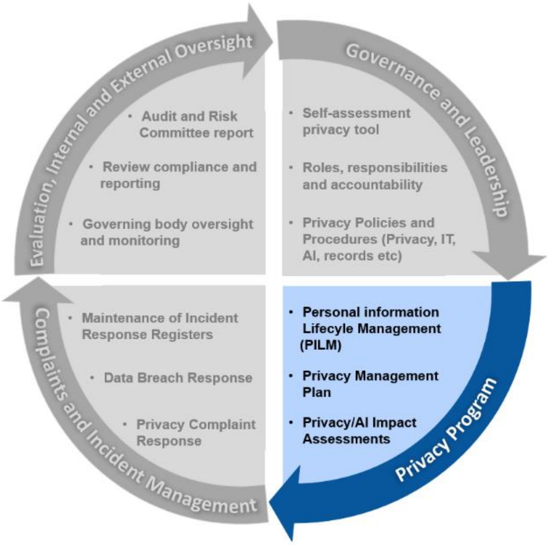
Privacy Governance Framework

February 2024

Privacy program


Evaluation, Internal and External Oversight
Audit and Risk Committee report
Review compliance and reporting
Governing body oversight and monitoring
Governance and Leadership
Self-assessment privacy tool
Roles, responsibilities and accountability
Privacy Policies and Procedures (Privacy, IT, AI, records etc)
Complaints and Incident Management
Maintenance of Incident Response Registers
Data Breach Response
Privacy Complaint Response
Privacy Program
Personal information Lifecyle Management (PILM)
Privacy Management Plan
Privacy/AI Impact Assessments

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