information and privacy commission new south wales

Fact Sheet **Updated November 2020**

The PPIP Act: Agency systems, policies & practices

This guidance is provided to assist agencies in the performance of their responsibilities under the *Privacy and Personal Information Protection Act 1998* (PPIP Act).

It provides suggested actions to improve agency systems, policies and practices that relate to the handling and management of personal information under the PPIP Act.

It provides useful and relevant guidance to all agencies covered by the PPIP Act about systems and processes that should be in place to support an effective privacy framework.

Operating environment in the public sector

The PPIP Act outlines the obligations to protect the personal information agencies collect about individuals and creates responsibilities for the management and handling of personal information. The Information Protection Principles (IPPs)[1] are legal obligations which NSW government agencies must abide by when they collect, store, use or disclose personal information. These obligations and responsibilities apply to all NSW government agencies, whether they are a state government agency, local council, university, or Minister/Minister's office.

To ensure agencies can confidently uphold their responsibilities under the PPIP Act, the statutory requirements must be well supported by leadership, investment in training, systems and processes, including assurances, certifications and a privacy respectful culture.

Managing privacy

The suggested actions set out below are designed to provide assistance and guidance to agencies in the exercise of privacy functions and respond to risks that may arise in the performance of those functions and decision-making arrangements:

1. **Delegations:** Agencies should regularly review their delegations to ensure that they reflect the requirements of the PPIP Act. Agencies are not permitted to delegate their obligations under the PPIP Act to other agencies, even if the other agency is within the same cluster. Where a person seeks internal review of an agency's conduct under Part 5 of the PPIP Act, the review is to be undertaken by that agency.
2. **Websites:** Agencies should regularly review their website content to update forms and information relevant to the operation of the PPIP Act and HRIP Act, including where agencies have been impacted by machinery of government changes.
3. **Policies:** Agencies should regularly review all of their policies relevant to privacy responsibilities to ensure that they accurately reflect any changes as a result of cluster arrangements. Following review of these policies, agencies should circulate and actively promote the location of updated policies to all staff.

Privacy Management Plans

The PPIP Act requires agencies to prepare and implement a Privacy Management Plan.[2]

A Privacy Management Plan should comply with section 33 of the PPIP Act and contain provisions relating to:

- the agency's policies and practices for complying with the PPIP Act and the HRIP Act
- how the agency will make its staff aware of these policies and practices
- the agency's procedures for dealing with privacy internal reviews under Part 5 of the PPIP Act
- other relevant matters relating to the protection of the personal and health information that the agency holds.

Agencies should ensure that their Privacy Management Plan is current and up to date.

The Privacy Management Plan should provide a clear policy statement that describes the types of personal information[3] that the agency collects, the purposes of the use of that personal information and where personal information is stored and how it can be accessed, particular to the agency's operating context.

[1] Sections 8-19 PPIP Act
[2] Section 33 PPIP Act
[3] Section 4 PPIP Act

Training and systems

Agencies should implement a program of regular training to support the performance of functions under the PPIP Act, which may also include information management more broadly, including:

- the agency Code of Conduct and Public Service Commission's Ethical Framework as they relate to the PPIP Act
- Privacy Management and Governance
- the offence provisions under the PPIP Act.[4]

Training should be tailored appropriately for specific roles and responsibilities, in particular, those charged with responsibility for collecting, using and disclosing personal information. That training should extend to all employees, including contractors and temporary employees, senior managers and executives. For all staff, training should be contextualised and specific to the functions of staff in their particular roles.

Agencies should develop a mechanism to ensure that their training content and policies are regularly reviewed to ensure currency, and that there is a process in place for staff to undertake refresher training at regular intervals.

Agencies should review and consider application of targeted and specific training that is contextualised to the functional policies in place, with focus on the privacy aspects of those roles and responsibilities. Agencies should implement a mechanism to ensure privacy training is available to new staff as part of the induction process and refresher training is available to all staff on an annual basis.

PPIP Act - Governance for authorised disclosure of personal information

Agencies should develop processes to inform the management of the authorised disclosure of personal information. Processes should include when, how and in what circumstances an authorised disclosure may be permissible and any authorisation approvals that must be in place to permit such disclosures.

PPIP Act - Privacy breach management

Agencies should have a comprehensive privacy breach management process and procedure in place that includes a risk assessment for any unauthorised disclosures should they occur. That process and procedure should:

- be a single and comprehensive policy for management of privacy breaches
- address the particularity of roles and responsibilities as appropriate to cluster agency, agency and functional areas
- provide for an escalation model
- address management of cyber security breaches which involve personal information
- clearly define what is personal information and what is a data breach
- specify a timeframe in which persons affected by a privacy breach will be notified
- include a mechanism of assurance for ensuring that the remedial actions have been implemented.

Privacy Reporting

Agencies should establish internal reporting requirements for privacy breaches to be reported to Senior Officers on at least a quarterly basis, including the number of breach notifications notified to the Privacy Commissioner. The report should include actions taken in response to advice suggested by the Privacy Commissioner, including where a decision is made to not adopt such advice, the reasons for not doing so, and the number of internal reviews/complaints received as a direct response to the data breach. More information on data breaches can be found on the IPC website.

For more information

Contact the Information and Privacy Commission NSW (IPC):

Freecall: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Website: www.ipc.nsw.gov.au

[4] Sections 62-63 PPIP Act