information and privacy commission new south wales

Fact Sheet **October 2020**

Digital Projects

This fact sheet provides guidance to agencies on the information access and privacy issues they should consider where designing and implementing a digital project.

This information is intended to be applied by agencies during the development of digital projects of any size or scope but will be of particular importance for those agencies intending to seek funding under the NSW Government's Digital Restart Fund.

It is essential that agencies consider their obligations under the *Government Information (Public Access) Act 2009* (GIPA Act), *Privacy and Personal Information Protection Act* (1998) (PPIP Act) and *Health Records and Information Privacy Act 2002* (HRIP Act) when designing and implementing digital projects.

Legislated rights remain inalienable notwithstanding the transition to digital government and outsourcing arrangements that promote enhanced use of technology and data.

GIPA Act

The object of the GIPA Act is to open government information to the public to maintain and advance a system of responsible and representative democratic government.

The GIPA Act places obligations on agencies within NSW to publish and release proactively some types of information that they create and hold. The GIPA Act also provides rights for persons to apply for access to government information.

PPIP Act and HRIP Act

The PPIP Act and HRIP Act govern how personal and health information must be collected, stored, used and disclosed by public sector agencies and, in the case of the HRIP Act, private sector organisations.

The PPIP Act and HRIP Act also provide rights for persons to access and request amendment to their personal information held by a public sector agency.

These rights remain applicable where government uses technology to provide services and inform decisions.

What are digital projects?

Digital projects can encompass a vast range of projects and applications. Essentially a 'digital project' is any project that develops or employs a technological solution to deliver a function or activity of a public sector agency.

This may include, but is not limited to, projects that involve online service delivery platforms, artificial intelligence, automated decision-making, data linkage or analytics, machine learning, smart infrastructure and internet of things devices.

What information access questions should you consider?

Every digital project will, in some way, involve the creation or use of government information. Section 4 of the GIPA Act defines government information as information contained in a record held by an agency.

Under the GIPA Act a record includes any document or other source of information compiled, recorded or stored in written form or by electronic process, or by any other manner or by any other means.[1] This means that in addition to paper or hard copy records, digital records can be the subject of a GIPA application, where that information is held by the agency.

See the IPC Fact Sheet Digital Records and the GIPA Act for further information.

Agencies should consider the following key information access questions when designing and implementing a digital project:

Who holds the information?

Will the information collected or generated through the digital project be held by a NSW public sector agency or will it be held by another entity providing services under contract?

In this regard agencies should note clause 12 of Schedule 4 of the GIPA Act which defines when government information is held by an agency. This provision provides, inter alia, that "information contained in a record held by a private sector entity to which the agency has an immediate right of access" is deemed to be held by the agency.

[1] GIPA Act clause 10 of Schedule 4

Where agencies enter into contractual arrangements with private sector entities for the provision of digital services to the public, they should be mindful of their obligations under section 121 of the GIPA Act.

Section 121 applies where an agency enters into a contract with a private sector entity (the contractor), where the contractor is to provide services to the public on behalf of the agency.

Under section 121(1), contracts to provide services to the public on behalf of an agency must provide for the agency to have an immediate right of access to the following information contained in records held by the contractor:

- information that relates directly to the performance of the services by the contractor
- information collected by the contractor from members of the public to whom it provides, or offers to provide, the services
- information received by the contractor from the agency to enable it to provide the services.

It is the agency's responsibility to ensure the contract provides for the immediate right of access.

Additionally agencies should act in accordance with the responsibilities they have to inform the public about the information they hold and describe the ways in which functions, in particular decision making functions are publicly available.[2] Accordingly even if some aspects of decision making or functions of an agency are undertaken by a third party, agencies will still have a duty to describe that function. This may impact contractual arrangements particularly those that seek to limit access to information by inclusion of commercial in confidence provisions.

For further information on your agencies obligations under section 121 see the IPC Fact Sheet: Guide to section 121 of the GIPA Act for agencies.

In what format is the information held and under what arrangement?

The GIPA Act is technology neutral and applies to 'information' held by public sector agencies regardless of the format in which that information is created or held. Accordingly, data sets, algorithms and test suites may be subject to GIPA Act access requirements.

Additionally, the GIPA Act recognises that access to information can be provided by creating a new record and/or deleting information from a record to ensure that information is available.

How is access to be provided?

Agencies should consider what steps might be required to provide access to information in a variety of circumstances, and what types of information can be proactively released. While this may differ depending on the context of your project and the technology being utilised, it might include:

- access to metadata
- provision of machine-readable data sets
- access to audio visual material
- redaction of identifying or other personal information
- explaining how a system reached a decision
- access to software specifications or datasets used for machine enhanced decision-making.

Importantly access extends to ensure that citizens can understand the information provided so that the object of the GIPA Act and the public interest in disclosure of information are upheld and promoted. Citizens are entitled to understand how decisions that affect them or are likely to affect their rights privileges, benefits or obligations and penalties are made by government. Agencies have a responsibility under the GIPA Act to ensure these rights are preserved.[3]

What privacy questions should you consider?

Digital projects that involve the collection, use or disclosure of personal or health information must comply with the requirements of the PPIP Act and/or HRIP Act.

The specific privacy issues that need to be considered will vary depending on the type and scope of the project. However, agencies should consider the following high-level privacy questions when designing and implementing a digital project:

Will the project involve the use of personal or health information?

'Personal information' is defined in the PPIP Act as any information or opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.[4]

A digital project may involve the use of personal information even where the data sets being used are not considered to be personal or health information.

This arises where the identity of an individual may become 'reasonably ascertainable' by combining data sets or from insights derived from analytics performed on the data.

See the IPC Fact Sheet: Reasonably ascertainable identity for further information.

Agencies should also be mindful of the risks of re-identification that can arise from projects that link de-identified or aggregated data sets.

See the IPC Fact Sheet: De-identification of personal information for further information.

[2] GIPA Act, section 20.
[3] GIPA Act section 23
[4] PPIP Act, section 4.

Will the project involve sharing personal or health information with another agency or organisation?

The *Data Sharing (Government Sector) Act 2015* authorises NSW government sector agencies to share data with other NSW government sector agencies for specific purposes as set out in the legislation. However, any sharing that occurs under the Data Sharing Act must be done in accordance with the PPIP Act and HRIP Act.

A public sector agency can only share (disclose) personal information if one of the exceptions under section 18 of the PPIP Act (or another exemption under the Act) applies:

- the disclosure is directly related to the purpose for which the information was originally collected, and the agency has no reason to believe the individual whose information is to be shared would object to it being shared
- the individual is likely to be aware or has been made aware that information of that kind is usually shared
- the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual or another person.

Note that different exceptions apply in relation to health information under the HRIP Act.

See the IPC Guide: Data sharing and privacy for further information.

What privacy governance arrangements are in place for the project?

When designing digital projects your agency needs to ensure appropriate privacy governance arrangements are put in place. This should include:

- whether the project will involve the collection, use or disclosure of personal or health information
- who will have access to the information and for what purpose?
- how long will the information be held?
- secure storage and disposal arrangements
- any security or access audit arrangements
- procedures for responding to a data breach event.

Privacy by Design

Taking a privacy by design approach can ensure that all appropriate privacy considerations have been considered in the design of your digital project.

This means that you consider privacy at all stages of the project, from conception through to the development and implementation phases. By developing an organisation-wide awareness of privacy, a privacy by design approach shifts the focus to preventing privacy-related issues, rather than simply complying with privacy laws.

Privacy Impact Assessments

One way of implementing a privacy by design approach is to undertake a privacy impact assessment (PIA).

A PIA is a systematic assessment of a project which identifies the impact that the project may have on the privacy of individuals and sets out a process or recommendations in addressing this risk.

A PIA enhances the quality of information available to decision makers and demonstrates that a project has been designed with privacy in mind. It should assess whether proposed project accords with legislative requirements and agency policies concerning privacy, data security and information management.

The timing of a PIA is crucial. A PIA should be conducted early enough to genuinely affect project design, yet not too early as to prevent an agency from obtaining the necessary information about the project to adequately assess any privacy risks.

When should you consult with the IPC?

Consulting with the IPC can assist agencies to identify and address potential privacy and information access risks during the development of digital projects. Agencies should consider consulting with the IPC at a point in time where the project has been sufficiently scoped to allow for an assessment of potential risks but not so far advanced that changes cannot be made to the project design to mitigate those risks.

Agencies should consult with the IPC on a digital project when it:

- involves personal or health information about individuals, including where that information will be de-identified or aggregated
- involves information about government functions, particularly projects which fully or partially automate decision-making
- impacts on the rights, entitlements, liabilities and conditions of individuals
- impacts on the ability of an individual to access information
- involves the sharing of information with another public sector agency or with a private sector entity
- involves data matching, analytics or linkage, particularly where the project involves personal or health information
- creates new information, for example, where a system uses analytics to derive new insights from government information.

See the IPC Fact Sheet: Role of the Privacy Commissioner: Consulting the IPC on projects and initiatives for further information on consulting the IPC.

Further resources

The following IPC resources may be of assistance to agencies when designing and implementing digital projects:

Information access resources

- Guideline 6: Agency Information Guides
- Guideline 7: Open data

- IPC Fact Sheet: Managing access to audio-visual information under the GIPA Act
- IPC Fact Sheet: Automated decision-making, digital government and preserving information access rights

Privacy resources

- IPC Fact Sheet: Consent and bundled consent

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

NOTE: The information in this fact sheet is to be used as a guide only. Legal advice should be sought in relation to individual circumstances.