information and privacy commission new south wales

Privacy Governance Framework

February 2024

Contents

Privacy Governance Framework 3
What are the legislative essentials? 4
Governance and leadership 5
Privacy program 7
Complaints and incident management 9
Evaluation, internal and external oversight 11

Privacy Governance Framework online

This document is also available in a web-based version via the IPC website: Privacy Governance Framework.

Privacy Governance Framework

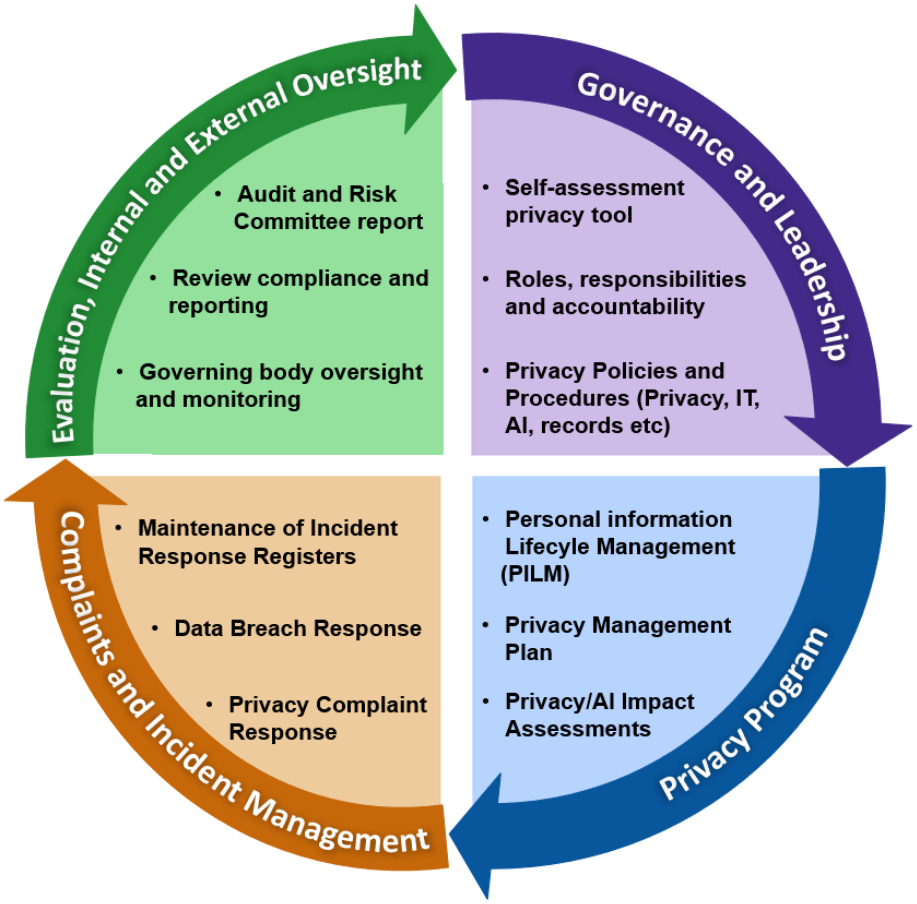
The Privacy Governance Framework (the Framework) is a dynamic tool designed to assist New South Wales public sector agencies implement robust privacy governance throughout their organisation to manage personal and health information.

Governance underpins effective and efficient public sector administration and facilitates the policy objectives of each agency, local council, state owned corporation and university. Privacy governance is an integral part of service provision and is the responsibility of governing authorities, the agency head, senior management, legal, information technology and privacy officers (explained in the Governance and Leadership section). While effective governance and leadership are essential, collaboration across the agency is a critical factor in achieving a robust privacy program.

This Framework can be used and incorporated into existing governance mechanisms within an agency. Oversight and accountability for privacy and the management of personal information can be achieved through existing audit and risk committee processes, or similar review and risk management oversight processes which are already in place.

The Privacy Governance Framework exists to provide guidance and help agencies, local councils universities and state owned corporations to comply with the *Privacy and Personal Information Protection Act 1998* (including the Mandatory Notification of Data Breach (**MNDB**) Scheme) (**PPIP Act**), the *Health Records and Information Privacy Act* 2002 (**HRIP Act**), by:

- Better understanding privacy risks and opportunities, including the potential use and implementation of new data driven technologies (e.g., artificial intelligence (**AI**));
- Addressing roles and responsibilities throughout the agency in relation to privacy management;
- Keeping the interests of the individual paramount in a user centric manner
- Embedding a proactive approach to privacy management and privacy-by-design throughout the agency;
- Implementing robust personal information lifecycles – that is, the collection, use, security and disposal of personal information complies with the PPIP Act and the HRIP Act;
- Prompt notification in the event of an eligible data breach to the NSW Privacy Commissioner and affected individuals where there is unauthorised access to or unauthorised disclosure of, or a loss of personal information that is likely to result in serious harm;
- Ensuring there are up-to-date privacy policies and procedures (including a privacy impact assessment policy and a data sharing and privacy policy), a privacy management plan and a data breach policy in accordance with the requirements of the PPIP Act, HRIP Act and MNDB Scheme;
- Ensuring there is privacy-by-default, and a transparent and open governance approach whatever the business practice or technology involved; and
- Embedding a culture of protecting personal information within the agency.



What are the legislative essentials?

The objectives of the PPIP Act and the HRIP Act are to give individuals confidence that the handling of their personal and health information by NSW public sector agencies is appropriate in all circumstances. Both Acts set the rules to support this.

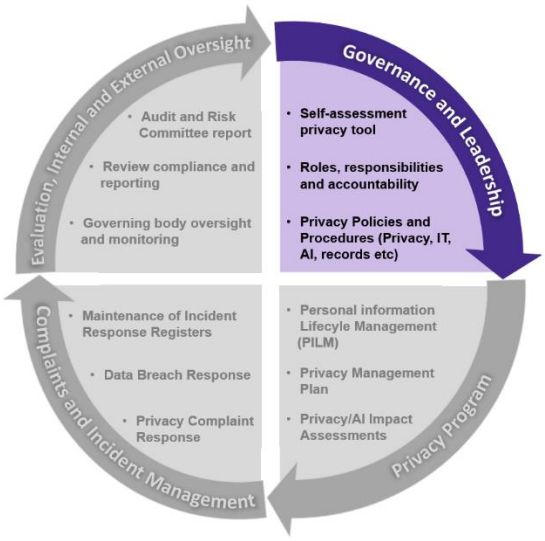
Personal information is any information that identifies an individual such as written records which may include an individual's name and address, photographs, images, video or audio footage.

Health information is any personal information or opinion about an individual's physical or mental health; health services provided to an individual or to be provided in the future; information collected in connection with organ donation; or other personal information that is genetic information about an individual arising from a health service provided.

The PPIP Act and the HRIP Act outline the responsibilities of agencies, the rights of individuals, and the role and functions of the Privacy Commissioner. At the heart of these are the Information Protection Principles (IPPs) and the Health Privacy Principles (HPPs). They follow the 'information life cycle' as agencies collect personal and health related information, process, store and share or dispose of it. The IPPs and HPPs are complemented by other mechanisms including codes of practice, public interest directions (where applicable), privacy management plans and complaints management.

Agencies must comply with these core requirements. The Privacy Governance Framework and the privacy program, which includes the privacy management plan, are the key mechanisms for complying.

Governance and leadership



Proactive governance leadership and management of personal information, health information and privacy will improve the overall information assets of your agency and build trust with your customers and users. Public and private sector organisations are becoming increasingly scrutinised on their handling of privacy issues, information security and risks. Therefore, it is important to ensure that an effective privacy governance framework is in place in your agency.

An effective privacy governance framework benefits everyone and begins with leadership by the agency head. A framework helps to clarify each person's role in privacy management and ensures that they are held to account. Once appropriate and adequate policies, processes, systems and reporting are in place, privacy management will be a seamless integration into business-as-usual practices. This will help foster a culture of viewing privacy and personal information as an asset and not as a liability.

A privacy governance framework should be included in the agency's Privacy Management Plan.

Roles and responsibilities

While the mix of roles and responsibilities will vary depending on an agency's size and circumstances, effective privacy implementation includes the following key functions and roles:

- **Privacy Officers** are responsible for developing privacy management plans, procedures, and conducting internal reviews. They should be sufficiently expert to inform agency staff and members of the public of privacy issues.
- **Information Technology** and **Cybersecurity staff** identifying and monitoring data privacy breaches.
- **Business Managers** are responsible for considering privacy issues, implementing privacy policies and procedures and managing the handling of personal information across their business unit activities (projects, programs and service delivery).
- **Human Resources** and/or the **Training and Development** function is responsible for inducting and training staff about the agency's privacy policies and procedures.
- **Front line staff** comply with the policies and procedures set out by their agency.
- **Governance** and **Legal** functions are responsible for ensuring and managing legal compliance, reporting and providing advice about the agency's privacy obligations and needs for flexibility.
- **Audit and Risk Committees** identify and monitor agency learnings and ensure risk frameworks adequately consider privacy risk impacts.

For an agency to achieve a robust privacy program, collaboration is essential across staff with key roles and responsibilities for privacy, information security, records and other areas appropriate to that agency.

Checklist

- Does the agency's leadership team understand their responsibilities under privacy legislation?

- Is a collaborative culture evident from the interactions of those with key roles and responsibilities across the agency?
  If not, what are the steps and mechanisms that can be put in place to achieve improved interaction and collaboration to achieve a robust privacy program?
- Do roles in my agency have clearly articulated privacy management responsibilities? Are staff aware of their own individual accountabilities? Privacy is everybody's business and responsibility.
- Do I have a forum where I can discuss privacy management issues and risks pertaining to my agency?
- Does my agency have adequate mechanisms in place to detect when privacy breaches occur? For example, do the data breach policy and the internal incident management framework enable staff to report privacy breaches at the time of occurrence? Does this process facilitate appropriate actions being taken to remediate a breach?
- Does my agency have any mechanisms in place to prevent a privacy breach from occurring? For example, IT security safeguards preventing inadvertent disclosure of information.
- Are my agency's privacy management plans, policies and procedures adequate and kept up to date?
- Does the agency's privacy management plan include details about its data breach response processes?
- Is privacy considered as part of the agency's change management framework?
- Do your strategic objectives call for greater sharing of personal and health information with other agencies?
- Do you want to analyse data about citizen interactions, or create health records linkages to plan or improve individual/wider agency services or develop policy?

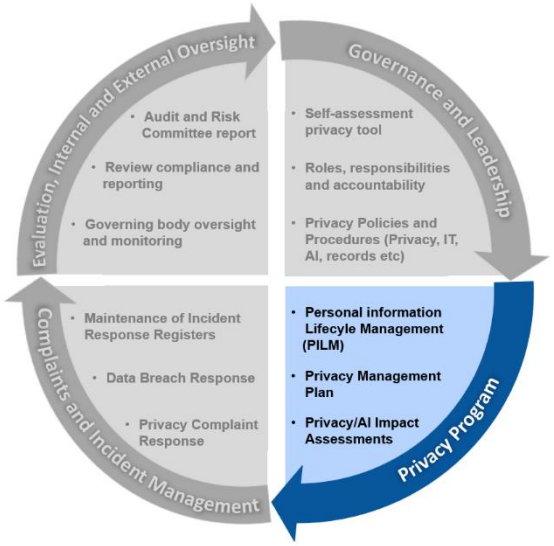
Where to start?

Carry out a Privacy Maturity Assessment to assess your agency's systems and policies to ensure their compliance with privacy requirements – download the Privacy Self-assessment Tool.

Resources

- Fact Sheet – The PPIP Act: Agency systems, policies and practices
- Information Governance Agency Self-assessment Tools
- Agency Privacy Management Plans
- Essential Guidance Toolkit on information access and privacy fundamentals
- The PPIP Act 1998
- The PPIP Regulation 2019
- Information Protection Principles (IPPs)
- The HRIP Act 2002
- Health Privacy Principles (HPPs)
- Privacy and health records – Codes of Practice
- Privacy and health records – Public Interest Directions
- Privacy and health records – Statutory Guidelines
- Understanding your privacy obligations

Privacy program



A privacy program provides a structured system to enable your organisation to comply with privacy regulatory requirements and ensure a transparent and open governance approach whatever the business practice or technology involved. Processes, procedures and policies need to be tailored to the individual functions and activities an organisation undertakes and should be reviewed periodically.

The foundation stone of the privacy program is the Privacy Management Plan, in which each public sector agency describes the strategic plan and measures it proposes to take to ensure that it complies with the PPIP Act, including the requirements of the MNDB Scheme, and the HRIP Act. Each NSW public sector agency **must** have a Privacy Management Plan and provide a copy to the NSW Privacy Commissioner. It should also be made publicly available on the agency's website and made available in other ways on request.

The privacy program enables each agency to manage multiple privacy priorities and projects including privacy-led initiatives, projects involving technology system changes or implementation of new technologies that store or use personal and/or health information.

The benefits of a privacy program include:

- Systematic approach to privacy projects, initiatives and priorities.
- Proactively managing personal information and improving personal information lifecycle management from collection to disposal throughout the agency.
- Implementing privacy-by-design, through Privacy Impact Assessments (**PIAs**) to ensure that privacy impacts are built into projects, proposed system changes, or new technologies including artificial intelligence (**AI**), that use and/or store personal information. PIAs should be reviewed and updated when material changes occur.
- Communicating material changes to policies, procedures and practices to employees and relevant stakeholders.
- Reducing risks of regulatory breach through the systemic and proactive approach implemented by the agency to comply with the PPIP Act and the HRIP Act.
- Reducing the risk of data breach by implementing the measures and systems required under the MNDB Scheme.
- Continual monitoring of the privacy program and its components**.**
- Evaluating and reporting on privacy performance within the agency as part of the agency's overall risk management, see the Evaluation, auditing and reporting section.

Checklist

- Is your agency's privacy management plan (**PMP**) up to date?
- Does your agency have a register of the types of personal information it holds, where that information is located and when it should be destroyed?
- Is your agency's data breach response plan (**DBR**) up to date?
- Do you have a systemised process for reviewing the PMP and DBR? This includes for example:

  - a timeframe requirement for the PMP and the DBR to be reviewed, such as annually; and
  - specifying the position responsible for carrying out and reporting on the review of each of the PMP and the BDR, together with any recommended updates to the PMP and DBR.
- Is there active personal information lifecycle management occurring on a continuing basis? This includes, for example:
  - Is only necessary personal information being collected, used and stored?
  - Is there a process in place to reconcile retention of personal information in accordance with record-keeping requirements with the requirement to dispose of personal information that is no longer required to be retained in accordance with the PPIP Act and the HRIP Act?
  - What is the mechanism for ensuring that personal information, which is no longer required to be retained, is being securely disposed of?
  - What are the roles and responsibilities of those involved in ensuring the above steps are actively managed and the collaboration across agency staff to ensure that personal information lifecycle management is occurring on a continuing basis?
- Are PIAs being carried out throughout the organisation for projects, system changes or changes to current or new technology including AI, involving the processing of personal information?

Privacy Program Components

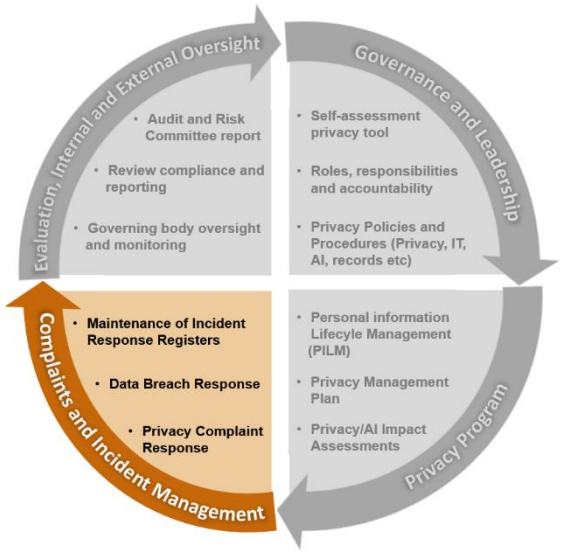
The privacy program includes:

- Privacy Management Plan
- Privacy Impact Assessments
- Privacy Protocol for Handling Complaints
- Managing data breaches in accordance with the PPIP Act

Relevant Resources

- Identifying Privacy Issues
- Privacy Compliance Checklist
- Privacy Management Plans Guide
- Privacy Management Plan Checklist
- Protocol on the preparation and assessment of Privacy Codes of Practice under the PPIP Act and HRIP Act
- Use of CCTV
- ID Scanning
- Mobile Apps: Know the Risks
- Privacy and persons with reduced decision-making capacity

Complaints and incident management



Transparency about how an agency manages its personal information and responds to complaints and data incidents involving personal information is fundamental to complying with the PPIP Act, HRIP Act and the MNDB Scheme.

Privacy complaints

A privacy complaint may come under:

- the PPIP Act, section 53, if it relates to personal information and the Information Protection Principles (IPPs); or
- the HRIP Act, section 21, if it relates to health information and the Health Privacy Principles (HPPs).

Complaints under PPIP Act and the HRIP Act are dealt with by way of Internal Review. The process is the same under both Acts although the alleged conduct is assessed against different standards (the IPPs and the HPPs). The process for carrying out the review and recording the determination is set out in the Privacy Internal Review for Agencies Checklist.

An agency should understand the role of the IPC and its approach to using its regulatory powers. IPC's Regulatory Framework describes how it aims to promote, assure, and enforce the PPIP and HRIP Acts.

Relevant Resources

- Privacy Internal Review for Agencies Checklist
- Managing Unreasonable Complainant Conduct
- Checklist for public sector staff: responding to a request for access to health information
- IPC Regulatory Framework

Data breach incidents

Agencies are required to prepare and publish a Data Breach Policy as required by the MNDB Scheme. The Data Breach Policy details how the agency will respond to a data breach including clear roles and responsibilities for managing a data breach or suspected data breach. The Policy sets out the steps the agency will follow if a breach occurs, including notifying affected individuals and the Privacy Commissioner.

Agencies are required to establish and maintain:

- An internal register of eligible data breaches; and
- A public register of any public data breach notifications made under section 59N(2) of the PPIP Act.

Relevant Resources

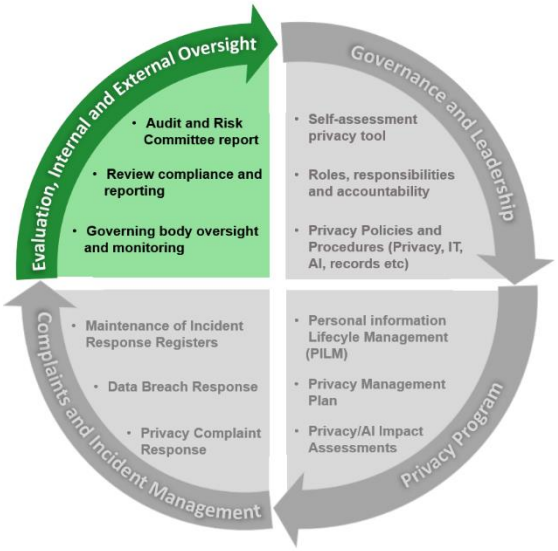
- Mandatory Notification of Data Breach Scheme
- Guide to preparing a data breach policy
- Fact Sheet for agencies: Exemptions from notification to affected individuals
- Guide to managing data breaches in accordance with the PPIP Act

- Form: Data Breach Notification to the Privacy Commissioner
- Guide to Regulatory Action under the MNDB Scheme
- Guideline - Guidelines on the assessment of data breaches under Part 6A of the PPIP Act
- Guideline - Guidelines on the exemption for risk of serious harm to health or safety under section 59W
- Guideline - Guidelines on the exemption for compromised cyber security under section 59X
- Data Breach Self-assessment Tool for MNDB
- Data Breach Prevention Checklist
- Fact sheet – NSW public sector agencies and data breaches involving tax file numbers
- Fact sheet – Tips for reducing data breaches when sending emails
- Transition to the Cloud: managing your agency's privacy risks
- Essential Eight Guide to managing cyber security incidents

Evaluation, internal and external oversight

Evaluation, auditing and reporting

Agencies should ensure that there are adequate processes in place to track and measure privacy performance. The identifiable privacy performance measures should then be reported to the agency leadership in accordance with the agency's risk management processes. Auditing and risk functions should ensure that privacy is part of the audit process within the agency, ensuring that its policies and processes are regularly reviewed, up to date, and fit for purpose. Additionally, agencies need to ensure they comply with regulatory oversight and NSW Government accountability mechanisms.



Agencies should have in place metrics and processes in place to collect data to track privacy management and the maturity of their privacy program over time. This can help support business cases for additional resourcing, demonstrate improved privacy maturity and/or show areas of weakness and opportunity. Importantly, it can also assist in building the overall operational resiliency of the agency.

Checklist

- Is data captured to assess privacy requests or complaint responses? If not, what metrics are appropriate to put in place? For example: the average length of time taken to respond to a privacy request, or the average length of time to carry out an internal privacy review.
- Is the organisation pro-actively examining the privacy implications, risks and benefits of new technologies it introduces into the organisation and have a process for addressing identified risks.
- Are organisational risk registers regularly reviewed to ensure privacy risks are being appropriately managed?
- Is your agency collecting data on personal information lifecycle management? For example, are systems being reviewed and measured:
    - to assess whether all of the personal information being collected is necessary, or
    - to ensure and record active disposal of personal information when it is no longer required to be retained?
- Is data being collected in relation to privacy training and awareness initiatives, and is it being included in your agency's overall privacy reporting?
- Is data being collected on privacy impact assessments (PIAs)? In particular, whether risk mitigation measures documented in the PIA have been carried out and whether any requirements for periodic reviews have been done, as required by a PIA.
- Are data breach incidents and reporting being included in your agency's overall privacy reporting?
- Following a data breach, and the investigation that the agency is required to carry out in 5.5.1 of the Guide to managing data breaches in accordance with the PPIP Act (i.e. to investigate what went wrong and to update relevant policies and procedures to remedy any issues to prevent future breaches), have the agreed remediation actions arising from the post-incident review been carried out and documented in the Privacy Management Plan?

What are the oversight and accountability mechanisms?

The PPIP Act and the HRIP Act make public sector agencies accountable for the way they handle personal information and health information and records, including sharing information with a third party.

These mechanisms include:

- The Privacy Commissioner's oversight role.
- Parliamentary oversight of the Privacy Commissioner via the Committee on the Ombudsman, the Law Enforcement Conduct Commission and the Crime Commission (OmboLECC).
- The NSW Civil and Administrative Tribunal who provide individuals with a channel for review and potential redress if their privacy concerns are unresolved.

Further mechanisms available under the HRIP Act include the ability to refer complaints, where appropriate, to the Health Care Complaints Commission and the Commonwealth Privacy Commissioner.

- *Annual Reports (Departments) Regulation 2010*
- *Annual Reports (Statutory Bodies) Regulation 2010*

Document information

Identifier/Title:	Privacy Governance Framework
Business Unit:	IPC
Author:	Privacy Commissioner
Approver:	Privacy Commissioner
Date of Effect:	February 2024
Next Review Date:	February 2026
EDRMS File Reference:	D24/000742/DJ
Key Words:	Privacy, governance, privacy program, complaints and incident management, evaluation, internal and external Oversight