Privacy Management Plan - Trans-Tasman IP Attorneys Disciplinary Tribunal

Background

This Privacy Management Plan (**PMP**) is a strategic planning document in which the Trans-Tasman IP Attorneys Disciplinary Tribunal (**the Tribunal):**

- identifies specific, measurable privacy goals and targets; and
- sets out how the Tribunal will meet its compliance obligations under Australian Privacy Principle 1.2 of Schedule 1 of the *Privacy Act 1988* (**Act**).

The Tribunal will measure and document its performance against this PMP at least annually.

An effective PMP will help embed within the Tribunal, a culture that respects privacy and will assist the Tribunal to build a reputation for strong and effective privacy management. This PMP will provide the Tribunal with the opportunity to improve productivity, develop efficient processes and manage both the risk of a privacy breach and its response, should a breach occur.

About this PMP

This PMP describes the actions that the Tribunal will take to meet its privacy compliance obligations and maturity targets for the year following the PMP's Commencement Date (specified below). The Tribunal will take steps to achieve these actions and record how it has done so with support from the Tribunal's Secretariat and Privacy Officers in IP Australia.

During the Recommended Review Period (specified below), the Tribunal will review this PMP and assess how well it has met and delivered its privacy targets.

PMP commencement date	23-01-2024
PMP end date	Following commencement, this PMP will operate until 30 June 2024 or the date on which the Privacy Management Plan is next updated after 30 June 2024.
Recommended review period	Annually (Review to be undertaken in Q4 of the Financial Year).

Privacy risk profile

The Tribunal's privacy risk profile is **medium**. Agencies with medium privacy risk profiles are agencies which provide some public services but handle less personal information, or which influence the privacy practices of other agencies. The Office of the Australian Information Commissioner (**OAIC**) advises that 'agencies that administer payments or provide individual services will generally have a higher privacy risk profile…because handling personal information is a core function'.

An objective assessment of the Tribunal's obligations under the Act, its activities and functions, the nature and volume of the personal information it holds and the sensitivity of this information has resulted in a medium privacy risk profile rating. The rationale for this risk profile rating is outlined below.

The Tribunal's Medium Privacy Risk profile rationale

(1) **The Tribunal's Functions and Activities**: The Tribunal is a statutory body established under regulation 20.61 of the *Patents Regulations 1991*. The functions of the Tribunal are to hear and determine disciplinary proceedings commenced by the Trans-Tasman IP Attorneys Board (**the Board**) against an individual patent attorney in Australia or New Zealand, or an individual trade marks attorney in Australia (collectively **registered attorneys**), or an incorporated patent attorney in Australia or New Zealand, or an incorporated trade marks attorney in Australia. In accordance with performing its functions and activities, the Tribunal may collect, hold, use and/or disclose personal information as enabled by the relevant Acts and Regulations administered by IP Australia.

Where required by legislation or otherwise appropriate, the Tribunal may also refer matters to the Board. Personal information collected by the Tribunal may be disclosed to overseas recipients. In particular, some members of the Tribunal are New Zealand residents and personal information, including (potentially) sensitive information may be disclosed to these persons, for the purposes of conducting disciplinary proceedings against a registered attorney.

It is not anticipated that the Tribunal will conduct any high privacy risk projects in the short-term that will involve a new or changed way of handling personal information that is likely to have a significant impact on the privacy of individuals – which would require a Privacy Impact Assessment to be completed under the Code. The Tribunal also only meets when there has been a matter referred to it by the Board. This referral is very infrequent (once every two to three years).

(2) **Privacy Influence and Trust**: The Tribunal collects personal information via individuals making a complaint about the conduct of a registered attorney; parties to proceedings (or their authorised representatives); and witnesses summoned to appear at proceedings or provide written evidence. The Tribunal depends on the trust of the community to continue to maintain its professionalism, integrity and reputation.

(3) **Amount and Type of Personal Information Handled:** The Tribunal handles a small volume of personal information. This information may include the following: the names and addresses of registered attorneys; the name and contact details of a complainant (including address, email address, phone and fax number); educational qualifications and academic performance of registered attorneys; employment details and statement of skills of registered patent or trade marks attorneys; details of the registered attorney's professional dealings with the complainant; details of any alleged unprofessional or unsatisfactory conduct; character references; details of any alleged fraud, or alleged failure to hold required academic qualifications or meet knowledge requirements at the time of registration; and any other personal information included in a complaint or in the supporting evidence for a complaint (including personal information of a witness summoned to appear or provide written evidence). The Tribunal may also be required to collect sensitive information, for example, to commence proceedings.

The Tribunal's Maturity Framework – Current state

This PMP assesses and records the Tribunal's privacy maturity levels in accordance with OAIC's Privacy Maturity Assessment Framework (**Maturity Framework**). The Maturity Framework consists of five elements, each of which are critical tenets of APP 1.2 and Code compliance, and constitute good privacy practice. The five elements are:

1. **Governance & Culture** – This element measures how well the Tribunal has established robust governance structures for privacy and embedded privacy into its culture.
2. **Privacy Strategy** – This element measures how well the Tribunal has integrated privacy into other key information management disciplines.
3. **Privacy Processes** – This element measures how fit-for-purpose, comprehensive and effective the Tribunal's key privacy processes are.
4. **Risk & Assurance** – This element measures how well-developed the Tribunal's privacy risk and assurance processes are.

5. **Data Breach Response** – This element measures how ready the Tribunal is to handle a data breach and to learn from it.

Within each of the five elements sits a set of attributes. Attributes are the criteria against which the Tribunal measures privacy maturity. There is a total of 21 attributes under 5 elements. The Maturity Framework requires agencies to self-assess their maturity across four maturity levels of 'Initial', 'Developing', 'Defined' and Leader. If the maturity level is 'Initial', this indicates the agency's privacy practice is ad hoc and unpredictable. Practices, procedures and systems are reactive and inconsistent, relying on individual effort and heroics. If the maturity level is 'Developing', this indicates that privacy practice is improving, with repeatable processes developing. Practices, procedures and systems are more proactive and repeatable. If the maturity level is 'Defined', this indicates the privacy culture is well developed and defined. Practices, procedures and systems are consistent, proactive, documented, integrated into broader organisational frameworks and measured. Where the maturity level is set at 'Leader', the agency takes an innovative approach to achieving privacy best practice. Practices, procedures and systems are continuously improved and the Leader helps others to innovate and achieve.

The maturity levels are shown in the following section.

Privacy maturity assessment outcomes

1. Governance & Culture				
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**	**Steps to reach target level**
1.1 Privacy Champion	**Defined**	**Defined**	The Tribunal has designated a Privacy Champion under the *Privacy (Australian Government Agencies – Governance) APP Code 2017*. As IPA provides Secretariat services for the Tribunal, the Privacy Champion of IP Australia, being the Deputy Director General of IP Australia, is the designated Privacy Champion of the Tribunal. to the Privacy Champion consistently promotes a culture of privacy that values and protects personal information and support the integration	Steps to improve the privacy culture within the Tribunal will include: - the Privacy Champion continuing to leverage privacy resources and best practice approaches used by other agencies to strengthen privacy culture through the Privacy Champions Peer Group. - The performance of the Tribunal in relation to privacy to become a KPI for the Privacy Champion.

			of privacy practices, procedures and systems into broader organisational frameworks.	- The Privacy Champion will have a mandate to engage and speak publicly on relevant issues including greater participation in Privacy Awareness Week activities
1.2 Privacy Values	**Defined**	**Defined**	The Tribunal's documented values clearly promote a culture of respecting and protecting personal information to build trust. The Tribunal's PIA and privacy evaluation processes incorporate an assessment of how the initiative aligns to the Tribunal's values. The Tribunal relies on IP Australia's PIA and privacy evaluation processes.	
1.3 Privacy Officer	**Defined**	**Leader**	IP Australia's Privacy Officers are the designated Privacy Officers for the Tribunal. They have established practices, procedures and systems to support their obligations and these are documented and integrated into broader organisational frameworks. There is a Tribunal wide awareness of the Privacy Officers. The Privacy Officers make proactive privacy improvements which extend beyond compliance, and their performance is measured in this regard.	The Privacy Officers will continue to review practices, procedures and systems that correlate with the Tribunal's data governance, customer engagement and business functions to identify innovative ways to achieve the Board's privacy goals. The Privacy Officers will also continue to discuss best practice privacy approaches with other organisations at forums targeted toward privacy officers (OAIC and AGS events) when opportunities arise. The Privacy Officers will assist the Privacy Champion in raising awareness of privacy values, including assisting with Privacy Awareness Week.
1.4 Management & Accountability	**Developing**	**Defined**	The Tribunal has ultimate responsibility for maintaining privacy compliance. Activities associated with compliance are undertaken by IP	Employ communications to raise the Tribunal's awareness of how to seek assistance on privacy issues.

			Australia's Privacy Officers, on behalf of the Tribunal. There is adequate resourcing for managing privacy compliance activities (for example, handling enquiries, complaints, and access and correction requests). Some members are aware of privacy accountabilities and how to seek assistance. The Secretariat supports the Tribunal and IP Australia's Privacy Officers in maintaining privacy compliance.	IP Australia's Privacy Officers will keep the Tribunal's privacy practices under continuous review, including reviewing privacy policies and notices regularly.
1.5 Awareness	**Developing**	**Defined**	Tribunal members view privacy neutrally as a compliance issue. There is a developing appreciation of the importance of privacy.	Due to the ad hoc nature of Tribunal meetings, Tribunal members will be emailed every 6 months about privacy awareness issues. The information in these emails is developed by the IP Australia's Privacy Officers and circulated by the Tribunal secretariat. Privacy Officers will look to change perception on privacy so the Tribunal's views it as a positive and valuable part of business as usual, this will be done by strengthening the knowledge of policies and expectations; encourage the Tribunal to provide feedback on the privacy processes; and create a culture that respects privacy and treats both personal information and data as a valuable asset.

2. Privacy Strategy				
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**	**Steps to Reach Target Level**

2.1 Privacy Management Plan	**Developing**	**Defined**	The Tribunal has a Privacy Management Plan in place and some Tribunal members are aware of it. The Privacy Management Plan includes measures for addressing any known privacy compliance gaps.	The Privacy Management Plan is approved by the President and is circulated to the Tribunal members when updates are made or during the onboarding process for new Tribunal members.
2.2 Inventory of Personal Information	**Defined**	**Defined**	There are established processes to access or provide access to personal information. The Tribunal has documented its personal information holdings, and understands all data flows in and out of the Tribunal (including where third parties hold that information). The Tribunal cannot access the database that holds the relevant personal information. However, the Secretariat, as the only Team who has access to the information, can provide access to the Tribunal on an as needed basis. Ownership, accountability and access to the registered attorney databases that hold personal information are clear and documented. The record also details how long the information will be retained and when it will be de-identified and destroyed. The Tribunal Secretariat has implemented processes that routinely monitor changes to its personal information holdings. The processes for documenting the relevant matters in relation to personal information holdings and monitoring changes are managed by the Secretariat.	
2.3 Data Quality Processes	**Defined**	**Defined**	Existing procedures and systems managed by IP Australia routinely empower individuals to keep the personal information that the agency holds	

			about them complete, accurate and up to date. The onus to ensure that personal information is up-to-date and accurate is on the attorney. The Secretariat is in regular (at least once a year) contact with attorneys and conducts activities that encourage attorneys to update their personal information.	
2.4 Information Security Processes	**Defined**	**Defined**	The Tribunal and Secretariat have an established information-security aware culture and understand that the Tribunal relies on IP Australia's IT systems to store and access personal information. The Tribunal can only access information stored on those systems via the Secretariat – no Board member has access to IP Australia's systems. The Tribunal and Secretariat members understand the commonalities and differences between privacy and security and are aware of all relevant privacy and security policies and processes. Policies and processes of IP Australia that extend to the Tribunal and Secretariat relating to mutual risks and issues (such as data breaches, access controls, appropriate use of technology, workplace surveillance, retention etc.) integrate privacy and security requirements with clear hand off processes to reduce delay and duplication of effort by stakeholders.	

3. Privacy Processes

Attribute	Current Level	Target Level	Rationale/Commentary	Steps to Reach Target Level
3.1 External Privacy Policy & Notices	**Defined**	**Defined**	Privacy messaging is viewed positively as an important part of the Tribunal's privacy practice. A clear, comprehensive and plain English privacy policy is provided to the public and goes beyond compliance, focusing on customer experience, openness and transparency. There is a clear link between privacy notices, and the privacy policy and privacy messaging is consistent and easy to locate.	
3.2 Internal Policies & Procedures	**Developing**	**Defined**	Internal privacy policies and procedures are in place and can be readily accessed and used. The Tribunal is aware of these policies and procedures, although they may not have worked directly with them. Internal privacy policies and procedures are regularly reviewed to ensure compliance with current law or relevance to agency practices (the Tribunal Privacy Policy was last updated in 2022).	
3.3 Privacy Training	**Developing**	**Defined**	Information is provided to all members of the Tribunal and Secretariat on induction then as required (i.e. if requirements were to change) annually. Information tends to target specific issues without sufficient context or an explanation of broader privacy issues. Member completion rates and understanding of privacy is not monitored unless there is a breach or complaint.	Privacy Officers will develop privacy training material to be included in Tribunal Member onboarding and to occur annually in line with privacy awareness efforts

3.4 Privacy Impact Assessments	**Developing**	**Defined**	PIA process exists but it is only used for high privacy risk projects. Privacy issues which do not meet the high privacy risk threshold are rarely considered. The Tribunal has not been involved in a high privacy risk project.	A newly-developed Privacy Impact Threshold Assessment Template will be made available by Privacy Officers in IP Australia to help determine if a PIA is required for new project by the Tribunal
3.5 Dealing with Suppliers	**Defined**	**Defined**	A documented and clear assessment process exists in IP Australia that applies to Tribunal related procurements and is applied consistently where a third party may have access to personal information. Third parties are only engaged if their privacy practices are equivalent to the Tribunal's or any gaps are mitigated by contractual controls. Contractual terms relating to privacy are supported by documented operational processes between the parties (for example on incident management and escalation processes).	
3.6 Access & Correction	**Defined**	**Defined**	Clearly documented processes exist that are consistently applied in respect of access to Tribunal related information and queries about Tribunal related privacy and information matters, with a strong understanding by the Tribunal Secretariat of rights and processes. Privacy Officer acts as a central contact on privacy matters within the agency, however responses can be decentralised to the Tribunal Secretariat where appropriate. Request handling is open, collaborative and customer-focused. Privacy Act response timeframe rarely exceeded.	

3.7 Complaints & Enquiries	**Defined**	**Defined**	The Tribunal's webpagerefers the public to a specific privacy contact channel (privacy@ipaustralia.gov.au) which directs complaints or enquiries to the Privacy Officers in IP Australia. If privacy complaints or enquiries are made through the Secretariat, the Secretariat will refer the matter to the Privacy Officers in IP Australia.	

4. Risk & Assurance				
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**	**Steps to Reach Target Level**
4.1 Risk Identification & Assessment	**Defined**	**Defined**	Strong, clear and consistent processes exist in IP Australia that extend to Tribunal activities for identifying and assessing privacy risks. Privacy in relation to Tribunal matters and information is integrated into IP Australia's wider risk management framework. Proactive steps are taken to identify privacy risks using all available sources of information (such as complaints, breach data, enquiries etc.).	
4.2 Reporting & Escalation	**Defined**	**Defined**	Privacy is monitored within IP Australia's broader risk and assurance framework, which extends to Board related activities, providing an integrated way of reporting on privacy risks, issues, incidents and complaints to the Tribunal. The Tribunal, through IP Australia, documents its compliance with privacy obligations, including keeping records on privacy process reviews, breaches and	

			complaints and routinely reflects on ways to improve its processes. The Tribunal's PIAs, privacy management plans and reviews of internal processes are endorsed by the Tribunal's privacy champion.	
4.3 Assurance Model	**Developing**	**Defined**	Some assurance activities occur in respect of the Tribunal's privacy management plan, processes and controls and in response to breaches or incidents, as part of IP Australia's broader assurance activities. For example, the 'three lines of defence' model has been adopted for specific risks such as incident management. Under this model: • First line - privacy controls are implemented in response to breaches or incidents. • Second line - the Privacy Officer has oversight over breaches or incidents and controls that are adopted. • Third line - internal audit staff conduct assurance activities to ensure that controls are being applied properly.	The Privacy Officers will continue to investigate measures to further develop assurance activities. OLC may also consider a semi-regular external audit of privacy processes.

5. Data Breach Response				
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**	
5.1 Data Breach Response Plan	**Defined**	**Defined**	There is a plan in place for data breaches relating to Tribunal activities and information with clear and documented roles and escalation paths. Members are aware of how to recognise a data	The Privacy Officers will continue to test the Data Breach Response Plan to gauge its effectiveness against different scenarios. From this testing Privacy Officers will continue to

			breach and are likely to speak up. There is a strong culture of openness and trust that results in confidence and honesty. Accountabilities for data breach responses and decision making are spread across the agency. Process is integrated with other critical business functions, including information security, communications and risk and assurance. Effective processes exist to ensure lessons learned and prevention measures are documented and implemented. Greater awareness is needed and processes need to be developed to ensure relevant parties are included in data breach responses.	document lessons learned and implement prevention measures identified. Privacy Officers will continue to train Tribunal Members on identifying and escalating issues. Privacy officers will also develop process to ensure all relevant parties are included in the data breach response from the start.
5.2 Data Breach Notification	**Defined**	**Defined**	Clear processes are in place to evaluate breaches relating to Board activities and information and to assess whether notification is necessary or desirable. Other stakeholders understand the obligations and benefits of notification.	

Adequacy of privacy policy and notices

Section 17 of the *Privacy (Australian Government Agencies – Governance) APP Code 2017* (**the Code**) requires an agency to regularly assess the adequacy of its privacy practices, procedures and systems (including its privacy policy and collection notices) to ensure their adequacy for the purpose of compliance with the APPs and currency. Generally, completion of a PMP facilitates compliance with this requirement.

The Tribunal's Privacy Policy is currently being reviewed and a review of the Tribunal's privacy notices is due to commence. The privacy policy and privacy notices will be reviewed regularly, in line with the activities in the PMP. This ensures compliance with the Code.

Goals for improvement

The privacy goals and targets in this section are based on the Tribunal's privacy maturity assessment outcomes. This section includes mandatory actions which the agency must take in order to meet its compliance obligations under APP 1.2 (Code, s 9(2)(b)), include improving our timeliness to respond to privacy complaints / queries.

Compliance Actions

Where an agency has identified in its privacy maturity assessment that it is at the 'Initial' level in relation to a compliance attribute, this indicates that there is a compliance gap because the agency must have a minimum maturity level of 'Developing' for that attribute in order to comply with the Privacy Act or the Code. All compliance gaps must form part of this PMP and may require prompt remediation. Remediation actions are set out below.

Attribute	Remediation action	Responsible person, position or team	Due	Required resources, dependencies and/or related documents (specify or link)
No compliance actions have been identified in this PMP.				

Privacy Policy & Notices Actions

Remediation actions related to any gaps in the adequacy of the agency's Privacy Policy (APP 1) or Privacy Notices (APP 5) are captured below.

Gap Type	Remediation actions	Responsible person, position or team	Due	Required resources, dependencies and/or related documents (specify or link)
There are no privacy policy & notices actions defined in this PMP.				

Maturity Improvement Actions

The table below sets out actions which the Tribunal plans to achieve in order to improve its privacy maturity. Any uncompleted actions from previous PMPs which are still relevant should also be documented in this section to ensure that they form part of the agency's next PMP.

Attribute	'Developing' Criteria	'Defined' Criteria	Reasons 'Defined' Criteria is not currently met	Actions	Responsible person, position or due	Due
1.4 Management & Accountability	Tribunal has assigned responsibility for privacy compliance including senior oversight and operations. There is adequate resourcing for managing privacy compliance activities (for example, handling enquiries, complaints, and access and correction requests). Some staff are aware of privacy accountabilities and how to seek assistance.	Roles and accountabilities for privacy compliance and oversight are documented and well understood across the agency, and messaging regarding roles and accountabilities is tied to the agency's broader strategic objectives. The agency regularly measures its performance in relation to privacy management (for example, timeliness and quality) and seeks to implement learnings for	There is a need to raise the Tribunal's awareness around roles and accountabilities for privacy compliance, in particular where to go for assistance with privacy issues.	Communications to raise the Tribunal's awareness of how to seek assistance on privacy issues. IP Australia's Privacy Officers will keep the Tribunal's privacy practices under continuous review, including reviewing privacy policies and notices regularly.	OLC with Secretariat	30 June 2024

		continuous improvement.				
1.5 Awareness	Members view privacy neutrally as a compliance issue. There is a developing appreciation of the importance of privacy.	Staff view privacy as a positive and valuable part of business as usual. There is strong knowledge of agency policies and expectations. Staff are encouraged to take opportunities to provide feedback on the agency's privacy processes (via established channels such as suggestion boxes and staff meetings).	No current process for Tribunal members to provide feedback on privacy matters.	Due to the ad hoc nature of Tribunal meetings, Tribunal members will be emailed every 6 months about privacy awareness issues. The information in these emails is developed by the IP Australia's Privacy Officers and circulated by the Tribunal secretariat. Privacy officers will look to change perception on privacy so the Tribunal views it as a positive and valuable part of business as usual, this will be done by strengthening the knowledge of policies and expectations;	OLC with Secretariat	30 June 2024

				encourage the Tribunal to provide feedback on the privacy processes; and create a culture that respects privacy and treats both personal information and data as a valuable asset.		
2.1 Privacy Management Plan	Tribunal has a Privacy Management Plan in place and some staff are aware of it. The Privacy Management Plan includes measures for addressing any known privacy compliance gaps.	Senior management and key staff are aware of the agency's Privacy Management Plan and the agency's primary objectives under it. The Privacy Management Plan is considered when setting resourcing budgets for the year ahead. The Privacy Management Plan addresses the handling of personal information	There is a need to raise the Tribunal's awareness of the Privacy Management Plan and the primary objectives under it.	The Privacy Management Plan is agreed to by the Privacy Champion and is to be circulated to the Tribunal when updates are made or during the onboarding process for new Tribunal members.	OLC with Secretariat	Q1 FY23/24

		throughout the information lifecycle with specific consideration given to areas that the agency assesses as having greater risk. It also includes actions to improve privacy maturity outcomes.				
3.2 Internal Policies & Procedures	Some internal privacy policies and procedures are in place but they are not comprehensive and are highly compliance-focused and poorly operationalised. Some members are aware of these policies and procedures, but they may not be consistently followed. Internal privacy policies and procedures are regularly reviewed to ensure compliance with current law or relevance to agency	Clear, relevant and comprehensive internal privacy policies and procedures are in place. Internal privacy policies and procedures go beyond compliance and are well-operationalised. Staff are aware of these policies and procedures and they are followed consistently, resulting in a common approach to privacy	The Tribunal has an external facing privacy policy but has no internal privacy policies and procedures.	Develop internal privacy procedures	OLC with Secretariat	Q2 FY23/24

	practices.	across the agency. Internal privacy policies and procedures are proactively reviewed to ensure compliance with current law, community expectations and relevance to current agency practices and in response to privacy risks and opportunities.				
3.3 Privacy Training	Training is provided to all staff on induction and annually. Training is compliance-focused and tends to target specific issues, such as information security and secrecy obligations without sufficient context or an explanation of broader privacy issues. Staff completion rates and understanding of	Training is operationalised to ensure relevance to all staff depending on their role and business unit. A clear and integrated training program is in place with regular opportunities for refresher or more specialised training (for example, on drafting a PIA as part	There is currently no formal privacy training provided to new Tribunal members	Develop privacy training material to be included in Tribunal Member onboarding and to occur annually in line with privacy awareness efforts	OLC with Secretariat	Q2 FY 23/24

	privacy is not monitored unless there is a breach or complaint.	of a change-management process). Training goes beyond compliance, is comprehensive, links to the agency's internal and external policies and messaging and is periodically updated Staff completion rates and understanding of privacy are monitored.				
3.4 Privacy Impact Assessments	PIA process exists but it is only used for high privacy risk projects. Privacy issues which do not meet the high privacy risk threshold are rarely considered. Where PIAs are completed, they are run by privacy or risk staff and not well integrated into wider agency change management	Clear PIA process exists which is well-integrated into other risk assessment and change-management processes and connected to the agency's values. Preliminary risk assessments are routinely undertaken to assess whether or not a PIA is required. PIAs are completed by	There is currently limited understanding of Tribunal members about when a PIA is required.	A newly-developed Privacy Impact Threshold Assessment Template will be made available by Privacy Officers in IP Australia to help determine if a PIA is required for new project by the Tribunal	OLC with Secretariat	Q2 FY 23/24

	processes.	relevant change manager or project manager in collaboration with privacy and risk staff. PIAs are independently reviewed when appropriate.				
4.3 Assurance Model	Some assurance activities occur in respect of the privacy management plan, processes and controls and in response to breaches or incidents. For example, the 'three lines of defence' model has been adopted for specific risks such as incident management. Under this model: • First line - privacy controls are implemented in response to breaches or incidents.	Well-developed assurance activities occur in respect of the privacy management plan, processes and controls and other identified risks, or proactively because of other risk identification activities. A defined 'three lines of defence' model is in place, with strong privacy officer involvement: • First line - operational privacy risks are identified and	The first line of defence not in place. Privacy risks need to be identified and recorded in a risk register. The third line of defence needs to be in place. No internal audit (or independent assessors) conduct regular privacy-related assurance activities.	The Privacy Officers will continue to investigate measures to further develop assurance activities. OLC may also consider a semi-regular external audit of privacy processes.	OLC with Secretariat	30 June 2024

	• Second line - the Privacy Officer has oversight over breaches or incidents and controls that are adopted. • Third line - internal audit staff conduct assurance activities to ensure that controls are being effected properly.	recorded in risk register and control activities are documented. • Second line – the Privacy Officer collaborates with information security, data governance and risk functions to provide oversight of privacy risk management. • Third line - internal audit (or independent assessors) conduct regular privacy-related assurance activities.				
Attribute	**'Defined' Criteria**	**'Leader' Criteria**	**Reasons 'Leader' Criteria is not currently met**	**Actions**	**Responsible person, position or due**	**Due**
1.3 Privacy Officers	The designated Privacy Officer has established practices, procedures and systems to support their obligations and these are documented	The designated Privacy Officer has established practices, procedures and systems that correlate with the agency's data governance, customer	Whilst Privacy Officers have established privacy processes, more effort is needed to innovate, promote and share information relating to privacy.	The Privacy Officers will take initiative and continue to review practices, procedures and systems to identify innovative ways to achieve	OLC with Secretariat	Annually

	and integrated into broader organisational frameworks. There is agency wide awareness of the Privacy Officer. The Privacy Officer makes proactive privacy improvements which extend beyond compliance, and their performance is measured in this regard.	engagement and business transformation functions. The Privacy Officer is encouraged to innovate their practices, procedures and systems. The Privacy Officer willingly assists other agencies by sharing information and learnings about their role as Privacy Officer.		privacy goals. The Privacy Officers will discuss best practice privacy approaches with other organisations at forums targeted toward privacy officers (OAIC and AGS events) when opportunities arise. The Privacy Officers will assist the Privacy Champion in raising awareness of privacy values, including assisting with Privacy Awareness Week.		

Bringing the PMP together and prioritising actions

This section of the PMP identified all compliance actions and actions for improvement, as well as who is responsible for delivery of each action, interdependencies and due dates. From here, prioritisation is a key part of establishing an achievable PMP. Agencies should take a risk-based approach to prioritising and timing their improvement activities.

Measure performance

The Tribunal expects to review its performance under this PMP between 1 January 2024 and 30 June 2024. The table below provides a central location to track progress.

Action	Achieved	Future actions / commentary
1.1 Privacy to be considered a KPI for the Privacy Champion	Scheduled	Considerations on whether this should be included/has already been included as a KPI
1.1/1.3 Privacy Champion to engage and speak publicly on relevant privacy issues including involvement in Privacy Awareness Week activities.	Scheduled	Privacy Officers will continually engage with Privacy Champion on privacy awareness activities
1.3 Privacy Officers will continually review practices to identify innovative ways to achieve the agency's privacy goals and engage with other organisations when opportunities arise.	Scheduled	Privacy Officers will engage with this work throughout 2023 and 2024
1.4 Communications to raise the Tribunal's awareness of how to seek assistance on privacy issues with Privacy Officers and review Board's privacy practices	Scheduled	This will be included in new Tribunal member onboarding and as required at Tribunal meetings or out-of-session emails
1.5 Due to the ad hoc nature of Tribunal meetings, Tribunal members are emailed every 6 months about privacy awareness issues. The information in these emails is developed by the IP Australia's Privacy Officers and circulated by the Tribunal secretariat.	Scheduled	This will now become standard meeting practice
1.5 Raise awareness to change perceptions on privacy	Scheduled	Privacy Officers to raise awareness through communications
2.1 Provide the Tribunal with a copy of this plan	Scheduled	Update and review to be presented and approved out of session and shared during onboarding
3.2 Develop internal privacy procedures	Scheduled	Tribunal and Secretariat to consider this later in FY23/24 and will be assisted by Secretariat and Privacy Officers
3.3 Develop privacy training material	Scheduled	Tribunal to consider this during FY23/24 and will be assisted by Secretariat and Privacy Officers
3.4 Provide the Tribunal with guidance material on when a PIA is required	Scheduled	Tribunal will be assisted by Secretariat and Privacy Officers during Q2-Q3 FY23/24

4.3 Develop a Privacy Monitoring and Compliance Plan	Scheduled	Tribunal to consider this during Q3&Q4 FY23/24
5.1 Update Data Breach Response Plan to meet required standards	Scheduled	Privacy Officers to assist Tribunal to review Data Breach Response plan in Q2 FY23/24