information
and privacy
commission
new south wales

# Digital Restart Fund: assessing information access and privacy impacts

**Updated September 2022**

# 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) consulted with the Information and Privacy Advisory Committee (IPAC) NSW, who contributed to the development of the information access and privacy risks and risk mitigation strategies included in this advice. The IPC also consulted with Cyber Security NSW, with that advice 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 $2.1 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, the 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. It also provides information about the IPC's processes for providing advice on projects, including the steps taken to close the feedback loop.

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 legal and 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. It may also assist citizens in understanding the information access and privacy impacts that may arise from digital projects and potential solutions.

In the context of the GIPA Act a responsive and representative democratic government is founded upon the right to access government information, to hold government to account and promote transparency and integrity.

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

When government uses technology to inform its decision-making the trustworthiness of the technology is paramount. In this context trustworthiness 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.

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**

September 2022

# Closing the feedback loop at each project stage

Often with DRF projects, advice will be requested at each stage of the project's delivery. This is because funding is usually approved in tranches, with some projects having discovery, alpha, and beta stages, covering project design to implementation. Given this, the IPC will provide advice at each project stage, with each advice addressing any new information contained in each related business case. In these instances, the IPC aims to reach out to the project's product owner to 'close the loop' on previous feedback provided. Closing the loop will usually consist of contacting the product owner, to seek to understand how the previous IPC advice provided has been considered and implemented by the project/product team. Once this communication has taken place, this feedback loop can help the IPC to formulate the new advice. For example, the IPC may reference the consultation and reiterate or tailor the information access and privacy advice accordingly. This process helps to ensure that the IPC's advice remains relevant, meaningful, and helpful to the Minister and to NSW government agencies, whilst proactively contributing to agencies' compliance with information access and privacy laws.

# Process for agencies considering advice

## Assessing the project and addressing key considerations

When agencies receive IPC advice, project leads can take steps to address the key project privacy and information access considerations in a number of different ways. Project leads should undertake the following:

- Undertake wide consultation across their organisation, including legal experts, policy owners, digital and technology teams and data architecture experts, as well as program manager and delivery professionals. Internal resources are the best first starting point as they are likely to have the knowledge and expertise to support project owners in providing additional information through which to address recommendations arising from the IPC's advice. For example, internal legal and policy teams are likely to direct project owners to internal resources such as pre-existing Agency Information Guides, or they may have experience in engaging professionals required to undertake a Privacy Impact Assessment (PIA).

- Assess whether the project being proposed in its existing form is likely to adhere to the information access and privacy laws and principles that are flagged in the IPC's advice, following the engagement of subject matter experts. Familiarity with the principles of human centred design and privacy by design, as well as a broad understanding of NSW technology/ethics/cyber policies will support project leads in remaining alert to any critical project risks identified.

- Ensure that the project is responsive to the information access and privacy guidance and recommendations. This may require reconsideration of technical and policy issues and adjustments to preserve these rights. Likewise practical solutions may need to be implemented to ensure ongoing compliance.

- During the design phase of the project, agencies should also take additional precautions to ensure that better practice principles are adopted. Undertaking user and product testing to ensure that the project being delivered meets appropriate digital service standards. Following the design and delivery phase of the project, project leads should also ensure sustainable and ongoing monitoring of digital systems. The establishment of consistent review and audit cycles will ensure that digital projects remain compliant with NSW information and privacy legislation.

# 1. Portals, websites, and hubs

The IPC has reviewed projects involving the integration of government transactions, information, and services into single online platforms, in the form of portals, websites or hubs for citizens to access. These can take the form of transaction platforms, centralised information portals or even federated access models. A notable example of this is the increasing number of transactions with various government agencies (with the potential to extend this to Commonwealth agencies and other jurisdictions) available via Service NSW's digital platforms. Likewise, government sectors/agencies are also establishing portals for storage and access to information by separate agencies with limited or no public access.

## 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**<br>In the context of a portal or website 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. | • Consider what data is being collected and what data will be generated, as well as how often that data is refreshed or otherwise updated. This will present different risks if third party providers are engaged under contract.<br>• Maintaining up to date agency information guides (AIG)[2].<br>• 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].<br>• Ensuring transparency by publishing policies relating to the operation of the portal and how citizens' information may be shared[4].<br>• 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. |

[2] Section 20, GIPA Act.

[3] Section 20, GIPA Act.

d), GIPA Act.

[4] Section 23, GIPA Act.

| *Risks* | *Mitigation strategies* |
|---|---|
| | - Agencies can transfer parts of an access application to another agency that holds the information.[5]<br>- 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[6].<br>- Agencies should consider using technical options that facilitate ready access to information e.g. by creating a new record or by redacting information to facilitate access.[7] |
| **Inability to access information held by third parties**<br>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, including provisions relating to retention of data rights, facilitating access to audit logs and receiving notice from the supplier of any adverse incidents including system failures[8].<br>- An agency is to keep a register of government contracts (its government contracts register) that records information about each government contract to which the agency is a party that has (or is likely to have) a value of $150,000 (including GST) or more (class 1 contracts)[9].<br>- 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. |

[5] Section 44(2), GIPA Act

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

[7] GIPA Act section 74 and 75

[8] Section 121, GIPA Act.

[9] Section 27, GIPA Act.

| *Risks* | *Mitigation strategies* |
|---|---|
| **Digital exclusion, accessibility and explainability**<br>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, with opt-in functionality to support citizen choice.<br>• Consideration at design stage as to how digital products can be made as accessible as possible, e.g. chatbots can provide a means of promoting low cost accessibility in digital platforms.<br>• When information is drawn together from different inputs to produce a result that informs decision making agencies should ensure that an explanation of inputs and treatment is preserved and available.<br>• Ensure that the system is accessible and functional across a range of different browsers, operating systems and devices, including computers and mobile devices |

## Privacy

| *Risks* | *Mitigation strategies* |
|---|---|
| **A failure to comply with the Information Protection Principles (IPPs) and/or the Health Privacy Principles (HPPs)**<br>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. A PIA should consider the potential harms and impacts to an individual/s and identify protections that can be built into the project adopting privacy by design. |
| **Unauthorised access, use or disclosure of personal information**<br>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.<br>• Separately, consent should be sought in relation to the use of their personal information, should this be necessary, eg because a new use or disclosure is involved. 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. |

| *Risks* | *Mitigation strategies* |
|---|---|
| | • Providing clear information to citizens on who to contact to access and/or correct their personal information.<br>• Access controls should be in place to limit the agency staff who have access to, and their use and disclosure of, personal information, while access audit logs should also be maintained to ensure accountability and transparency.<br>• Agencies should also consider industry better practice, such as the use of multi-factor authentication systems where feasible, in order to enhance system security. |
| **Risk of data breaches**<br>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.<br>• Training on privacy and data security for all staff handling personal information, including an understanding of the various types of threat actors that are likely to exist, and how to design systems in a way that minimises risk.<br>• Ensure that adequate consultation takes place with relevant Cyber Security stakeholders, and this should include alignment with the NSW Cyber Security Strategy.<br>• Cyber security risk assessments should be undertaken in the early stages of the project:<br>○ Identify additional controls to attain appropriate levels of maturity for mandatory requirements in the NSW Cyber Security Policy<br>○ Include appropriate funding for these controls and cyber security maturity levels<br>○ Apply secure-by-design principles.<br>• Ensure that procurement contracts include appropriate clauses to meet Cyber Security requirements.<br>• Ensure a regular audit and assurance program is in place and appropriately funded. |
| **Lack of compliance with privacy laws by third party vendors**<br>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 | • Ensuring contracts with third parties include provisions requiring compliance with privacy laws.<br>• Ensure a regular audit and assurance program is in place and appropriately funded, either by the vendor/contractor or by the purchasing agency. |

| *Risks* | *Mitigation strategies* |
|---|---|
| may not be subject to the Commonwealth *Privacy Act 1998*). | |
| **Inability of affected citizens to access help, obtain resolution of complaints or obtain any remediation or recompense**<br>The involvement of multiple agencies can lead to confusion or diffusion of accountability etc from a citizen perspective | • Ensure that help, complaint handling and remediation functions are thought through from a citizen perspective so that they are as easy, simple and cheap to access as is the case with individual agencies, including but not limited to 'no wrong door' arrangements or a single point of contact for affected citizens. |

## 2. Smart technology, machine learning, and AI

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.
- The use of smart technology and camera monitoring systems.

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.<br>• *Black-box tinkering* may be used in the development of an algorithm to test scenarios and reveal the blueprint of the decision-making process. |

| *Risks* | *Mitigation strategies* |
|---|---|
| | - When using AI or machine learning, agencies should: 1. Publicly state when and how the machine enhanced technology is being used[10] 2. proactively publish a general explanation of the workings of the technology employed, and 3. provide a specific explanation to citizens affected on request. 4. Decision making should also be explainable in instances where the system continues to learn from new and existing inputs.<br>- The use of algorithms should be accompanied by ongoing monitoring and evaluation to maintain transparency in decision-making and ensure the technology operates as intended. This will help to ensure models remain accurate, and free of differential impact, including any departure from the stated objective e.g. algorithmic bias, including bias that might perpetuate discrimination or injustice.<br>- Conducting a rights impact assessment will ensure that legal and ethical risks are identified.<br>- 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[11].<br>- Agencies should also ensure that policies regarding their use of smart technology, drones and any AI systems are publicly available[12]. |
| **Inability to access information held by third parties**<br>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[13].<br>- An agency is to keep a register of government contracts (its government contracts register) that records information about each government contract to which the agency is a party that has (or is likely to have) a value of $150,000 (including GST) or more (class 1 contracts)[14].<br>- Contracts with third party providers should specify the information that would be required, e.g. the inputs to an algorithm, the source data or |

[10] GIPA Act section 20(1)(b)

[11] Section 20, GIPA Act.

[12] Section 23, GIPA Act.

[13] Section 121, GIPA Act.

[14] Section 27, GIPA Act.

| *Risks* | *Mitigation strategies* |
|---|---|
| | test suites together with inputs to test the reliability of any machine enhanced decision-making process.<br>• Prior to entering into contracts with third party providers agency purchasers should consider intellectual property of the algorithm and request information regarding provenance and specify if the algorithm in use is available from an open source. |
| **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.<br>• Government procurement contracts ensure the vendor: remains accountable to government for system configuration, assessment and compliance.[15]<br>• Any machine enhanced decision-making technology or input to service delivery by government should ensure access to information to serve a pro integrity purpose that supports a participatory democracy.[16] |
| **Technological ‘Psyops’/Manipulation:**<br>The use of techniques such as AI, targeted digital advertising, and behavioural ‘nudging’ to alter citizens beliefs, desires, or emotions. | • Nudge operations are risk factors to autonomy. Maintaining up to date agency information guides (AIG)[17] can help to mitigate this risk.<br>• 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[18].<br>• Ensuring transparency by publishing policies relating to the operation of the AI and how citizens’ information may be shared[19]. |

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

[16] Section 3 GIPA Act

[17] Section 20, GIPA Act.

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

[19] Section 23, GIPA Act.

## Privacy

| *Risks* | *Mitigation strategies* |
|---|---|
| **Inaccurate or inappropriate decision-making**<br>There is a risk that AI driven decision-making could lead to outcomes in which a lack of human oversight leads to adverse outcomes. | • Ensuring that the principles of human centred design are upheld and humans are kept within the loop of the decision- making process in any circumstances where personal information is used that are likely to have a non-trivial impact on the citizen. |
| **Incidental collection of personal information**<br>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.<br>• 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. A PIA should consider the potential harms and impacts to an individual/s and identify protections that can be built into the project adopting privacy by design.<br>• 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**<br>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.<br>• Training on privacy and data security for all staff handling personal information.<br>• Ensure that adequate consultation takes place with relevant Cyber Security stakeholders, and this should include alignment with the NSW Cyber Security Strategy.<br>• Cyber security risk assessments should be undertaken in the early stages of the project:<br>○ Identify additional controls to attain appropriate levels of maturity for mandatory requirements in the NSW Cyber Security Policy |

| *Risks* | *Mitigation strategies* |
|---|---|
| | ○ Include appropriate funding for these controls and cyber security maturity levels<br>○ Apply secure-by-design principles.<br>• Ensure that procurement contracts include appropriate clauses to meet Cyber Security requirements. |
| **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, who can access it and how[20]** | • Maintaining an up to date AIG[21].<br>• Agencies publishing on their website information about their functions, including decision-making functions, and identify the types of information held[22].<br>• 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[23]. |

[20] Section 20(1)(c) – (g)

[21] Section 20, GIPA Act.

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

[23] Section 23, GIPA Act.

| *Risks* | *Mitigation strategies* |
|---|---|
| | • Ensuring that individuals have easy access to clear processes for handling requests for assistance, inquiries, or complaints. |
| **Inability to access information held by third parties**<br>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[24].<br>• An agency is to keep a register of government contracts (its government contracts register) that records information about each government contract to which the agency is a party that has (or is likely to have) a value of $150,000 (including GST) or more (class 1 contracts)[25].<br>• 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**<br>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. A PIA should consider the potential harms and impacts to an individual/s and identify protections that can be built into the project adopting privacy by design. |
| **Unauthorised access, use or disclosure of personal information**<br>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. |

[24] Section 121, GIPA Act.

[25] Section 27, GIPA Act.

| *Risks* | *Mitigation strategies* |
|---|---|
|  | • 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.<br>• 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**<br>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.<br>• Training on privacy and data security for all staff handling personal information.<br>• Ensure that adequate consultation takes place with relevant Cyber Security stakeholders, and this should include alignment with the NSW Cyber Security Strategy.<br>• Cyber security risk assessments should be undertaken in the early stages of the project:<br>○ Identify additional controls to attain appropriate levels of maturity for mandatory requirements in the NSW Cyber Security Policy<br>○ Include appropriate funding for these controls and cyber security maturity levels<br>○ Apply secure-by-design principles.<br>• Ensure that procurement contracts include appropriate clauses to meet Cyber Security requirements. |
| **Lack of compliance with privacy laws by third party vendors**<br>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 | • Ensuring contracts with third parties include provisions requiring compliance with privacy laws. |

| *Risks* | *Mitigation strategies* |
|---|---|
| privacy laws (and may not be subject to the Commonwealth *Privacy Act 1998*). | |
| **Increased risk of error when handling personal information**<br>Single notification services may increase error when handling personal information as inaccurate information becomes shared between multiple agencies across new databases | • Strengthening governance arrangements and data breach/error handling remediation processes via the following:<br>○ Ensuring that a data breach policy is in place, with clearly articulated responsibilities.<br>○ Training on privacy and data security for all staff handling personal information. |
| **Digital exclusion**<br>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. |

# 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**<br>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. | • Any machine enhanced decision-making technology or input to service delivery by government should ensure access to information to serve a pro integrity purpose that supports a participatory democracy.[26]<br>• Consider what data is being collected and what data will be generated. This will present different risks if third party providers are engaged under contract.<br>• Maintaining an up to date AIG[27].<br>• Consider all opportunities to provide subsets of aggregated data as open data. |

[26] Section 3 GIPA Act

[27] Section 20, GIPA Act.

| *Risk* | *Mitigation strategies* |
|---|---|
| | - Agencies should ensure transparency around how the data they collect and analyse will influence its decision-making[28].<br>- 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[29].<br>- Agencies should also include additional terms in the contract for the provision of government services that ensure they are notified of any adverse outcomes/incidents.<br>- An agency is to keep a register of government contracts (its government contracts register) that records information about each government contract to which the agency is a party that has (or is likely to have) a value of $150,000 (including GST) or more (class 1 contracts)[30]. |
| **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.<br>- Government procurement contracts ensure the vendor: remains accountable to government for system configuration, assessment and compliance.[31]<br>- Any machine enhanced decision-making technology or input to service delivery by government should ensure access to information to serve a pro integrity purpose that supports a participatory democracy.[32] |

[28] Section 23, GIPA Act.

[29] Section 121, GIPA Act.

[30] Section 27, GIPA Act.

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

[32] Section 3 GIPA Act

## Privacy

| *Risks* | *Mitigation strategies* |
|---|---|
| **Data analysis or data linkage breaches the IPPs or HPPs** | - 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. A PIA should consider the potential harms and impacts to an individual/s and identify protections that can be built into the project adopting privacy by design. |
| **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.<br>- Where deidentified data is being linked, agencies will need to consider and put in place strategies to mitigate the risk of reidentification.<br>- 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**<br>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.<br>- Training on privacy and data security for all staff handling personal information.<br>- Ensure that adequate consultation takes place with relevant Cyber Security stakeholders and this should include alignment with the NSW Cyber Security Strategy.<br>- Cyber security risk assessments should be undertaken in the early stages of the project:<br>o Identify additional controls to attain appropriate levels of maturity for mandatory requirements in the NSW Cyber Security Policy<br>o Include appropriate funding for these controls and cyber security maturity levels<br>o Apply secure-by-design principles.<br>- Ensure that procurement contracts include appropriate clauses to meet Cyber Security requirements. |

# 5. Digital identity projects

A significant feature of modern digital government involves the consideration of citizen identity and credential tracking technology, with governments increasingly investing resources in scoping, developing and rolling out digital identity projects. These projects have the possibility of featuring various identity related information such as driver licences and birth certificates, as well as credentials such as education and training certificates, or proof of vaccination status, with the intention of sharing these documents in digital form, and storing this information in digital wallets, with many NSW Government agencies taking a leading role in facilitating this transition into the future.

This technology has the ability to create greater convenience for citizens and reduce some existing risks, for example, by reducing the frequency that paper documents are scanned and emailed. Likewise digital identity projects can reduce the risk of lost documentation or even fraud. However, digital identities also give rise to a range of information access and privacy risks, which are outlined below, along with mitigation strategies.

## Information access

| *Risks* | *Mitigation strategies* |
|---|---|
| **Unintended consequences as a result of machine learning or facial verification technology that may perpetuate discrimination or injustice** | • 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.<br>• The use of algorithms should be accompanied by ongoing monitoring and evaluation to ensure models remain accurate and free of any algorithmic bias, including bias that might perpetuate discrimination or injustice<br>• 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[33]. |

[33] Section 20, GIPA Act.

| *Risks* | *Mitigation strategies* |
|---|---|
| | • When using AI or machine learning, agencies should 1. Publicly state when and how the machine enhanced technology is being used[34] 2. proactively publish a general explanation of the workings of the technology employed 3. provide a specific explanation to citizens affected on request, and 4. Decision making should also be explainable in instances where the system continues to learn from new and existing inputs. |
| **Inability to access information held by third parties**<br>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[35].<br>• An agency is to keep a register of government contracts (its government contracts register) that records information about each government contract to which the agency is a party that has (or is likely to have) a value of $150,000 (including GST) or more (class 1 contracts)[36].<br>• 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.<br>• Agencies should also include additional terms in the contract for the provision of government services that ensure they are notified of any adverse outcomes/incidents. |
| **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.<br>• Government procurement contracts ensure the vendor: remains accountable to government for system configuration, assessment and compliance.[37] |

[34] GIPA Act section 20(1)(b)

[35] Section 121, GIPA Act.

[36] Section 27, GIPA Act.

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

| *Risks* | *Mitigation strategies* |
|---|---|
| **Digital exclusion and accessibility**<br>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.<br>• Chatbots can provide a means of promoting low cost accessibility in digital platforms. |
| **Digital surveillance**<br>The development of increasingly sophisticated modes of digital surveillance, including face, gait and other biometrics data. | • Maintaining an up to date AIG[38].<br>• Agencies should ensure transparency around how the data they collect and analyse will influence its decision-making[39].<br>• 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[40].<br>• Ensuring transparency by publishing policies relating to the operation of digital identity projects and how citizens' information may be shared[41.] |

## Privacy

| *Risks* | *Mitigation strategies* |
|---|---|
| **Incidental collection of personal information**<br>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.<br>• 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. A PIA should consider the potential harms and impacts to an individual/s and identify protections that can be built into the project adopting privacy by design.<br>• 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 |

[38] Section 20, GIPA Act.

[39] Section 23, GIPA Act.

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

[41] Section 23, GIPA Act.

| *Risks* | *Mitigation strategies* |
|---|---|
| | Cloud Policy and the Smart Places Strategy may be relevant in this regard.<br>• Where facial recognition technologies are involved, in addition to a PIA, less privacy-intrusive technologies should be considered as a viable alternative where applicable. |
| **Inaccurate or outdated collection or storage of personal information and linked identity services** | • Agencies should take proactive steps to ensure that when capturing, storing or using citizen information that the information is up to date and accurate.<br>• Furthermore, where applicable, agencies should seek to inform customers in cases where their details may no longer be relevant and provide active steps for customers to update their information and choose the nature in which that information is used to update any linked services. |
| **Risk of unauthorised access to personal information**<br>The collection and use of personal information, including metadata, which includes names, location details, addresses, search terms and other sensitive information poses a privacy risk if incorrectly handled. | • 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.<br>• Particular care should be taken when handling personal information of vulnerable cohorts of people, whose data if exposed, could subject them to extreme risk of harm. |
| **Data breaches**<br>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.<br>• Training on privacy and data security for all staff handling personal information.<br>• Ensure that adequate consultation takes place with relevant Cyber Security stakeholders and this should include alignment with the NSW Cyber Security Strategy.<br>• Cyber security risk assessments should be undertaken in the early stages of the project<br>○ Identify additional controls to attain appropriate levels of maturity for mandatory requirements in the NSW Cyber Security Policy<br>○ Include appropriate funding for these controls and cyber security maturity levels<br>○ Apply secure-by-design principles. |

| *Risks* | *Mitigation strategies* |
|---|---|
| | - Ensure that procurement contracts include appropriate clauses to meet Cyber Security requirements. |
| **Lack of compliance with privacy laws by third party vendors** | - Procurement contracts with third party vendors should include provisions requiring compliance with privacy laws. |
| **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. A PIA should consider the potential harms and impacts to an individual/s and identify protections that can be built into the project adopting privacy by design. |
| **Unauthorised access, use or disclosure of personal information**<br>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.<br>- 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.<br>- 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.<br>- 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. |
| **Declining citizen trust** | - Agencies can take steps to ensure that citizen trust remains paramount in the design of digital identity products, ensuring that services are always opt-in and that non-digital options remain available for use.<br>- Additionally, requests for informed consent should be made available at any point that citizen personal information is captured, stored or shared as part of the project, and the option for this consent to be rescinded should |

| *Risks* | *Mitigation strategies* |
|---|---|
| | be available at every stage in the customer journey. |
| **Digital exclusion and accessibility**<br>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, including to request access to their personal information[42]. |
| **Digital surveillance**<br>The development of increasingly sophisticated modes of digital surveillance, including face, gait and other biometrics data. | • Agencies should ensure the collection and use of data, including biometrics data, complies with IPPs and HPPs or authorising legislation[43].<br>• Agencies should take a privacy by design and human centred design approach and consider whether a less privacy intrusive approach is available. |

# 6. 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.

[42] Section 14, PPIP Act

[43] Section 25, PPIP Act

In most instances, improving an agency's cyber security maturity will support and preserve information access and privacy rights, by keeping government information secure. Given this, the IPC's advice on cyber security projects does not routinely apply a risk rating.

# 7. 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
- NSW AI Assurance Framework: https://www.digital.nsw.gov.au/policy/artificial-intelligence/nsw-ai-assurance-framework

*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:** | September 2022 |
| **Next Review Date:** | September 2023 |
| **EDRMS File Reference:** | D22/028060/DJ |
| **Key Words:** | Digital Restart Fund, digital projects |