information and privacy commission new south wales

Privacy Governance Framework

February 2024

Privacy Governance Framework

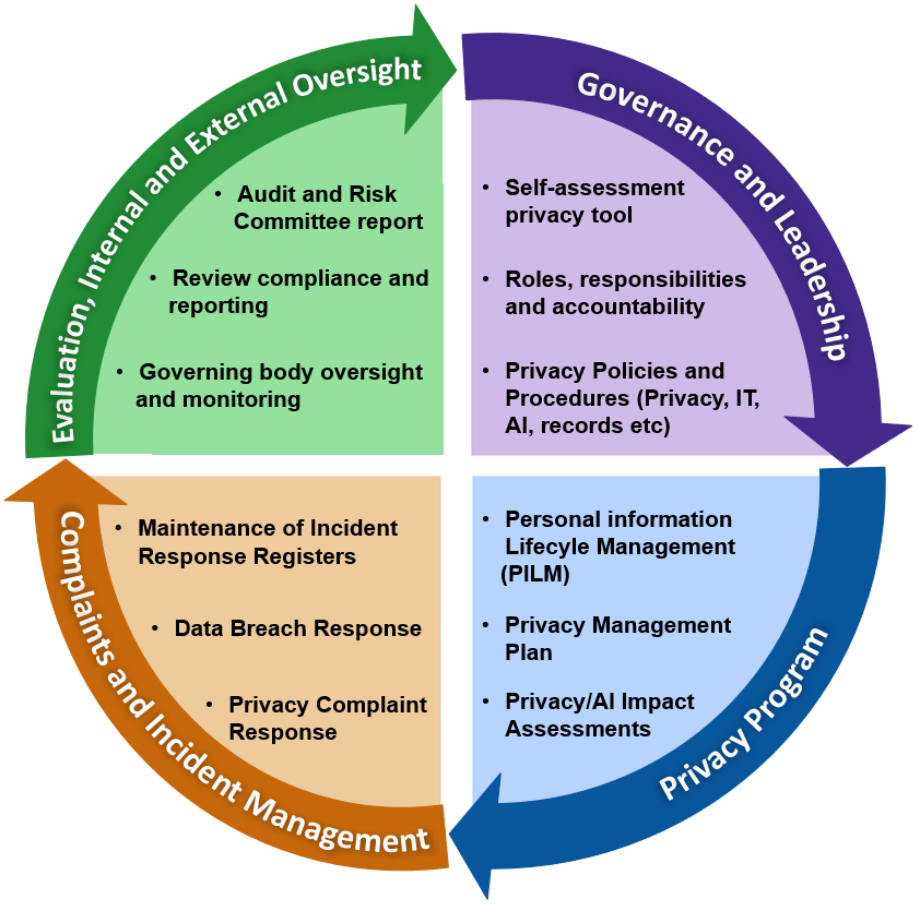
The Privacy Governance Framework (the Framework) is a dynamic tool designed to assist New South Wales public sector agencies implement robust privacy governance throughout their organisation to manage personal and health information.

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.