It is important that your initiative makes this possible. And, even better, there are ways to make dealing with access requests easy and cheap.

The baseline is that there should be a process for responding to a request. If the Privacy Commissioner is investigating a complaint about access to information, this will be the first place they look.

How can your initiative make information access easier?

By making information easy to find, access, extract and clearly marking material that should be withheld such as legal advice or confidential material.

Better Practice

Even better practice is to contain the information about that person, along with the information used for any decision in one place. This means that a person processing an access request can do so quickly and easily.

Best practice

The best possible practice is to allow people to control information about themselves using a self-service system. This means that they can access information directly and they don't need to ask us for access. This provides them better certainty and reduces the cost processing requests.

Identifying issues for Principle Five	Common Mitigations
<ul style="list-style-type: none"> • The information is difficult to locate • Confidential and privileged information is mixed in with general information • If individuals cannot easily access their information, this may lead to suspicion and mistrust • A contractor does not efficiently provide information held for MBIE leading to non-compliance. 	<ul style="list-style-type: none"> • Ensure information stored is identifiable and retrievable • Make it easy for people to access their information by setting up a self-service process for them to see the information you hold, including their details and transactions • Make sure that access requests are tracked (they can be verbal or written) • Keep sensitive information separate.

Question 6.1 – Will people be able to access their own information?

Consider and discuss whether people will be able to access their own information. As discussed on page 22, self-service is best practice, but it might not be relevant to your initiative.

Question 6.2 – If not, how will people be able to access their own information?

Describe the process for people to request information about themselves.

Question 6.3 – How will an initiative/project tell people about their right to access their information, and the process to request information?

Consider and describe how people will know about the request process. For example, will the request process be hyperlinked from the privacy statement? Will it sit on the front page of your website?

Question 6.4 – Who will be responsible for responding and the timeliness of the response?

Monitoring information requests and the timeframes is critical for the performance of any information request process. It can take time and commitment. Describe who will be responsible for this. This is the sister question to 6.5 below.

In considering this, consider how many information requests you expect and the resourcing options.



Example: The Hidden Databases

An agency expanded its databases on a need-by-need approach. Each time they added a new database there no thought was given to centralising the data records. This meant when they received large information requests a staff member would have to enter six different databases to access the data for release.

This process considerably increased the time it took to perform access requests, resulting in delays in customers getting information, and many complaints. This could have been avoided if the central systems allowed information to be easily retrieved.

The other common place this issue occurs is with physical records and information sent for archiving. It can result in non-compliance.

Principle 7

Where we hold personal information about a person that is incorrect, that person can request that it is corrected.

We are also obliged to tell that person any action we take in response to their request.

Correction can mean three things:

- 1) We can change the information to say something else.
- 2) We can remove the information altogether.
- 3) We can add information so that the overall record is right.



Sometimes we may disagree, and rather than correct the information, we can attach a correction statement that identifies that the customer has a different point of view.

Why does this matter for you?

If a system or initiative is set up so that records cannot be altered, amended, or added then MBIE will be unable to meet its privacy obligations. Therefore, it is important you consider this requirement in your system design.

This also matters because customers often know best. This means that their view on what the data is or should be is often the best route to accurate and reliable data. Sure, sometimes clients may have ulterior motivations for a correction, but this can be factored into the correction process.

Identifying issues for Principle Seven	Common Mitigations
<ul style="list-style-type: none"> • Poorly managed correction requests can lead to poor quality data • Failing to correct personal information can lead to inaccurate information affecting the individual and the provision of services • Correction may be hampered if data is held by contracted service providers • Poor quality information is passed to other agencies compounding errors and problems for the individual • Information is duplicated in different parts of the organisation but only corrected in one 	<ul style="list-style-type: none"> • Ensure information stored is identifiable and retrievable • Make it easy for people to access their information by setting up a self-service process for them to see the information you hold, including their details and transactions • Make sure that correction requests are tracked (they can be verbal or written) • Keep sensitive information separate

Question 7.1 – Will people be able to correct their own information?

Best practice (and usually the easiest solution) is that people can correct their own information. It is worth considering whether this is possible. If it is, it is also worth considering the cost of the solution. Self-service may cost more upfront, but often it reduces the burden on call centre and data processing staff. This is why the tool starts with considering this option.

Question 7.2 – If not, how will a person be able to request a correction to their own information?

If a person cannot correct their information, how will your initiative enable requests? For example, is there an existing process in place that can be used? Also consider how requests for correction will be identified and actioned.

The [Privacy team](#) may be able to help with finding an existing process.

Question 7.3 – How will you tell people about their right to correct information about themselves and the process to correct their information?

People won't correct their own information unless they know they can and believe it is worthwhile. It is worth considering both issues. The government spends considerable money on misdirected mail, misspent entitlements and updating evidence of identity.



Old or incorrect information also means people miss entitlements they deserve. Letting people know how to update their information and the benefits of doing so helps everyone involved.

Question 7.4 – Who will be responsible for the correction decision and response, and the timeliness of the decision and response?

This is the sister question to 6.4 above. Monitoring correction requests and timeframes is critical for the performance of any information request process. It can take time and commitment. Describe who will be responsible for this.



Example: Date of Birth

A government spent a considerable amount on installing a new system to track identities. When it was launched, it was found the requirement to update an identity record has been de-scoped from the project. This meant that the system created a new identity rather than updating the existing identity. This undermined the point of the system and required a new project to fix the problem. This cost money, time and affected the deployment of the system.

Principle 8

Before we use information, we need to take reasonable steps to ensure that the information is accurate, up-to-date, complete, relevant and not misleading.

This principle is important on two fronts: making decisions using incorrect information is bad for customers, but it also requires rework and can lead to the incorrect allocation of entitlements.

There is no strict test of how accurate information must be. Instead, it depends on the significance of the information and its purpose. The more serious the implications of the information being inaccurate, the more accuracy is required.

Some tools and techniques can assist:

- Record when information is collected
- Record an expiry date (when the information should no longer be used)
- Record how information is collected, so later users can consider its source
- Ring the customer to check important information is valid before using it (for example an old address)
- Remove or correct incorrect information proactively

Identifying issues for Principle Eight

- Incomplete or incorrect information can lead to incorrectly informed decisions
- Information kept too long can be out of date
- Inaccurate information can increase the risk of inappropriate use and unlawful disclosure (such as change of address).
- Updating personal information without maintaining audit trails of the updates increases the risk of unauthorised changes going undetected

Common Mitigations

- If the information was collected some time ago check that it is up-to-date
- Before you take an adverse action against someone based on the information, give them the opportunity to question or refute its accuracy
- Regularly check the reliability of equipment used to collect and process information and consider systemic bias

Question 8.1 – How will you ensure that personal information is accurate, up to date and relevant and not misleading?

Consider how your initiative will maintain and ensure information accuracy.

To do so consider what the impact would be on the individual if their information was not accurate or up-to-date, and is used. Then design a solution that ensures a level of accuracy reasonable for that consequence. For example, if you are sending documents to a victim of domestic abuse that standard of accuracy is significantly higher than mailing out advertorial content.

Question 8.2 – How will you ensure that any underlying assumptions and personal information used is not affected by bias?

Principle 9

The Privacy Act does not set out particular timeframes for how long MBIE should keep personal information. Instead, it requires that we keep information having regard to the purposes for which the information was collected. Once information is no longer required we should dispose of it.

All government agencies have a legal obligation under the Public Records Act 2005 to create, capture and manage full and accurate records of their business activities. This obligation applies to both permanent staff and contractors.

Public records include personal information when it is used to make a decision, or as evidence of work activities. MBIE has a guide on [public records information](#). It also has a [Disposal Schedule](#) which outlines how long MBIE must retain information.

How long you need to keep information may be contained in other legal requirements. These obligations override principle 9.



A common issue under principle 9 is that systems are designed with no ability to delete or remove personal information

Identifying issues for Principle Nine

- Keeping data longer than necessary increases the risk of a data security breach or unauthorised use or disclosure
- Keeping information too long increases the risk it will be out of date, misleading or inaccurate
- The careless or ineffective disposal of records may lead to unauthorised access or disclosure
- Destroying information when you still need it creates problems – if there is no plan, there is more likelihood of a mistake

Common Mitigations

- Where information is no longer needed for the purpose for which it was collected, but needs to be retained (e.g. to comply with specific legislation), add safeguards to remove it from operational use
- Destroy transactional data when the transaction is complete and only keep metadata
- Design the system to include a facility to flag records for review or deletion when the minimum retention period expires
- Minimise the amount of information to be disposed of by minimising the amount of information collected

Question 9.1 – How long will the personal information be retained?

Describe how long you need to keep information for the purpose it was collected. Consider any legal, policy, or technical reasons. It is worth pausing on this question to consider the purposes for the information that you detailed above and how long each of these will last.

Question 9.2 – How will you identify information that is ready to be disposed of?

If information is collected and stored in a single folder without clear labelling it is difficult to identify what should be disposed of and when. Consider how you will identify the information ready to be disposed of.

Question 9.3 – How will personal information be disposed of when no longer required?

Consider the processes for disposal. Describe how the disposal of data will be managed securely at the end of the retention period. Include any third party acting on MBIE's behalf.

Principle 10

The general rule is that personal information collected for one purpose should not be used for another purpose.

There are exceptions that apply to this general rule.

The information is publically available

If the information is publically available then you can use it for another purpose if doing so is reasonable and fair.

The flipside of this exception is that in some circumstances using information that is publically available can still be a breach of the privacy principles if it is unfair to use the information in a specific way. This issue is usually only relevant with sensitive information (such as historic criminal convictions). For example, it may be unfair to consider a historic photo someone has posted on social media in a promotion decision even though it is public information.

Maintenance of the law

The information can also sometimes be used if it is necessary to maintain the law, including the prevention, detection, investigation, prosecution and punishment of offences. For instance a person cannot complain that the Inland Revenue is breaching their privacy because Inland Revenue are investigating their tax return.

The information is used in a non-identifiable form

Information can be used in a form in which the person is not identifiable, for example research, statistics, or a fully anonymised study. If you intend to use this exception you will need to justify that the information is not capable of re-identification.

Identifying issues for Principle Ten

- If MBIE uses information for a reason other than it is collected individuals may be surprised or upset by the unanticipated secondary use
- If collaboration, outsourcing and information sharing with other agencies and authorised third parties is inadequately managed, then personal information may be used inappropriately
- Personal information collected on behalf of another agency is used without legal authority.

Common Mitigations

- Clearly define the proposed information use
- Develop robust access control protocols that limit access on a 'need to know' basis.
- Ensure that access controls are updated regularly to accommodate departing staff, changes in roles and expiry of contractor's terms
- Provide for regular auditing of access by both authorised and unauthorised users

Question 10.1 – How will you ensure that the personal information is only used for the purpose for which it was originally collected or where there is a justified exception?

Consider how you will ensure that information is only used properly. Linking back to Questions 1.3 – 1.4 or the original purpose for collection.

Question 10.2 – How will you record the reason for which personal information was collected?

For principle 10, the best place to start is with an optimistic view of where information would be useful, only then consider whether that use is justified, and only then consider if there is a relevant ground in principle 10. This is because we often hear people say that they can't use information how they want to because of the Privacy Act even though no such restriction exists.

If needed, go back to the initial purpose for collection. Sometimes new purposes are found at this stage, so don't feel stuck by your initial thoughts on the purpose for collecting information, so long as your changes to the purpose are justified then change them.

If you are planning to use information for a different reason to the one you have told the individual you will need to justify it. Justifiable exceptions include,

- That information is publically available and it is not unfair or unreasonable to use the information for the purpose you intend;
- That the individual has provided further authorisation;
- That the purpose is necessary to:
 - Protect public revenue,
 - Maintain the law,
 - Conduct court proceedings,
 - Protect public health or safety,
 - Protect the life or health of the individual concerned or another individual;
- Using the information where the individuals cannot be identified;
- Using the information for statistical or research purposes where the individual will not be identifiable in any published form.

Principle 11

Principle 11 requires that we don't disclose information unless we have a reasonable belief that we have a lawful basis.

A reasonable belief is a belief that we can justify in some way. Further, it is something that a random person would agree is more likely than not.

There are a number of lawful basis. The grounds contained in the Privacy Act include:

- That the disclosure is for one of the reasons the information was collected.
- That the information is publically available, and in the circumstances disclosure is not:
 - Unfair
 - Unreasonable
- That the disclosure is to the individual or an authorised individual
- That non-compliance is necessary to,
 - Avoid prejudice to the maintenance of the law
 - Enforce a law imposing a pecuniary penalty
 - Protect the public revenue,
 - Conduct court proceedings.
- Disclosure is *necessary* to prevent or lessen serious harm to public health, public safety or the individual concerned.
- Disclosure is in a form where the person cannot be identified
- Disclosure is for the purpose of selling a going concern or business.
- Disclosure is required or authorised by any other enactment.

The information

It is important to remember that the justification is limited to the specific information necessary for that disclosure. For example, it is not always necessary that a full file is disclosed when a part of the document would meet the same purpose. So, consider sharing a part file or specific information.

This limited disclosure becomes even more important when the disclosure is not for the purpose it was collected or to the person. Often these situations (such as threats of self-harm or harm to others) are difficult to deal with in the moment. For this reason, it is worth considering whether your initiative needs a business process or rules for special grounds of disclosure.

Question 11.1 – Will the information be shared with any other person or agency (other than the individual it is about)?

The best place to start is with the benefits of sharing information rather than the disclosure grounds. Start thinking optimistically about how disclosing information would benefit the initiative. From there you can start considering disclosure grounds.

Question 11.2 – If yes, describe the reason for it being shared?

The benefit of shaping the information sharing around the need rather than the grounds is that you end up with an initiative that shares information as much as is necessary, beneficial and lawful. It also avoids a common issue we see, that people say they can't share the information they want to even though there is a perfectly justifiable legal basis.

Question 11.3 – If information will be share, describe how the information will be shared?

Describe the means by which personal information will be shared. Consider any security issues that are likely with this disclosure. For example: API, or SeeMail.

What controls will you have in place to protect this sharing? For example, will third parties you share information with be allowed to share it onward to another party? If you are sharing information with a third party, will they have appropriate safeguards in place?

Question 11.4 – Will any information be disclosed or ransferred offshore?

For example, will personal information be stored offshore by a 3rd party cloud service provider?

Question 11.5 – If information will be transferred or disclosed offshore, will MBIE maintain equivalent safeguards over the information and that people's privacy rights are maintained?

Identifying issues for Principle Eleven	Common Mitigations
<ul style="list-style-type: none"> • If personal information is disclosed without a disclosure ground it could lead to embarrassment, stigma, or damage to an individual's reputation. • If authorisation for MBIE staff or third parties to access personal information is too wide and not maintained, then personal information may be used or disclosed unlawfully. • Re-identification may be possible. If sensitive information about a person's 	<ul style="list-style-type: none"> • The solution should enable appropriate role based access to personal information. • Implementing business processes to ensure that information will only be disclosed and shared within Information Sharing Agreements. • The initiative will ensure that appropriate privacy protections are transferred along with the information disclosed, through

<p>activities or whereabouts fall into the wrong hands, concerns over personal could safety arise.</p>	<p>contractual arrangements or terms and conditions in sharing agreements.</p>
--	--

Principle 12

This privacy principle adds an obligation on any New Zealand agency to take extra steps when it considers sending personal information to an offshore entity.

The agency must be satisfied that the personal information about New Zealanders is going to a place that has comparable safeguards. If it can't do that, the agency needs to be very explicit with every individual involved and make sure that they express their authorise taking their risk of overseas disclosure. The persons understand the consequences of the disclosure and waive the protections.

Question 12.1 - Will any information be disclosed to a person or entity offshore (not including cloud storage solutions)? If yes, which country?

For example, publishing information to a website or through use of online surveys.

Question 12.2 - If information is to be disclosed offshore, what privacy protections will be in place?

For example: encryption, contracts or agreements that specify privacy and information security measures.

Principle 13

A unique identifier is a number or code that is assigned to an individual, such as a customer number, IRD number or drivers licence number (for the avoidance of doubt, a person's name is not a unique identifier).

Principle 13 requires that unique identifiers should not be assigned unless necessary—for instance for administrative efficiency. Necessary means it has to be more than helpful.

It also stops an agency from using another agency's unique identifier unless it is one of the purposes for which it was the unique identifier was assigned. For instance, we cannot use an IRD number as an identifier for a non-tax related purpose.

We also have to have a reasonable belief in the identity of an individual before we use an identifier assigned to them.

Question 13.1 List any unique identifiers being used and describe why it is necessary to use them

If you are going to use a unique identifier consider how it will be used, where it originated from, and whether it is truly needed. It is worth considering what will happen if a user refuses to provide the unique identifier.

If you are using a unique identifier for any statutory reason, note that here.

Question 13.2 What steps will be taken to prevent the misuse of unique identifiers?

Agencies need to take reasonable steps to protect unique identifiers from being misused. This is to reduce the frequency and impact of identity theft.

<i>Identifying issues for Principle Twelve</i>	<i>Common Mitigations</i>
<ul style="list-style-type: none"> • Service provision is conditional on the supply of a unique identifier assigned by another agency • Unrelated information about an individual can be linked by association through the use of another agency’s unique identifier • Use of the same unique identifier by different agencies creates a de-facto universal unique identifier 	<ul style="list-style-type: none"> • Only collect a unique identifier provided by another organisation if you have specific legal authority to collect it and you need a record of the identifier to perform your function • Check that the unique identifier has been designed with your intended purposes in mind – is it fit for the purpose to which you are putting it? • If you need to verify eligibility by using an identifier issued by another organisation, note that the identification has been sighted but do not assign the number to the individual for your own use

Governance & assurance issues

Describe how this initiative affects the way that MBIE manages the privacy of personal information?

This question should flow from the previous sections. At a high level, how does your initiative change things? It could be that it doesn’t at all, or it could create additional risks needing mitigations and management. It could be that it improves standards.

How are the specified risks and controls going to be managed?

This isn’t asking about your specific risks and controls. It is asking how you will *manage* those risks and controls. How will you ensure risks are maintained, updated, and how you will assure yourself that controls are working as intended.

How will the risks and controls be reviewed?

While controls are useful, from time-to-time they need updating. How will you go about updating those controls (i.e. will there be a responsible manager, a governance role or a, periodic review?)

Part Three:
Question-by-Question

How will this initiative impact on any other process or initiative?

This is a difficult question, as often we don't know what else is happening across MBIE which could be affected by our work. For this reason it is important to spend some time on this question. A common example is that an initiative relies on data processing by another team that isn't aware of or resourced for the change.

Return to your process flow and consider the resources required for each stage.

What other system or process assurance will be undertaken?

Final question. Will there be audits or reviews of the initiative? If so, detail these. This is useful as a record of the assurance activity MBIE undertakes.



How would you describe the impact to the people whose information you are using?



How will you know your initiative is working as expected?