



27 January 2023

Reference 2223-1107

M Jones

fyi-request-21212-87a75647@requests.fyi.org.nz

Tēnā koe

Thank you for writing to the Ministry of Business, Innovation and Employment (MBIE) on 24 November 2022, to request the following, under the Official Information Act 1982 (the OIA):

a copy of MBIE's full feedback to the Government Chief Privacy Officer (GCPO) on their draft Privacy Maturity Assessment Framework.

On 6 December 2022, you clarified your request to be for the following:

MBIE's 2020-21 Privacy maturity self-assessment, as submitted to the Government Chief Privacy Officer, as part of the PMAF beta test in June, but also any supplementary feedback on the beta version of the PMAF itself, including any commentary on the addition of considerations from the DPUP, and any concerns or comments about the new structure and content of the new PMAF.

MBIE recognises the need to be a responsible and trustworthy kaitiaki (guardian) of the personal information we collect and use to support the delivery of our services and functions. We acknowledge the importance of engendering trust from the public through our privacy practices, and inclusion of Te Ao Māori worldviews in privacy and data governance.

One way we measure our effectiveness in this regard is through the Privacy Maturity Assessment Framework (PMAF), which was developed by the Government's Chief Privacy Officer (GCPO), to give agencies a way to assess both their privacy capacity and maturity.

This is done through a self-assessment across five core expectations:

- Taking a people-centred approach
- Building and maintaining a privacy culture
- Building and maintaining privacy capability
- Establishing a sense of collective responsibility; and
- Being a capable treaty partner.

More information about the PMAF can be found on the GCPO's website, at the following address:

<https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/privacy-maturity-assessment-framework-pmaf-and-self-assessments/>.

MBIE submits the PMAF self-assessment annually. The 2022 self-assessment showed MBIE as an organisation is at a 'managed' privacy maturity, indicating that the efforts and resources we have committed to our privacy programme have succeeded in laying a foundation on which we can continue to build maturity.



Documents relating to the first ('beta') PMAF assessment are attached, as follows:

- The email from MBIE's Chief Legal Advisor Ann Brennan to the GCPO, sent on 28 June 2021, with MBIE's feedback on the draft PMAF, as **Document 1**
- *MBIE 2020-21 Privacy Maturity Self-assessment Framework Beta Test Report to the Government Chief Privacy Officer*, an internal memo coversheet signed by MBIE's Chief Executive on 23 June 2021, approving the submission of MBIE's self-assessment to the GCPO, as **Document 2**
- *Privacy Maturity Assessment Framework Tool (Beta)*, guidance from the GCPO to agencies about the new PMAF as **Document 3**.
- MBIE's submission to the GCPO, as **Document 4**.
- **Appendix II** to the PMAF Beta Test document, which contains the text also in MBIE's submission to the GCPO, for additional readability (due to constraints in the initial PMAF template), as **Document 5**.

I have withheld one mobile number from **Document 1** under section 9(2)(a) of the OIA, to protect the privacy of natural persons.

Thank you again for writing to MBIE. Under section 28(3) of the OIA, you have the right to refer our response to an Ombudsman for review.

Nāku noa, nā



Ann Brennan
MBIE Chief Legal Advisor & Chief Privacy Officer
Legal, Ethics and Privacy
Ngā Pou o te Taumaru

1

From: Tina Chiles on behalf of Ann Brennan
Sent: Monday, 28 June 2021 8:47 am
To: gcpo@dia.govt.nz
Subject: PMAF Beta test - feedback from MBIE
Attachments: MBIE CE approval for 2020-21 PMAF beta test to GCPO June 2021.pdf; MBIE 2021 PMAF Tool - Beta Final June 2021.xlsx

Kia ora Russell

Thank you for the opportunity to participate in the beta testing of the new PMAF framework.

Please find attached MBIE's feedback.

The first attachment covers the approval from our Chief Executive Carolyn Tremain. The second attachment is the completed PMAF tool, as requested in EXCEL format.

For completeness, we include in this e-mail our feedback on the framework, the tool format and the process, which we will cover off in more detail in the upcoming workshops and relationship meetings with your office.

Test Results – Framework

- The new draft Privacy Maturity Assessment Framework (PMAF) is intended to provide a more 'narrative-based picture of an agency's privacy maturity', and steps away from the previous framework's score-based approach. This is not really in line with other maturity self-assessment approaches e.g. PSR or gERMAF. We think this will make it difficult for the GCPO to provide system-wide insights or any form of benchmarking information to agencies e.g. how do we compare to agencies who are of a similar size and complexity as MBIE.
- The new PMAF has been influenced by considerations contained in the Data Protection and Use Policy. The requirements of the DPUP are relevant to social services, but are not always compatible with the requirements of an agency with regulatory, investigative or enforcement functions. By referencing the DPUP, does this adequately accommodate ALL types of agencies under the GCPO's mandate? What do agencies do if the DPUP is not applicable or relevant when assessing their maturity?
- The 'intended focus' of the PMAF doesn't reference what the specific benefits are to an individual agency from completing the PMAF outside of helping an agency better meet their legal obligations under the Privacy Act 2020. There is no mention of how the tool can help agencies to identify and prioritise resources to lift privacy capability.
- Criteria wording is highly open to interpretation, and MBIE is unclear how the narrative data supporting each agency's self-assessment will be collated, ranked and reported to Ministers. We suggest mentioning that other maturity assessment frameworks (e.g. PSR) provide examples of 'indicators' of maturity for each element (noting 'it may include, but are not limited to') so that each agency can choose the level which best represents their organisation. This might be helpful to provide further clarity so that the criteria are not open to interpretation so much.
- There are instances of conflation of privacy considerations and those of ethics and data management, as noted in the feedback contained in the tool itself.
- Operationalisation of the tool has been difficult, particularly to the interpretive nature of some of the criteria wording, and perhaps a glossary would be helpful. An example is the criteria around engagement with Māori, where "Māori privacy interests" are not defined, and are therefore difficult to assess and justify. In addition, it is MBIE's understanding that the new PMAF has not been created in consultation with Māori in any specific way other than aligning with the DPUP, the development of which did include consultation with relevant groups to provide appropriate wording and criteria.
- In an agency of the size and functional diversity as MBIE, it is difficult to apply each criteria to the organisation as a whole. There are some areas of MBIE that hold a higher or lower level of privacy

maturity. This is largely commensurate with the level of sensitivity of the personal information each part of MBIE manages.

- We have noted in CE1.2 that due to MBIE's regulatory function, some criteria may not always be applicable to us. It is noted that we were therefore required to make a decision to consider that we achieved a 'managed' status in this area, regardless of not fulfilling all of the criteria due to those criteria not being applicable. It would be preferable to have a clear indication in the framework that if certain criteria are not applicable to an agency, they do not necessarily lead to a lower rating.
- We suggest adding a reference to the Te Kawa Mataaho Public Service Commission Code of Conduct to the Core Expectation criteria CE4.
- There is no measure of whether an organisation has carried out a stocktake of the personal information it holds. This can be a costly, but essential undertaking, and inclusion of this in the previous PMAF has helped incentivise this activity, and
- The purpose and intended outcomes of the use of the weighting function of the new PMAF tool are unclear.

Test Results – Tool Format and Process

- It has been difficult to provide responses to each criteria as there is only space to give narrative responses to overall elements
- There appears to be a bug in the spreadsheet that means even if each criteria is completed this does not show in the overall results summary
- The tool is difficult to enter large blocks of text into, partly because of the design and the fact that it is a protected workbook. It would have been useful to make minor changes, for example alter the font colour to be more readable, or use the find function or carry out a spell-check, but these features are unavailable as the Excel spreadsheet is locked
- The tool does not provide output that can be printed for consultation and sign offs
- Spell check missing
- Font and colour are near impossible to read, and
- Format is not laptop friendly (requires large screen).

Ngā mihi

Ann

Ann Brennan (*she/her/Ms*)

Chief Legal Advisor & Chief Privacy Officer, MBIE

GM Legal, Ethics and Privacy Branch

Corporate, Governance and Information

Ministry of Business, Innovation & Employment

DDI: +64 4 901 2081 | Mob: [011 9201 1111](tel:01192011111) | www.mbie.govt.nz

Level 10, 25 The Terrace – Pastoral House, Wellington 6011 | Postal Address Level 4, 25 The Terrace, 6011





DATE	21 June 2021
TO	Carolyn Tremain, Chief Executive
PREPARED BY	Ann Brennan, Chief Privacy Officer and Chief Legal Advisor
APPROVED BY	Richard Griffiths, Deputy Chief Executive, Corporate, Governance and Information
SUBJECT	MBIE 2020-21 Privacy Maturity Self-assessment Framework Beta Test Report to the Government Chief Privacy Officer

Purpose

1. This cover sheet seeks your approval to submit the Ministry's 2020-21 Privacy Maturity Self-Assessment Framework (PMAF) beta test to the Government Chief Privacy Officer (GCPO) by 30 June 2021.

Recommendations

2. It is recommended that you:

Note the Organisational Capability and Assurance Committee (OrCA) endorsed the Draft 2020-21 PMAF Beta Test Report on 9 June 2021. The draft Minutes Extract is attached as Appendix I in the 2019-20 PMAF Cover Memo to you (which is also attached).

Yes / No

Note the attached 2020-21 PMAF Chief Executive Cover Memo.


Yes / No

Approve the attached final 2020-21 PMAF Beta Test Report for submission to the GCPO by signing this memo.

Yes / No

Direct MBIE's Chief Privacy Officer to submit the approved 2020-21 PMAF Beta Test Report to the GCPO by 30 June 2021.

Yes / No



Carolyn Tremain

Chief Executive

23 /06/2021

RELEASED UNDER THE OFFICIAL INFORMATION ACT

3 Privacy Maturity Assessment Framework Tool (Beta)

Introduction

This tool is for agencies to complete this year's privacy self-assessment for the Government Chief Privacy Officer (GCPO). This year's self-assessment is part of the beta testing of the new PMAF. Results will not form the agency baseline.

The completed self-assessment as an **Excel attachment** (not a PDF scan) must be emailed to gcpo@dia.govt.nz by the agency's Chief Executive. The email must include confirmation that the Chief Executive has reviewed the self-assessment.

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

Instructions

Each section of the PMAF has its own tab which will calculate the overall maturity level for that section. The Summary tab will display the overall maturity level for each section/tab, as well as the maturity level for each criteria and element. There will be no one overall maturity level given.

There are three steps to completing the self-assessment:

1. Select the appropriate maturity level for each criteria using the drop-down box under Criteria Level. When the maturity level is selected, the description for that level will be displayed.
2. Provide the narrative to support the resulting maturity level for each element.
3. Adjust the element weighting (optional). Each element has a default weighting of 10 which can be

Feedback

This spreadsheet is a work in progress. There remains additional testing and accessibility adjustments to be made. Please let us know if there are any glitches or issues with the functionality not working properly.

Please let us know how this tool is working for you and any recommendations for improvement. Any substantive recommendations will be incorporated after the 30 June 2021 self-assessment submissions.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

4

Core Expectations						
Element	Weighting	Criteria	Criteria Description	Criteria Level	Level Description	Overall Level
CE1	10	Take a people-centred approach to privacy that is respectful of those the information is about and provides the public with effective services.				Managed
		CE1.1	Having a people-centred privacy programme	Managed	The Data Protection and Use Policy's principles are appropriately integrated with privacy policies and practices, and the privacy programme focuses on change initiatives to embed a people-centred approach.	
		CE1.2	Connecting with service users	Managed	There are established processes and easy-to-use methods, when appropriate, for connecting with service users or their representatives to include their views in decision-making processes about collection and use of their personal information.	
		CE1.3	Being transparent	Managed	The agency is transparent about what kinds of personal information it collects and uses, why and how it is used, choices people may have and how to access and request correction to their personal information. This information is presented in easy-to-understand ways.	
		<p>CE1.1 Given MBIE's wide and diverse functions, many of which are regulatory, it is not always appropriate to integrate the Data Protection and Use Policy's principles into all our practices relating to the handling of personal information. Instead, MBIE has a specific collective focus of being people-centred in our organisational strategy (Te Ara Amorangi). In addition, we have ensured our organisational values are built into our overall Privacy Policy, specifically, "Hikina Whakatutuki: Grow New Zealand for All: Ensuring appropriate care, respect, and controls are considered when handling the personal information in our care is key to MBIE's overall objective to Grow New Zealand for All: Pae Kahurangi: We protect what's precious, our taonga. Respectful handling of the personal information in our care is key to demonstrating MBIE's value of retaining and building trust and confidence to enable us to build our future. Maia: We explore new ideas. Assessing risks to individual privacy when developing or adopting new processes, systems and technologies will</p>				
CE2	10	Build and maintain a privacy culture that embodies the public service values of being impartial, accountable, trustworthy, respectful, and responsive.				Managed
		CE2.1	Creating a privacy culture	Managed	Leadership delivers consistent and positive messages about how privacy is everyone's responsibility and how privacy is an enabler of public trust and quality service delivery. Privacy culture is periodically assessed, possibly as part of a broader organisational culture survey.	
		CE2.2	Communicating privacy values and aspirations	Managed	Senior leadership and privacy leaders communicate the agency's clearly defined privacy values and aspirations in relevant terms throughout the agency on a schedule that is proportionate to their agency's needs.	
		CE2.3	Developing privacy awareness	Managed	Privacy awareness clearly communicates the agency's values, expectations and behaviours to staff and contractors, and promotes the use of Privacy by Design.	
<p>CE2.1 Privacy culture is surveyed on an annual basis, and results are shared and discussed with leadership. Leadership delivers positive messaging around privacy responsibilities, including a webinar with the Privacy Commissioner hosted by our CE which was attended by well over 1000 of our staff.</p> <p>CE2.2 The Privacy Programme is governed and supported by senior leadership via the Organisational Capability and Assurance Committee, and delivers a schedule of privacy training activities, including both general MBIE-wide training, and bespoke engagement tailored and targeted for specific areas and functions within the organisation.</p> <p>CE2.3 MBIE's privacy messaging and training clearly communicates how privacy relates to our organisational values and behaviours. All new or significantly updated tools, systems or processes are required to undergo a Privacy Assessment to help identify potential privacy risks and</p>						
CE3	10	Build and maintain privacy capability so that people have the knowledge and skills they need to contribute to good privacy practice.				Managed
		CE3.1	Conducting privacy training	Managed	At their induction, and then on a regular basis, staff and contractors receive privacy training on the agency's privacy values, policies, practices and risks that is relevant to their roles and supports them to be effective and trusted custodians of personal information.	
		CE3.2	Monitoring and updating privacy training	Managed	Privacy training needs are monitored and training content is reassessed to ensure that it remains fit for purpose.	
		CE3.3	Providing additional privacy training	Managed	Staff and contractors know how to access appropriate advice that they should understand before they are given access to certain classes of personal information (for example, health information) that may fall under a Privacy Code and/or may require additional privacy knowledge to manage properly.	
<p>CE3.1 All MBIE people receive mandatory privacy training as part of their induction pathway, and the Privacy Team carries out a range of both general and targeted training and engagement as part of our annual work plan.</p> <p>CE3.2 Targeted and general privacy training needs are informed by MBIE's Privacy Team's privacy event management process, which notes trends in breach root causes and delivers reminders, general messaging and bespoke training as appropriate. Training needs are also based on relevant and topical developments, such as updated legislation and/or guidance from the OPC or GCPO, or privacy considerations related to the need for staff to work from home. Static privacy training (such as e-learning modules and guidance material on our intranet) is monitored for accuracy and updated as required.</p> <p>CE3.3 While there is no organisation-wide mechanism to restrict access to certain classes of personal information until staff and contractors have completed training specific to that classification, all staff and contractors must complete mandatory information security training before</p>						

CE4	10	Establish a sense of collective accountability in which managers and staff understand their duty to ensure that personal information is collected and used appropriately.			Managed	
		CE4.1	Implementing privacy practices	Managed		Functional areas that collect or make use of people's personal information (for example, procurement, service design, contracting and funding, analysis and research, etc) include recognised good practice advice (for example, DPUP) in their core processes.
		CE4.2	Linking privacy to organisational values	Managed		Organisational value frameworks, such as mission statements, draw a direct line between delivering quality service and exercising a collective focus on respectful and transparent practices in the use of personal information.
		CE4.3	Including privacy in employment	Managed		Letters of employment and job descriptions reference privacy obligations and responsibilities to develop and retain public trust in the collection and use of personal information.
<p>CE4.1: MBIE recognises that some of the most sensitive personal information it collects, stores and uses belongs to its staff. For this reason, MBIE's Privacy Policy specifically applies not only to specific functional areas but to "all staff, secondees and contractors, employed or engaged on any basis by the Ministry of Business, Innovation & Employment (the Ministry), whether they are casual, temporary or permanent, whether full time or part time and whether they are located in New Zealand or in any other country." MBIE's Privacy Policy informs operational privacy processes and practice.</p> <p>CE4.2: As per CE1.1, MBIE draws a direct line between privacy and our organisational values and behaviours. In addition, one of our organisational strategy's capability priorities is to be empowered by data, with a collective focus of being people centred, to achieve our desired outcome of ensuring participation is inclusive and fair.</p> <p>CE4.3: <i>Māori</i> - <i>Something like</i>. While MBIE position descriptions do not specifically refer to Privacy, they specifically refer to</p>						
CE5	10	Be a capable Treaty partner by supporting the Crown to fulfil its stewardship responsibility and strengthen Crown's relationships with Māori.			Basic	
		CE5.1	Identifying Māori privacy interests	Basic		When designing or updating a service or process that involves the collection, use or sharing of personal information, individual initiatives develop their own practices to identify Māori interests.
		CE5.2	Partnering with Māori	Managed		When Māori privacy interests have been identified a partnership approach is used and provides for personal information to be interpreted with reference to Māori priorities, values and worldviews.
<p>It is unclear from these criteria what Māori privacy interests are referred to specifically, so we have found it difficult to answer this section in general.</p> <p>CE5.1: When designing or updating a service or process, Māori privacy interests are identified on a case-by-case basis depending on the function of the area of MBIE carrying out the work in question.</p> <p>CE5.2: Partnering with Māori is spelled out as one of the focuses of our organisational strategy, and work on strengthening our maturity in this MBIE has a dedicated unit - Te Kūpunga, which is our Māori Economic Development Unit, and which sits within the Strategic Policy & Programmes group of MBIE. The Privacy Team has engaged with Te Kūpunga as appropriate on a case-by-case basis.</p>						
				Core Expectations Level	Managed	

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Leadership						
Element	Weighting	Criteria	Criteria Description	Criteria Level	Level Description	Overall Level
L1	10	Effective oversight for privacy practice through effective governance.				Managed
		L1.1	Privacy reporting	Managed	The privacy officer has regular updates and discussions with senior leadership/executive team, governance board and/or committees on the agency's privacy culture and values, privacy strategy and programme, and privacy issues and risks.	
		L1.2	Privacy and risk management	Managed	Functional oversight for privacy and its work programme is integrated into the risk management organisational structure and includes monitoring compliance.	
		L1.1: MBIÉ's Chief Privacy Officer function sits at Tier 3, is part of our senior leadership (tier 2 and 3) Organisational Capability and Assurance Committee, which receives a quarterly Privacy Report as well as any privacy related decision papers. In addition, a monthly privacy report is sent to a wide range of tier 2, 3 and 4 managers across the organisation. L1.2: Privacy risk management is fully integrated into MBIÉ's overall risk management framework. Quarterly compliance reports are submitted quarterly. In addition, the Privacy Team regularly engages with MBIÉ's organisational Risk function to align privacy risks with enterprise risk considerations and activities.				
L2	10	Delivery of objectives through management structure, roles and responsibilities, and the capacity to achieve these objectives.				Managed
		L2.1	Responsibility and accountability	Managed	Formal line management and governance includes responsibility and accountability for implementation of the privacy strategy and work programme. These responsibilities are suitably distributed throughout the agency to ensure their implementation and include the application of Privacy by Design principles.	
		L2.2	Resourcing	Managed	Resourcing for privacy staff and activities is considered at a strategic level within the agency and is commensurate with the agency's privacy profile and privacy work programme.	
		L2.3	Oversight and visibility	Managed	Privacy officer/team oversees the privacy work programme, maintains central oversight of privacy initiatives and activities on an agency-wide basis, communicates regularly with other related functions (for example, information management, security, risk management) and has clear alignment (where applicable) with their work programmes.	
L2.1: MBIÉ's privacy roles and responsibilities for frontline management staff are clearly set out in our Privacy Policy. L2.2: MBIÉ's Privacy Team is centrally resourced and resourcing needs are monitored and updated as required. L2.3: MBIÉ's Privacy Team has an annual programme or work that receives oversight and approval at a senior level. The Privacy Team proactively identifies and engages with relevant internal stakeholders who carry out related functions, such as our Integrity, Risk, and Information Security teams, on a regular basis.						
L3	10	Confidence in organisational progress through appropriate monitoring and assurance practices.				Managed
		L3.1	Privacy and assurance	Managed	The agency adopts and implements the first of the three lines of defence: First line: Business processes are designed to mitigate residual privacy risk to within the agency's risk tolerance. Second line: Privacy and risk activities are integrated with the wider system of internal controls as part of the agency's assurance framework. Third line: Internal audits or other equivalent independent assurance practices evaluate and improve the agency's privacy risk management, control and governance processes.	
					MBIÉ carries out dedicated activities in line with the "three lines of defence" risk management framework, and our Privacy and Risk teams actively work together to align privacy risks with other enterprise risk factors. We have recently closed a Privacy Programme workstream dedicated to building privacy risk into enterprise risk, and we have created a library of privacy controls individual MBIÉ branches can select from to inform their overall risk profile, which will allow them to mitigate these risks according to their individual business needs.	
Leadership Level					Managed	

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Planning, Policies and Practice						
Element	Weighting	Criteria	Criteria Description	Criteria Level	Level Description	Overall Level
PPP1	10	Strategy and planning: formulate a privacy approach, a strategy for achieving it, and a roadmap to bring it to life.				Managed
		PPP1.1	Planning	Managed	Privacy planning includes all areas of the agency, comprehensively addresses the collection, use, storage and security of personal information, and is flexible to accommodate changes in the wider business environment or the result of assurance activity.	
		PPP1.2	Planning documents	Managed	Privacy planning documents (for example, strategy, roadmap and work programme) are easy to understand, communicated to those with relevant responsibilities, and reviewed regularly to ensure that they remain relevant and aligned with the agency's organisational and system context (nature, scale and risk).	
		PPP1.3	Reporting	Managed	Progress towards privacy strategy, roadmap and work programme is tracked and reported regularly to senior leadership and relevant governance bodies.	
<p>PPP1.1 MBIE's Privacy Programme comprehensively addresses the full personal information lifecycle, and assesses privacy risk across the various functions to ensure privacy is included in planning across the agency. We have a comprehensive Privacy Threshold and Privacy Impact Assessment process that allows MIBE to build privacy by design into new projects.</p> <p>PPP1.2 MBIE has a dedicated Privacy Programme with extensive Programme planning and reporting documentation. This planning and documentation is in line with our organisational strategy and associated policies.</p> <p>PPP1.3 The Privacy Programme reports regularly to all relevant internal stakeholders, including senior leadership and privacy and assurance governance groups. This includes reporting of staff and contractor completion of mandatory privacy training, monthly and quarterly breakdowns of reported privacy breaches, near misses and complaints, and progress of the annual Privacy Work Programme.</p>						
PPP2	10	Competent practice: have policies to equip managers and staff to play their part in achieving the core expectations.				Managed
		PPP2.1	Policies	Managed	Privacy policies are easy to understand, are communicated and accessible throughout the agency, and reviewed regularly to ensure that they remain relevant and aligned with the agency's needs - accounting for nature, scale and risk.	
		PPP2.2	Contracts	Managed	The agency's procurement contracts include standard terms and conditions relating to privacy, and privacy policies include advice on personal information and external suppliers.	
<p>PPP2.1 MBIE's Privacy Policy was last updated in 2020, is clearly communicated and easy to find. It is updated at minimum every three years and is reviewed annually to ensure any factors such as new legislation are included. It is translated into training modules, guidance on our intranet and through our targeted and general privacy guidance, training and communications, to actively disseminate the Policy as widely as possible.</p> <p>PPP2.2 MBIE has specifically focused on the new Privacy Act's requirements around off-shoring personal information as an opportunity to ensure our contracts with third parties include standard terms and conditions around the appropriate collection, use, storage, sharing and disposal of personally identifiable information.</p>						
Planning, Policies and Practice Level						Managed

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Privacy Domains						
Element	Weighting	Criteria	Criteria Description	Criteria Level	Level Description	Overall Level
PD1	10	Require a clear understanding of the purpose and necessity of collection, use and sharing of personal information.				Managed
		PD1.1	Defining the purpose	Managed	The agency has appropriately integrated the Data Protection and Use Policy's 'Purpose Matters' guideline to accurately define purposes for collection, use, or sharing of personal information for projects and business processes.	
		PD1.2	Identifying choices	Managed	When purposes have been suitably well-defined, additional processes are explicitly applied to identify when and how choices may be offered or accommodated, in line with both the Data Protection and Use Policy's 'Purpose Matters' and 'Transparency and Choice' guidelines.	
		PD1.3	Reducing personal information	Managed	When creating or updating a service or process, consideration is given to eliminating or reducing the need for personal information by ensuring that its collection, use and sharing are needed to accomplish the stated outcomes. Existing practice is not used as a justification for continued collection and use.	
<p>The requirement to specifically incorporate the DPUP here is again limiting to MBE's response to the beta test of the self-assessment. MBE clearly defines the purpose for collection, use and sharing of personally identifiable information in its Privacy Policy, and assurance is achieved by the Privacy Threshold and Impact Assessment process that is clearly defined and promoted throughout the agency. The assessment process always includes considerations around data minimisation, transparency, and opt-in wherever possible or practicable, rather than opt-out, for data subjects.</p>						
PD2	10	Ensure the use and storage of personal information protects against inappropriate access, use, and modification, whilst also ensuring effective and efficient support for its intended use.				Managed
		PD2.1	Implementing Privacy by Design	Managed	Privacy, ICT, information management and other responsible teams work together to incorporate Privacy by Design methodology and principles when building and updating processes, products and services.	
		PD2.2	Implementing privacy engineering	Managed	When building and updating processes, products and services, privacy and ICT staff work together to incorporate the privacy engineering objectives of predictability, manageability and dissociability by using privacy design strategies (for example, minimise, hide, separate, aggregate, inform, control, enforce and demonstrate).	
<p>The Privacy Team actively engages with MBE's data security function on a regular basis to ensure there is agreement and alignment between requirements around the collection, storage, use, disclosure and disposal of personally identifiable information. This is principally achieved through the privacy assessment process, as well as regular scheduled meetings to discuss privacy engineering considerations and the intersection between the two functions.</p>						
PD3	10	Make it easy for people to access and request correction to their information.				Basic
		PD3.1	Having a process	Managed	Customers and clients can easily find and understand the process to make an access request.	
		PD3.2	Monitoring the process	Basic	The agency has an access request process. The requesters and the agency have little visibility of whether the access requests responses are meeting the legislative requirements.	
		PD3.3	Reviewing the process	Managed	Information management and ICT system reviews explicitly include consideration of easy access and collation of personal information to enable timely responses to access requests.	
<p>PD3.1 Each MBE function clearly communicates how to request access and correction of their information via their dedicated website privacy statement PD3.2 Given the size and diversity of MBE's various functions, there is no centralised approach to requests for access or corrections of personal information. Instead, requests of this kind are handled on an operational level by the team or business function handling the substantive engagement with the requestor. This approach is reassessed on a regular basis, and we instead have a function-by-function approach that ensures there is visibility of these requests in specific areas, such as Immigration New Zealand (INZ), where there is a dedicated team that monitors, responds to, and reports on these requests according to the INZ function PD3.3 This decentralised approach is regularly reassessed to ensure it is still appropriate in terms of volume and location of requests, and</p>						
PD4	10	Understand and assess privacy risks and manage commensurately.				Managed
		PD4.1	Knowing the agency's risks	Managed	Privacy risks are assessed based on an understanding and knowledge of personal information holdings, focusing on collection, uses, sharing activities, and storage.	

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Privacy Domains						
Element	Weighting	Criteria	Criteria Description	Criteria Level	Level Description	Overall Level
		PD4.2	Managing agency's risks	Managed	Agency privacy risk assessments, which provide a snapshot of an agency's current privacy risks and how it will manage them as an organisation, are part of the agency's overall risk assessment, and are conducted and reviewed periodically.	
		PD4.3	Managing project risks	Managed	Project risk assessments are done to assess the privacy risk of new or updated processes, products or services with the support of and oversight by the privacy team. They cover the whole information life cycle and have clear lines of ownership and accountability.	
<p>PD4.1: Privacy risks are actively monitored and assessed by the Privacy Team based on analysis of reported privacy events, our privacy assessment process, and the embedding programme's proactive activities</p> <p>PD4.2: MBIE's privacy risk assessments are carried out as a matter of course, as stipulated in the requirements of our Privacy Policy. Other privacy-related risk assessment and assurance has been mentioned in previous responses</p> <p>PD4.3: Privacy assessments are carried out in line with MBIE's Privacy Policy, stepping through the full information lifecycle from collection to disposal, and each are triaged by the Privacy Team, with clear expectations of project signoff</p>						
PD5	10	Reduce the impact of privacy breaches and incidents through good privacy practices.				Managed
		PD5.1	Having a privacy incident register	Managed	The agency has a privacy incident register that is used by staff and/or privacy team, a tested privacy incident response plan (including partners and third parties) that is integrated into its business continuity planning, and a process for learning from privacy incidents and breaches.	
		PD5.2	Minimising the collection of personal information	Managed	The agency collects only personal information that is clearly linked to the desired outcome and investigates alternative ways to accomplish the desired outcome that eliminates or reduces the need for personal information.	
		PD5.3	Retaining personal information	Managed	The agency has, maintains and promotes information policy and practices that include the retention and destruction of personal information and the destruction of personal information is authorised by the Government Chief Archivist.	
<p>PD5.1: MBIE has a comprehensive and well-promoted privacy event register that captures all privacy complaints, breaches and near-misses. Information on how to identify and report privacy events is well documented and circulated, and is included in all relevant privacy training and engagement throughout the organisation. The Privacy Team triages and proactively supplies guidance and support to appropriately contain, manage and escalate all privacy events. Information about root causes of privacy events is collated, reported, and used to inform messaging and engagement to ensure trends are identified and lessons learned from privacy events can be incorporated into future privacy-related processes and procedures.</p> <p>PD5.2: MBIE's Privacy Threshold and Privacy Impact Assessment process clearly defines purpose of collection of personal information, and this is a requirement of all new or significantly updated projects that involve the collection of personally identifiable information.</p>						
PD6	10	Enable personal information use, reuse and sharing to support a unified public service that provides the public with effective services.				Managed
		PD6.1	Having policies	Managed	Information management and privacy policies include enabling advice on how to appropriately use and share personal information when individuals can be identified. These policies also refer to relevant external sources (for example, information to support tamariki wellbeing, information sharing under Family Violence Act 2018).	
		PD6.2	Understanding communities interest	Managed	Privacy policies and other relevant policies incorporate advice for the appropriate reuse and sharing of non-personal information of interest to communities that doesn't identify individuals (for example, data and data sets, analysis, qualitative or quantitative information, statistics, research, reports or studies) from:	
<p>PD6.1: MBIE has a comprehensive Privacy Policy, and a suite of information sharing agreements that support the appropriate use and disclosure of personal information, incorporating the considerations of a number of related pieces of legislation that interact with our responsibilities and functional requirements.</p> <p>PD6.2: All collection and use of personally identifiable information falls under MBIE's overarching Privacy Policy. If that information is then published or shared in an aggregated or non-identifiable way, this will inform the overall risk profile of each individual project. Our privacy assessment process takes into account the non-identifiable use or disclosure of personal information, queries the possibility of re-identification, and is designed to ensure the protection of personal information used in this way.</p>						
Privacy Domains Level						Managed

Section	Criteria	Criteria Description	Criteria Level	Overall Level
Core Expectations	CE1.1	Having a people-centred privacy programme	Managed	Managed
	CE1.2	Connecting with service users	Managed	
	CE1.3	Being transparent	Managed	
	CE2.1	Creating a privacy culture	Managed	Managed
	CE2.2	Communicating privacy values and aspirations	Managed	
	CE2.3	Developing privacy awareness	Managed	
	CE3.1	Conducting privacy training	Managed	Managed
	CE3.2	Monitoring and updating privacy training	Managed	
	CE3.3	Providing additional privacy training	Managed	
	CE4.1	Implementing privacy practices	Managed	Managed
	CE4.2	Linking privacy to organisational values	Managed	
	CE4.3	Including privacy in employment	Managed	
	CE5.1	Identifying Māori privacy interests	Basic	Basic
	CE5.2	Partnering with Māori	Managed	
	Leadership	L1.1	Privacy reporting	Managed
L1.2		Privacy and risk management	Managed	
L2.1		Responsibility and accountability	Managed	Managed
L2.2		Resourcing	Managed	
L2.3		Oversight and visibility	Managed	
L3.1		Privacy and assurance	Managed	Managed
Planning, Policies &		PPP1.1	Planning	Managed
	PPP1.2	Planning documents	Managed	
	PPP1.3	Reporting	Managed	
	PPP2.1	Policies	Managed	Managed
	PPP2.2	Contracts	Managed	
Privacy Domains	PD1.1	Defining the purpose	Managed	Managed
	PD1.2	Identifying choices	Managed	
	PD1.3	Reducing personal information	Managed	
	PD2.1	Implementing Privacy by Design	Managed	Managed

Section	Criteria	Criteria Description	Criteria Level	Overall Level
	PD2.2	Implementing privacy engineering	Managed	
	PD3.1	Having a process	Managed	Basic
	PD3.2	Monitoring the process	Basic	
	PD3.3	Reviewing the process	Managed	
	PD4.1	Knowing the agency's risks	Managed	Managed
	PD4.2	Managing agency's risks	Managed	
	PD4.3	Managing project risks	Managed	
	PD5.1	Having a privacy incident register	Managed	Managed
	PD5.2	Minimising the collection of personal information	Managed	
	PD5.3	Retaining personal information	Managed	
	PD6.1	Having policies	Managed	Managed
	PD6.2	Understanding communities interest	Managed	

RELEASED UNDER THE OFFICIAL INFORMATION ACT

2020-21 PMAF BETA TEST - MBIE Responses

(As Word document, due to the EXCEL format sizing limitations in the PMAF tool)

Core Expectations

ID	MBIE Response
CE1	<p>CE1.1: Given MBIE's wide and diverse functions, many of which are regulatory, it is not always appropriate to integrate the Data Protection and Use Policy's principles into all our practices relating to the handling of personal information. Instead, MBIE has a specific collective focus of being people-centred in our organisational strategy (Te Ara Amiorangi). In addition, we have ensured our organisational values are built into our overall Privacy Policy, specifically, "Hikina Whakatutuki: Grow New Zealand for All: Ensuring appropriate care, respect, and controls are considered when handling the personal information in our care is key to MBIE's overall objective to Grow New Zealand for All. Pae Kahurangi: We protect what's precious, our taonga: Respectful handling of the personal information in our care is key to demonstrating MBIE's value of retaining and building trust and confidence to enable us to build our future.</p> <p>Māia: We explore new ideas: Assessing risks to individual privacy when developing or adopting new processes, systems and technologies will ensure our new initiatives are respectful of people's rights, comply with relevant legislation, and have the right protections in place to minimise the risk of something going wrong." Embedding our values and associated behaviours in our overarching Privacy Policy emphasises the importance of people as not only data subjects but as owners of valuable information that must be handled with respect. This people-centred focus informs MBIE's privacy-related training and processes. In addition, MBIE's Privacy Programme includes a specific programme of work that targets parts of the organisation that handles particularly sensitive personal information, and works closely with them to raise their privacy maturity (the Embedding Privacy Programme). This programme takes a specifically people-centric approach, focusing on driving behavioural change to ensure the information in these areas is handled with care and respect.</p> <p>CE1.2: As above, many of MBIE's functions are regulatory, and in some cases collection and use of personal information is required by law. This criteria will not always be applicable to agencies such as MBIE that carry out regulatory, investigative or enforcement activities.</p> <p>CE1.3: MBIE has clear collection/privacy statements that are easily accessible via our websites, as per the requirements of Information Privacy Principle 3 of the Privacy Act 2020.</p>
CE2	<p>CE2.1: Privacy culture is surveyed on an annual basis, and results are shared and discussed with leadership. Leadership delivers positive messaging around privacy responsibilities, including a webinar with the Privacy Commissioner hosted by our CE which was attended by well over 1000 of our staff.</p> <p>CE2.2: The Privacy Programme is governed and supported by senior leadership via the Organisational Capability and Assurance Committee, and delivers a schedule of privacy training activities, including both general MBIE-wide training, and bespoke engagement tailored and targeted for specific areas and functions within the organisation.</p> <p>CE2.3: MBIE's privacy messaging and training clearly communicates how privacy relates to our organisational values and behaviours. All new or significantly updated tools, systems or processes are required to undergo a Privacy Assessment to help identify potential privacy risks and mitigations so that these can be built in from the ground up in line with the principles of Privacy by Design.</p>
CE3	<p>CE3.1: All MBIE people receive mandatory privacy training as part of their induction pathway, and the Privacy Team carries out a range of both general and targeted training and engagement as part</p>

ID	MBIE Response
	<p>of our annual work plan.</p> <p>CE3.2: Targeted and general privacy training needs are informed by MBIE's Privacy Team's privacy event management process, which notes trends in breach root causes and delivers reminders, general messaging and bespoke training as appropriate. Training needs are also based on relevant and topical developments, such as updated legislation and/or guidance from the OPC or GCPO, or privacy considerations related to the need for staff to work from home. Static privacy training (such as e-learning modules and guidance material on our intranet) is monitored for accuracy and updated as required. Further, the library for performance and development plans contains performance objectives manager/staff can select for positions/staff with specific privacy training needs.</p> <p>CE3.3: While there is no organisation-wide mechanism to restrict access to certain classes of personal information until staff and contractors have completed training specific to that classification, all staff and contractors must complete mandatory information security training before they have permission to access any information held by MBIE. In addition, parts of the organisation that have been identified as routinely handling highly sensitive personal information are the subject of a dedicated programme of work to raise privacy maturity in these areas (the Embedding Privacy Programme).</p>
CE4	<p>CE4.1: MBIE recognises that some of the most sensitive personal information it collects, stores and uses belongs to its staff. For this reason, MBIE's Privacy Policy specifically applies not only to specific functional areas but to "all staff, secondees and contractors, employed or engaged on any basis by the Ministry of Business, Innovation & Employment (the Ministry), whether they are casual, temporary or permanent, whether full time or part time and whether they are located in New Zealand or in any other country." MBIE's Privacy Policy informs operational privacy processes and practice.</p> <p>CE4.2: As per CE1.1, MBIE draws a direct line between privacy and our organisational values and behaviours. In addition, one of our organisational strategy's capability priorities is to be empowered by data, with a collective focus of being people centred, to achieve our desired outcome of ensuring participation is inclusive and fair.</p> <p>CE4.3: While MBIE position descriptions do not specifically refer to Privacy, they specifically refer to Organisational commitment and public service as "Role models the standards of Integrity and Conduct for the Public Services Contributes to the development of, and helps promote and builds commitment to MBIE's vision, mission, values and services, by ... complying with all legislative requirements and good employer obligations. " All new starters sign the MBIE Code of Conduct and the Public Services Commission (PSC) Code of conduct, and the ICT Use Policy before they start their positions (with their letter of offer). Note: the MBIE Code of Conduct will be fully reviewed once the PSC has completed their review of their Code of Conduct which is currently under way.</p>
CE5	<p>It is unclear from these criteria what Maori privacy interests are referred to specifically, so we have found it difficult to answer this section. In general:</p> <p>CE5.1: When designing or updating a service or process, Maori privacy interests are identified on a case-by-case basis depending on the function of the area of MBIE carrying out the work in question.</p> <p>CE5.2: Partnering with Maori is spelled out as one of the focuses of our organisational strategy, and work on strengthening our maturity in this MBIE has a dedicated unit - Te Kupenga, which is our Māori Economic Development Unit, and which sits within the Strategic Policy & Programmes group of MBIE. The Privacy Team has engaged with Te Kupenga as appropriate on a case-by-case basis.</p>

Leadership

ID	MBIE Response
L1	<p>L1.1: MBIE's Chief Privacy Officer function sits at Tier 3. Our senior leadership (tier 2 and 3) Organisational Capability and Assurance Committee receives a quarterly Privacy Report as well as any privacy related decision papers. In addition, a monthly privacy report is send to a wide range of tier 2, 3 and 4 managers across the organisation. An enterprise privacy risk has recently been added to the SLT risk profile.</p> <p>L1.2: Privacy risk management is fully integrated into MBIE's overall risk management framework. Quarterly compliance reporting on the MBIE Privacy Policy is provided to the Enterprise Risk and Compliance branch and relevant business groups. 'Enterprise Risk and Compliance' provide oversight of privacy risks recorded on Business Group and Branch risk register to the Privacy team'. In addition, the Privacy Team regularly engages with MBIE's organisational Risk function to align privacy risks with enterprise risk considerations and activities.</p>
L2	<p>L2.1: MBIE's privacy roles and responsibilities for frontline management staff are clearly set out in our Privacy Policy.</p> <p>L2.2: MBIE's Privacy Team is centrally resourced and resourcing needs are monitored and updated as required. An 18 months programme of work is currently under way that embeds privacy advisors for a period of time within high privacy risk branches. This will enable them to help grow privacy capability and culture.</p> <p>L2.3: MBIE's Privacy Team has an annual programme of work that receives oversight and approval at a senior level. The Privacy Team proactively identifies and engages with relevant internal stakeholders who carry out related functions, such as our Integrity, Risk, and Information Security teams, on a regular basis.</p>
L3	<p>MBIE carries out dedicated activities in line with the "three lines of defence" risk management framework, and our Privacy and Risk teams actively work together to align privacy risks with other enterprise risk factors. We have recently completed work to include privacy risk into enterprise risk management processes, and we have created a library of privacy controls individual MBIE branches can select from to inform their overall risk profile, which will allow them to mitigate these risks according to their individual business needs. The Privacy Programme contains two workstreams dedicated to building capability around assurance, which are ongoing.</p>

Planning, Policies and Practices

ID	MBIE Response
PPP1	<p>PPP1.1: MBIE's Privacy Programme comprehensively addresses the full personal information lifecycle, and assesses privacy risk across the various functions to ensure privacy is included in planning across the agency. We have a comprehensive Privacy Threshold and Privacy Impact Assessment process that allows MBIE to build privacy by design into new projects.</p> <p>PPP1.2: MBIE has a dedicated Privacy Programme with extensive Programme planning and reporting documentation. This planning and documentation is in line with our organisational strategy and associated policies.</p> <p>PPP1.3: The Privacy Programme reports regularly to all relevant internal stakeholders, including senior leadership and privacy and assurance governance groups. This includes reporting of staff and contractor completion of mandatory privacy training, monthly and quarterly breakdowns of reported privacy breaches, near misses and complaints, and progress of the annual Privacy Work Programme.</p>
PPP2	<p>PPP2.1: MBIE's Privacy Policy was last updated in 2020, is clearly communicated and easy to find. It</p>

ID	MBIE Response
	<p>is updated at minimum every three years, and is reviewed annually to ensure any factors such as new legislation are included. It is translated into training modules, guidance on our intranet and through our targeted and general privacy guidance, training and communications, to actively disseminate the Policy as widely as possible.</p> <p>PPP2.2: MBIE has specifically focused on the new Privacy Act's requirements around off-shoring personal information as an opportunity to ensure our contracts with third parties include standard terms and conditions around the appropriate collection, use, storage, sharing and disposal of personally identifiable information.</p>

Privacy Domains

ID	MBIE Response
PD1	<p>The requirement to specifically incorporate the DPUP here is again limiting to MBIE's response to the beta test of the self-assessment. MBIE clearly defines the purpose for collection, use and sharing of personally identifiable information in its Privacy Policy, and assurance is achieved by the Privacy Threshold and Impact Assessment process that is clearly defined and promoted throughout the agency. The assessment process always includes considerations around data minimisation, transparency, and opt-in wherever possible or practicable, rather than opt-out, for data subjects.</p>
PD2	<p>The Privacy Team actively engages with MBIE's data security function on a regular basis to ensure there is agreement and alignment between requirements around the collection, storage, use, disclosure and disposal of personally identifiable information. This is principally achieved through the privacy assessment process, as well as regular scheduled meetings to discuss privacy engineering considerations and the intersection between the two functions.</p>
PD3	<p>PD3.1: Each MBIE function clearly communicates how to request access and correction of their information via their dedicated website privacy statement.</p> <p>PD3.2: Given the size and diversity of MBIE's various functions, there is no centralised approach to requests for access or corrections of personal information. Instead, requests of this kind are handled at an operational level by the team or business function handling the substantive engagement with the requestor. This approach is reassessed on a regular basis, and we have a function-by-function approach that ensures there is visibility of these requests in specific areas, such as Immigration New Zealand (INZ), where there is a dedicated team that monitors, responds to, and reports on these requests according to the INZ function.</p> <p>PD3.3: This decentralised approach is regularly reassessed to ensure it is still appropriate in terms of volume and location of requests, and overall privacy risk and appetite.</p>
PD4	<p>PD4.1: Privacy risks are actively monitored and assessed by the Privacy Team based on analysis of reported privacy events, our privacy assessment process, and the embedding programme's proactive activities. Business groups and branches are required to capture an enterprise privacy risk in their risk registers which is reviewed on a quarterly basis. This provides the Privacy Team and Enterprise Risk and Compliance oversight of the management of privacy risks across MBIE. The Privacy Programme contains two workstreams dedicated to building capability around assurance, which are ongoing.</p> <p>PD4.2: MBIE's privacy risk assessments are carried out as a matter of course, as stipulated in the requirements of our Privacy Policy. Other privacy-related risk assessment and assurance has been mentioned in previous responses.</p> <p>PD4.3: Privacy assessments are carried out in line with MBIE's Privacy Policy, stepping through the full information lifecycle from collection to disposal, and each are triaged by the Privacy Team, with</p>

ID	MBIE Response
	clear expectations of project signoff.
PD5	<p>PD5.1: MBIE has a comprehensive and well-promoted privacy event register that captures all reported privacy complaints, breaches and near-misses. Information on how to identify and report privacy events is well documented and circulated, and is included in all relevant privacy training and engagement throughout the organisation. The Privacy Team triages and proactively supplies guidance and support to appropriately contain, manage and escalate all privacy events. Information about root causes of privacy events is collated, reported, and used to inform messaging and engagement to ensure trends are identified and lessons learned from privacy events can be incorporated into future privacy-related processes and procedures.</p> <p>PD5.2: MBIE's Privacy Threshold and Privacy Impact Assessment process clearly defines the purpose of collection of personal information, and this is a requirement of all new or significantly updated projects that involve the collection of personally identifiable information.</p> <p>PD5.3: MBIE has a clearly defined Retention and Disposal schedule that is referenced whenever applicable in all relevant Privacy Threshold or Privacy Impact Assessments. The Privacy Team regularly engages with MBIE's Information Management function, and the Privacy Team includes two secondees who each have an extensive background in data management.</p>
PD6	<p>PD6.1: MBIE has a comprehensive Privacy Policy, and a suite of information sharing agreements that support the appropriate use and disclosure of personal information, incorporating the considerations of a number of related pieces of legislation that interact with our responsibilities and functional requirements.</p> <p>PD6.2: All collection and use of personally identifiable information falls under MBIE's overarching Privacy Policy. If that information is then published or shared in an aggregated or non-identifiable way, this will inform the overall risk profile of each individual project. Our privacy assessment process takes into account the non-identifiable use or disclosure of personal information, queries the possibility of re-identification, and is designed to ensure the protection of personal information used in this way.</p>

RELEASED UNDER THE OFFICIAL INFORMATION ACT