Fact Sheet March 2020

The Role of the Privacy Commissioner: Consulting the IPC on Initiatives and Projects

Public sector agencies and entities regularly consult the Privacy Commissioner and the Information and Privacy Commission (IPC) on initiatives and projects that may have privacy, data security or information governance dimensions.

This fact sheet sets out the best practice approach to incorporating privacy and information governance into the design of an initiative or project. Before consulting with the IPC, agencies should have addressed a number of considerations or taken actions that adhere to a best practice approach.

Role of the Privacy Commissioner and the IPC

Role of the IPC

The IPC is an independent, separate[1] agency established in 2011 that administers NSW legislation dealing with privacy and access to government information.

The IPC provides:

- independent oversight, review, complaint handling, investigative, reporting and monitoring of Minister's officers; State Owned Corporations[2]; the local government sector, public sector agencies and all NSW Universities in performance of privacy and information access functions.
- advice and assistance to agencies, entities and citizens about compliance with privacy and access to government information laws.

As a regulator of agencies and entities described above, the IPC and the Privacy Commissioner must maintain independence from government policy decisions and projects. Should a citizen complain to or seek review by the Privacy Commissioner about a government policy, program or decision, the Privacy Commissioner's functions and regulatory responsibilities must be freely exercised and not compromised.

What the Privacy Commissioner does

The Privacy Commissioner can:

- provide assistance to public sector agencies in adopting and complying with the information protection and health protection principles and privacy codes of practice
- initiate and recommend the making of privacy codes of practice
- provide advice on matters relating to the protection of personal information and health information and the privacy of individuals.

See section 36 of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) and section 58 of *Health Records and Information Privacy Act 2002* (HRIP Act) for a comprehensive list of the Privacy Commissioner's functions.

In consulting with the Privacy Commissioner (or the IPC) about a policy or project we can:

- Advise you about available privacy resources we have developed to assist you to comply with privacy laws
- Provide you with information about 'privacy by design' and privacy impact assessments (see below)
- Refer you to any relevant research, programs or policies relating to the protection of personal information and the privacy of individuals
- Advise about the application of public interest directions or codes of practice
- Advise about the IPC's regulatory functions.

[1] Part 3 of Schedule 1 of the Government Sector Employment Act 2013.

[2] Only in respect of the *Government Information (Public Access) Act 2009*.

What the Privacy Commissioner does not do

The Privacy Commissioner is a statutory officer and not a public service employee.[3] The Privacy Commissioner independently regulates government and private sector entities.

For more information on the Privacy Commissioner's Jurisdiction see: Fact Sheet - IPC Privacy Statement of Jurisdiction.

As an independent regulator, the Privacy Commissioner cannot:

- Endorse an initiative or project as privacy compliant
- Conduct or write a privacy impact assessment for an agency or entity
- Comment on the policy objectives of the program or project
- Give a public interest direction unless the Privacy Commissioner is satisfied that the public interest in requiring the agency to comply with privacy laws is outweighed by the public interest in the making the direction[4]
- Give legal advice about the interpretation or application of privacy laws
- Give advice about privacy laws of other jurisdictions.

Privacy Considerations of an Initiative or Project – Best Practice

General considerations

Agencies should have regard to the following privacy considerations in respect of an initiative or project:

- Existing privacy governance – have regard to the requirements of the PPIP Act, the HRIP Act, the agency's Privacy Management Plan
- Consider the types of information you are collecting, using, sharing: is it personal information[5], health information[6] or other types of non-personal information or a mix of these types of information
- Who holds the personal information[7]
- What is the form of personal information
- How is the personal information accessed
- To what extent is the information deidentified and what are the risks of reidentification
- Are there ways to achieve policy goals or objectives without compromising privacy obligations
- Does the public interest in the project or initiative outweigh the public interest in compliance with privacy laws.

Information-sharing considerations

Agencies should have regard to the following considerations in respect of information-sharing proposals:

- Who will be sharing information – this is important in order to understand if information will also be shared with non-government entities. The PPIP Act does not apply to private sector entities.[8] Agencies should consider whether their contracts with third parties include a requirement for the third party to comply with the PPIP Act and/or HRIP Act.
- What information is to be shared – the information may include a mix of personal information, health information and other information
- The life cycle of the information from collection to retention and security, to use and disclosure, to access and alteration
- What audit mechanisms are in place around monitoring access and sharing under the information sharing arrangement
- Are authorised user agreements required in respect of accessing information under information-sharing arrangements
- Do exemptions from privacy laws (including use and disclosure provisions) apply[9]
- Consider the options available for information-sharing: memorandum of understanding, contract or protocol; regulation, privacy code or public interest direction; creation of a specific exemption in legislation.

Before consideration can be given to developing a privacy code of practice or public interest direction we suggest that you:

[3] Section 35E, PPIP Act.
[4] Section 41(3), PPIP Act.
[5] Defined in section 4 of the PPIP Act.
[6] Defined in section 6 of the HRIP Act.
[7] Section 4(4) of the PPIP Act deals with the circumstances in which a public sector agency holds personal information.
[8] Although the HRIP Act applies to private sector persons.
[9] Division 3 of Part 2, PPIP Act.

- Map the flow of information to be shared, as this will assist you to determine whether an exemption is required to enable the disclosure
- Prepare a Privacy Impact Assessment (PIA) to ensure that any privacy impacts or risks are identified, addressed or mitigated prior to information sharing arrangements being commenced. This process will also assist in the development of a business case to support a proposed privacy code of practice or public interest direction.

Privacy Impact Assessment

Where a project or initiative has privacy, data security or information governance dimensions, agencies and entities are encouraged to undertake a PIA.

It is preferable that agencies and entities do so before consulting the Privacy Commissioner or the IPC on a project or initiative.

The IPC has published a Guide to Privacy Impact Assessments in NSW.

A PIA assists public and private sector organisations identify and minimise the privacy risks of changes to services or policies and new projects. A PIA is an important 'privacy by design' process that assists compliance with privacy obligations and delivers benefits to organisations.

A PIA should involve an assessment of:

- positive and adverse privacy impacts, including community reaction
- compliance with privacy and other relevant legislation
- controls that mitigate any identified risks.

Agencies are encouraged to share the PIA with the Privacy Commissioner and the IPC to make clear what privacy risks have been identified and what steps have been taken to mitigate the risks.

Privacy by Design

'Privacy by design' is a process for embedding good privacy practices into the design specifications of technologies, business practices and physical infrastructures. This means building privacy into the design specifications and architecture of new systems and processes.

Privacy by design is built around seven foundational principles:

- *Proactive not reactive, preventative not remedial*: meaning anticipating the risks and preventing privacy invasive events before they occur.
- *Privacy as a default setting*: ensuring that personal information is automatically protected in any given initiative or project as the default.
- *Privacy embedded into design*: privacy measures are embedded into the design of initiatives and projects so that privacy becomes an essential component of the core functionality being delivered. Privacy should be integral to the system, without diminishing functionality.
- *Full functionality*: positive-sum not zero-sum: legitimate interests and objectives should be accommodated in a positive-sum (win-win) manner, not through a zero-sum (either/or) approach, where unnecessary trade-offs are made.
- *End-to-end security – full lifecycle protection*: this ensures that all information is securely collected, used, retained, and then securely destroyed at the end of the process, in a timely fashion.
- *Visibility and transparency – keep it open*: the individual should be made fully aware of the personal information being collected, and for what purposes. All the component parts and operations should be visible and transparent to users and providers.
- *Respect for user privacy – keep it user centric*: the interests of the individual are paramount and safeguarded through privacy defaults, appropriate notice, and empowering user-friendly options.

Consulting the Privacy Commissioner and the IPC – Best Practice

What agencies should consult the Privacy Commissioner about

Agencies should consult the Privacy Commissioner if:

- The initiative or project is likely to have privacy, data security or information governance aspects
- There is an information-sharing proposal in respect of personal or health information
- The agency would like a public interest direction or code of practice
- The agency would like advice about education supports or resources that are relevant to their project or initiative.

Agencies should take certain steps before consulting the Privacy Commissioner and the IPC

Before consulting the Privacy Commissioner and the IPC on your initiative or project, you should:

- Have regard to the privacy considerations of an initiative or project described above
- Determine if you need to undertake a PIA and if so consider doing the PIA before approaching the IPC
- Ensure you take a 'privacy by design' approach to development of your initiative or project
- Review relevant guidance on the IPC's 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

The IPC can give general advice on rights and compliance under privacy and information access legislation, but cannot give legal advice. You should seek your own legal advice as required.