information and privacy commission
new south wales

Digital Restart Fund: assessing information access and privacy impacts

May 2021

Contents

Overview

This regulatory advice is issued pursuant to section 17(b) of the *Government Information (Public Access) Act 2009* (GIPA Act) and section 36(2)(g) of the *Privacy and Personal Information Protection Act 1998* (PPIP Act). The advice represents general regulatory advice to complement the more specific statutory advice provided by Commissioners under section 10 of the *Digital Restart Fund Act 2020* (DRF Act).

This advice provided to NSW government agencies sets out some of the commonly identified risks to information access and privacy rights across projects seeking funding from the Digital Restart Fund (DRF) and suggests mitigation strategies. In developing this advice, the Information and Privacy Commission (IPC) also consulted with Cyber Security NSW, whose advice is reflected in the sections regarding cyber security.

The IPC is committed to sharing its expertise and this general advice will be reviewed and refined as our expertise evolves in response to technological advancement.

Digital Restart Fund: assessing information access and privacy impacts

The NSW government has allocated $1.6 billion over three years to invest in digital transformation projects through the DRF. Under section 10 of the DRF Act, before approving funding for a project, the Minister must obtain and have regard to advice from the Information Commissioner and the Privacy Commissioner. This advice is required at each stage of a project, prior to funding being released.

Since September 2020, IPC has been assessing and applying a risk rating to all projects seeking funding from the DRF. With the widespread increase in digital service delivery by government, the IPC has reviewed diverse digital projects from a wide range of agencies involving both government and non-government providers. When engaging non-government providers contractual requirements should promote the preservation of rights and recognise that government remains accountable to citizens.

This advice sets out some of the commonly identified risks to information access and privacy rights across different types of digital projects and suggests mitigation strategies.

The IPC's approach to provision of advice provides practical guidance to ensure that legal rights are preserved. Legal Design is encouraged as a methodology that reflects a contemporary approach to the development of technology to ensure the preservation of legal rights[1].

Legal Design methodology consists of five main steps:

1. Understanding
2. Synthesis
3. Brainstorming and prototyping
4. Testing
5. Refinement.

Accordingly, the mitigation strategies recommended by Commissioners are calibrated to the relevant legislative requirement, the technology and fundamentally the citizen to achieve an outcome that reflects human centred design. The Legal Design approach is iterative, and the advice provided by the IPC assists agencies in understanding the potential impact on rights and synthesising potential technical solutions.

Commissioners recognise that further prototyping, testing and refinement may be required to achieve a rights preserving outcome. This advice seeks to raise the level of understanding of the impact of technology on rights and empower agencies to understand and implement rights preserving features from the outset. More broadly the advice contributes to just and legal outcomes by promoting accessibility and digital inclusion.

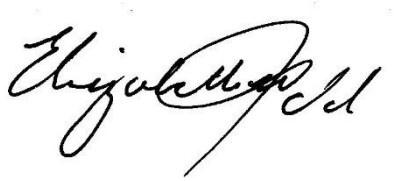
When government uses technology to inform its decision-making the integrity of the technology is paramount. In this context integrity requires evidence to explain both the goals of the system and prove that the system meets those goals. That evidence or explanation must be accessible in a low cost and low complexity form.

This advice does not contain an exhaustive list of the types of DRF projects for which funding may be sought, nor does it identify all potential information access and privacy impacts. Every digital project will, in some way, involve the creation or use of government information. A significant proportion of DRF projects will also involve the collection and use of personal information.

[1] Legal Design methodology underpins and is consistent with the Privacy by Design principles explained in the IPC's Fact Sheet - Privacy by Design.

Agencies are reminded that they will need to continue to comply with their obligations under the GIPA Act, PPIP Act and the *Health Records and Information Privacy Act 2002* (HRIP Act) even as the nature of their service delivery evolves and makes increasing use of digital technology.

This advice aims to distil the knowledge acquired by the IPC in assessing DRF projects, identifying the risks they present to information access and privacy rights and recommending risk mitigation strategies. The advice is designed to share that knowledge with agencies in an accessible manner to build the capacity of NSW public sector agencies and ensure that information access and privacy rights are preserved.



Elizabeth Tydd
IPC CEO, Information Commissioner
NSW Open Data Advocate

Samantha Gavel
Privacy Commissioner

May 2021

1. Portals: centralised information and transaction platforms

The IPC has reviewed projects involving the integration of government transactions, information and services into a single portal for citizens to access. A notable example of this is the increasing number of transactions with various government agencies available via Service NSW's digital platforms.

Impacts

Bringing information and transactions from different parts of government into a central location can enhance accessibility for citizens by streamlining application processes and grouping together relevant information. However, given that these projects involve the collation of information from multiple agencies, as well as the sharing of information between agencies and potentially third-party vendors, they can also create risks to information access and agencies' compliance with the GIPA Act. As citizens often need to provide their personal information to access digital portals, privacy risks also arise in relation to how this personal information is handled.

The following section sets out in more detail common risks to information access and privacy rights associated with centralised portals, with mitigation strategies also outlined.

Information access

Risks	*Mitigation strategies*
A lack of clarity around who holds the information and how it will be used In the context of a portal that brings together information from multiple sources, agencies will need to consider who holds information (for the purposes of the GIPA Act), in what format this information is held and what steps might be required to provide access to information in a variety of circumstances, as well as what types of information can be proactively released.	• Maintaining up to date agency information guides (AIG)[2]. • Agencies should ensure that they publish information on their websites about their functions, including decision-making functions, and identify the types of information they hold[3]. • Ensuring transparency by publishing policies relating to the operation of the portal and how citizens' information may be shared[4]. • Agencies should provide certifications at an appropriately senior level of their information holdings and the results of searches they have conducted in response to an access request. • Where agencies are able to download other agencies' information from a portal, processes should be introduced to consider auditing contact points to enable agencies to fulfill their responsibilities to transfer GIPA applications in whole or in part[5].

[2] Section 20, GIPA Act.

[3] Section 20(1)(b) and (d), GIPA Act.

[4] Section 23, GIPA Act.

[5] Part 4, Division 2, GIPA Act.

Inability to access information held by third parties Third party vendors/contractors may include providers of new platforms, software and/or cloud storage solutions. These entities may hold government information but are not covered by the GIPA Act.	• Ensuring that procurement contracts with third party providers require an immediate right of access for citizens to prescribed information[6]. • Implementing an audit capability and monitoring process to enable any systems managed and operated by third parties that contain government information to be securely managed and scrutinised.
Digital exclusion and accessibility Some citizens may lack the digital literacy or necessary equipment to access digital-only services.	• Retention of non-digital options for citizens who cannot or choose not to access digital services. • Chatbots can provide a means of promoting low cost accessibility in digital platforms.

Privacy

Risks	*Mitigation strategies*
A failure to comply with the Information Protection Principles (IPPs) and/or the Health Privacy Principles (HPPs) Portals that bring together services and transactions are likely to collect citizens' personal information, often sensitive health and financial data. Where privacy impacts are not considered in the early stages of a project, agencies risk breaching the IPPs and/or HPPs.	• Agencies are strongly encouraged to undertake a Privacy Impact Assessment (PIA) after initial discovery and before prototypes are developed. A PIA will map information flows, assess the project against NSW privacy laws and help to identify and mitigate privacy risks before a project proceeds.
Unauthorised access, use or disclosure of personal information A common feature of centralised portals is the sharing of citizens' personal information across multiple agencies, often through the availability of prefilled forms. It is important to ensure that wherever personal information is shared, that citizens are aware of this and have given their consent, and that access to personal information is minimised as far as possible.	• Ensuring that a privacy collection notice is displayed to portal users, to ensure that they are aware of how any personal information they provide will be used, shared, stored and disposed of. • Separately, consent should be sought in relation to the use of their personal information. Consent should be informed and current, and the use of bundled consents should be avoided. The IPC has developed guidance on issues relating to consent, which is available on our website. • Providing clear information to citizens on who to contact to access and/or correct their personal information.

[6] Section 121, GIPA Act.

	• Access controls should be in place to limit the agency staff who have access to personal information, while access audit logs should also be maintained to ensure accountability and transparency.
Risk of data breaches Bringing together large amounts of information and transactions can create an attractive target for malicious actors.	• Ensuring that a data breach policy is in place, with clearly articulated responsibilities. • Training on privacy and data security for all staff handling personal information. • Cyber security risk assessments should be undertaken in the early stages of the project - Identify additional controls to attain appropriate levels of maturity for mandatory requirements in the NSW Cyber Security Policy - Include appropriate funding for these controls and cyber security maturity levels - Apply secure-by-design principles.
Lack of compliance with privacy laws by third party vendors Third party vendors/contractors may include providers of new platforms, software and/or cloud storage solutions. These entities may have access to citizens' personal information as part of their involvement with the project but are not covered by NSW privacy laws (and may not be subject to the Commonwealth *Privacy Act 1998*).	• Ensuring contracts with third parties include provisions requiring compliance with privacy laws.

2. Drones and smart technology

Several government digital solutions now involve the use of technology to capture information and data, which can then be analysed and used to develop government policy. Notable examples of this include the integration of technology into the built environment under the Smart Places strategy and the use of drones for purposes including environmental conservation.

Impacts

The IPC has observed the following common features of projects involving the use of these types of technology:

- the deployment of solutions developed by third party vendors
- the collection of large amounts of data (including personal information)
- the use of third-party cloud storage solutions
- the use of machine learning to analyse large volumes of data and to extract insights to inform decision-making.

Each of these features gives rise to a range of information access and privacy risks, which are outlined below, along with mitigation strategies.

Information access

Risks	*Mitigation strategies*
Inability to review or explain decisions relying on AI models	• Incorporating mechanisms to preserve 'reviewability' within the design of a project. This may require ensuring the factors that inform a decision-making process are capable of being provided and that procurement contracts specify those requirements. Any use of AI or machine learning should comply with the NSW AI Strategy, Ethics Policy and User Guide, which incorporate considerations of agency obligations under privacy and information access laws. • *Black-box tinkering* may be used in the development of an algorithm to test scenarios and reveal the blueprint of the decision-making process. • The use of algorithms should be accompanied by ongoing monitoring and evaluation to ensure models remain accurate. • In respect of the creation of any new records, for example through the collection of new data or through analysis of data using AI or machine learning systems, agencies should consider how these records will be stored and accessed and ensure that their AIG is up to date[7]. • Agencies should also ensure that policies regarding their use of smart technology, drones and any AI systems are publicly available[8].
Inability to access information held by third parties Third party vendors/contractors may provide technological solutions to government and may hold government information.	• Ensuring that procurement contracts with third party providers require an immediate right of access for citizens to prescribed information[9]. • Contracts with third party providers should specify the information that would be required, e.g. the inputs to an algorithm, the source data or test suites together with inputs to test the reliability of any machine enhanced decision-making process.

[7] Section 20, GIPA Act.

[8] Section 23, GIPA Act.

[9] Section 121, GIPA Act.

A lack of accountability in decision-making and service provision	• Government procurement contracts should ensure that government: retains the right to access input, training and testing data; methodologies and documentation are accessible by government. • Government procurement contracts ensure the vendor: remains accountable to government for system configuration, assessment and compliance.[10]

Privacy

Risks	*Mitigation strategies*
Incidental collection of personal information Embedding smart technology into cities' infrastructure and the use of drones, for example, may lead to the incidental collection of citizens' personal information.	• Any personal information collected must be handled in accordance with the PPIP Act. • Agencies are strongly encouraged to undertake a PIA before using new technology to collect data. A PIA will map information flows, assess the project against NSW privacy laws and help to identify and mitigate privacy risks before a project proceeds. • Agencies should consider developing appropriate policy and procedures, which include requirements for privacy compliance, to govern the use of any new technology in their operations. Documents including the NSW AI Strategy, the NSW IoT Policy, NSW Cloud Policy and the Smart Places Strategy may be relevant in this regard.
Risk of unauthorised access to personal information	• Access controls should be in place to limit the number of staff who have access to any personal information that is collected, with access audit logs also maintained to ensure accountability and transparency.
Data breaches The large volumes of data and insights collected by smart technology and drones could make information holdings a target for malicious actors.	• Ensuring that a data breach policy is in place, with clearly articulated responsibilities. • Training on privacy and data security for all staff handling personal information. • Cyber security risk assessments should be undertaken in the early stages of the project - Identify additional controls to attain appropriate levels of maturity for mandatory requirements in the NSW Cyber Security Policy

[10] AINOW Algorithmic Accountability Policy Toolkit – Toolkit 01, October 2018.

	- Include appropriate funding for these controls and cyber security maturity levels - Apply secure-by-design principles.
Lack of compliance with privacy laws by third party vendors	• Procurement contracts with third party vendors should include provisions requiring compliance with privacy laws.

3. Single notification services

A number of DRF projects aim to ensure that citizens only need to provide the NSW Government with certain personal information once, in order to notify several agencies of a life event or to access a broad range of services.

Impacts

Single notification services commonly involve the establishment of new registers and/or databases, which multiple entities are then able to access or receive information from. Examples include the Seniors Energy Rebate and the Australian Death Notification Service. Both of these schemes involve the sharing of information between NSW Government agencies as well as with Commonwealth agencies and private sector entities. This type of information sharing gives rise to both information access and privacy risks, some of which are identified below.

Information access

Risks	*Mitigation strategies*
A lack of transparency around what information is held by agencies and who can access it	• Maintaining an up to date AIG[11]. • Agencies publishing on their website information about their functions, including decision-making functions, and identify the types of information held[12]. • Ensuring transparency by publishing policies relating to the operation of the project, including who the information is shared with. This will be particularly relevant where information is shared outside of NSW and with non-government entities[13]. • Ensuring that individuals have easy access to clear processes for handling requests for assistance, inquiries, or complaints.

[11] Section 20, GIPA Act.

[12] Section 20(1)(b) and (d), GIPA Act.

[13] Section 23, GIPA Act.

Inability to access information held by third parties Third party vendors/contractors may include providers of new platforms, software and/or cloud storage solutions. These entities may hold government information but are not covered by the GIPA Act.	• Ensuring that procurement contracts with third party providers require an immediate right of access for citizens to prescribed information[14]. • Implementing an audit capability and monitoring process to enable any systems managed and operated by third parties that contain government information to be securely managed and scrutinised.
Digital exclusion Some citizens may lack the digital literacy or necessary equipment to benefit from digital-only single notification solutions.	• Retention of non-digital options for citizens who cannot or choose not to access digital solutions.

Privacy

Risks	*Mitigation strategies*
A failure to comply with the Information Protection Principles and/or the Health Privacy Principles	• Agencies are strongly encouraged to undertake a PIA after initial discovery and before prototypes are developed. A PIA will map information flows, assess the project against NSW privacy laws and help to identify and mitigate privacy risks before a project proceeds.
Unauthorised access, use or disclosure of personal information With personal information being shared with several entities, agencies will need to take steps to ensure that this information is managed in line with privacy laws and citizens' consent.	• Agencies should ensure that they sufficiently inform individuals about each of the proposed collections, uses and/or disclosures that it intends with the personal information that is collected. • A privacy collection notice should be displayed to all users of single notification solutions, to ensure that they are aware of how any personal information they provide will be used, shared, stored and disposed of. • Separately, consent should be sought in relation to the use of their personal information. Consent should be informed and current, and the use of bundled consents should be avoided. This is especially important as many single notification systems expand over time to include more entities.

[14] Section 121, GIPA Act.

	• Access controls should be in place to limit the agency staff who have access to personal information, with access audit logs also maintained to ensure accountability and transparency.
Risk of data breaches Particularly where new databases or registers containing personal information are established, these can become attractive targets for malicious actors.	• Ensuring that a data breach policy is in place, with clearly articulated responsibilities. • Training on privacy and data security for all staff handling personal information. • Cyber security risk assessments should be undertaken in the early stages of the project - Identify additional controls to attain appropriate levels of maturity for mandatory requirements in the NSW Cyber Security Policy - Include appropriate funding for these controls and cyber security maturity levels - Apply secure-by-design principles.
Lack of compliance with privacy laws by third party vendors Third party vendors/contractors may include providers of new platforms, software and/or cloud storage solutions. These entities may have access to citizens' personal information as part of their involvement with the project but are not covered by NSW privacy laws (and may not be subject to the Commonwealth *Privacy Act 1998*).	• Ensuring contracts with third parties include provisions requiring compliance with privacy laws.

4. Data analytics projects

Increasingly, government agencies are seeking to use data for the purposes of analytics to inform their decision-making and service delivery. These projects can involve the use of automation and machine learning systems, linkage of data from multiple agencies (and non-government entities) and the use of third-party analytics solutions. The NSW Spatial Digital Twin project, for example, is bringing together data from different agencies in this way, creating a digital real-world model of NSW cities and communities to facilitate better planning, design and modelling.

The IPC has identified the following common information access and privacy risks in relation to data analytics projects:

Information access

Risk	*Mitigation strategies*
A lack of public access to new information created through a data analytics project It will be important to identify who holds any new information generated – what agency or other entity; in what format the information is held and under what arrangement (including contractual arrangements with third parties); and how access is to be provided.	• Maintaining an up to date AIG[15]. • Consider all opportunities to provide subsets of aggregated data as open data. • Agencies should ensure transparency around how the data they collect and analyse will influence its decision-making[16]. • Any use of machine learning or AI systems should comply with the NSW AI Strategy, Ethics Policy and User Guide, which incorporate considerations of agency obligations under privacy and information access laws.
Inability to access information held by third parties	• Ensuring that procurement contracts with third party providers require an immediate right of access for citizens to prescribed information[17].
A lack of accountability in decision-making and service provision	• Government procurement contracts should ensure that government: retains the right to access input, training and testing data; methodologies and documentation are accessible by government. • Government procurement contracts ensure the vendor: remains accountable to government for system configuration, assessment and compliance.[18]

Privacy

Risks	*Mitigation strategies*
Data analysis or data linkage breaches the IPPs or HPPs	• Undertake a comprehensive PIA in the early stages of the project, to identify the privacy impacts of linking, analysing or making data publicly available.

[15] Section 20, GIPA Act.

[16] Section 23, GIPA Act.

[17] Section 121, GIPA Act.

[18] AINOW Algorithmic Accountability Policy Toolkit – Toolkit 01, October 2018.

	• Undertaking a PIA will help to ensure compliance with privacy laws and to embed adequate privacy and security governance arrangements in the design of any analytics project and associated information sharing.
Unauthorised use or disclosure of personal information	• Projects using personal information for data analytics and/or linkage will need to ensure adherence with privacy laws, notably in relation to consent, use and disclosure of personal information. • Where deidentified data is being linked, agencies will need to consider and put in place strategies to mitigate the risk of reidentification. • Access controls should be in place, to limit the number of staff who have access to any personal information that is collected or used, with access audit logs also maintained to ensure accountability and transparency.
Data breaches Bringing together data from different sources could create a target for malicious actors.	• Ensuring that a data breach policy is in place, with clearly articulated responsibilities. • Training on privacy and data security for all staff handling personal information. • Cyber security risk assessments should be undertaken in the early stages of the project - Identify additional controls to attain appropriate levels of maturity for mandatory requirements in the NSW Cyber Security Policy - Include appropriate funding for these controls and cyber security maturity levels - Apply secure-by-design principles.

5. Cyber security projects

Part of the DRF has been set aside for projects aimed at uplifting cyber security maturity. Cyber Security NSW plays a key role in reviewing the business cases for these projects, which are also reviewed by the IPC.

Most of the cyber security DRF projects that the IPC has reviewed aim to uplift agencies' maturity against the NSW Government's Cyber Security Policy and the Australian Cyber Security Centre's Essential Eight. While the Essential Eight focus on cyber security maturity, they also provide controls that preserve information access and privacy rights. For example, the restriction of administration privileges, access audit logs; multifactor authentication and daily backups will contribute to:

- improved capacity to ensure government information, including citizens' personal information and government information broadly, is held appropriately and is accessible when requested

- improved protection of personal information under the PPIP Act and health information under the HRIP Act and preserve the strategic asset that is government information. Notably, improved cyber security maturity helps to mitigate the risk of data breaches.

Cyber security uplift projects regularly involve multiple third-party contractors, who may not be subject to the GIPA Act or NSW privacy laws. Strategies to protect and preserve information access and privacy rights under these contractual arrangements include:

- Ensuring that procurement contracts include provisions reflecting the requirements of section 121 of the GIPA Act and requiring compliance with privacy laws
- Incorporating preservation of information access and privacy rights into procurement evaluation
- Establishing a transparent authority framework to identify contractual issues that impact access to information and privacy.

6. Other useful resources

- Guide to Privacy Impact Assessments in NSW: https://www.ipc.nsw.gov.au/guide-privacy-impact-assessments-nsw
- Fact Sheet: Digital projects: https://www.ipc.nsw.gov.au/fact-sheet-digital-projects-agencies
- Fact Sheet: Digital records and the GIPA Act: https://www.ipc.nsw.gov.au/fact-sheet-digital-records-and-gipa-act
- Fact Sheet: Privacy by design: https://www.ipc.nsw.gov.au/fact-sheet-privacy-design
- Guide: Data Sharing and Privacy: https://www.ipc.nsw.gov.au/guide-data-sharing-and-privacy
- NSW Cloud Policy: https://www.digital.nsw.gov.au/policy/cloud-strategy-and-policy/cloud-policy
- NSW Cyber Security Policy: https://www.digital.nsw.gov.au/policy/cyber-security-policy
- NSW Government AI Strategy: https://www.digital.nsw.gov.au/policy/artificial-intelligence-ai/ai-strategy
- NSW Internet of Things Policy: https://www.digital.nsw.gov.au/policy/internet-things-iot
- Smart Infrastructure Policy: https://www.digital.nsw.gov.au/policy/smart-infrastructure-policy

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

Document information

Identifier/Title:	Digital Restart Fund: assessing information access and privacy impacts
Business Unit:	IPC
Author:	LCRA
Approver:	Information Commissioner and Privacy Commissioner
Date of Effect:	May 2021
Next Review Date:	May 2022
EDRMS File Reference:	D21/011328/DJ
Key Words:	Digital Restart Fund, digital projects