Summary Impact Analysis Statement

Details

Lead department	Department of Justice and Attorney-General
Name of the proposal	Information Privacy and Other Legislation Amendment Bill 2023
Submission type (*Summary IAS / Consultation IAS / Decision IAS)*	Summary IAS
Title of related legislative or regulatory instrument	Information Privacy and Other Legislation Amendment Bill 2023 – excluding amendments related to the proactive release of Cabinet documents
Date of issue	6 October 2023

Proposal type	Details
Minor and machinery in nature	The following proposals are machinery in nature and do not result in a substantive change to regulatory policy or new impacts on business, government or the community: • the proposal to clarify factors outside those listed in Schedule 4 of the *Right to Information Act 2009* (RTI Act) that may be considered in applying the public interest balancing test, which is technical in nature and a clarification of the existing law; • consequential amendments to the RTI Act, the *Information Privacy Act 2009* (IP Act) and various other Acts as a result of the legislated response described below. Amendments which are consequential on the proposal to create a single right of access to information involve minor and machinery changes, primarily removing duplicate provisions; • Amendments which remove a number of outdated references; • Amendments which make provisions easier to understand and use language which is consistent with modern drafting practice; • removing the mandatory requirements for agencies and Ministers to give an applicant a schedule of relevant documents, and charges estimate notice (CEN) where no charges apply, and clarify that applicants are limited to two CENs and that any narrowing of a second CEN would not require a third CEN to be issued; and • providing that the Information Commissioner's functions under the IP Act are excluded from investigations by the Queensland Ombudsman consistent with exclusion of the Information Commissioner's functions under the RTI Act.
Regulatory proposals where no RIA is required	The proposal to amend section 408E of the Criminal Code, which involves removal of the reference to 'hacking' (to clarify the type of conduct captured by the offence), increasing the maximum penalty of the 'simpliciter' offence from two to three years imprisonment and re-classifying it as a misdemeanour, and amending the definition of

	‘benefit’ to clarify that a benefit need not be pecuniary, relates to general criminal laws. No regulatory impact analysis is required under the Better Regulation Policy. The following proposals are deregulatory (remove regulation), and do not increase costs or regulatory burden on business or the community: • updating the definition of ‘generally available publication’ under the IP Act; • removing the requirement for access and amendment applications to be in the approved form; • removing requirements for agents to provide evidence of identity in all cases for access and amendment applications; No regulatory impact analysis is required under the Better Regulation Policy.

What is the nature, size and scope of the problem? What are the objectives of government action?

Data breach notification

Government collects a significant amount of personal information. A data breach may be caused by malicious action, human error or a failure in information handling or security systems. Examples of data breaches include:

- a USB or mobile phone that holds an individual's personal information being stolen;
- a database containing personal information being hacked; and
- someone's personal information inadvertently being sent to the wrong person.[1]

Data breaches have the potential to cause serious harms to individuals, depending on the type and sensitivity of the personal information involved in the data breach and the circumstances. Examples of serious harms could include identity theft or identity fraud, financial loss, physical harm, reputational harm, emotional harm (such as embarrassment distress) and discrimination.

The Crime and Corruption Commission (CCC)'s report, Ope*ration Impala, A report on misuse of confidential information in the Queensland public sector* (Impala Report)[2] detailed the serious impacts that a data breach can have on vulnerable persons, including victims of domestic violence. The report highlighted the case of *Zil v Queensland Police Service* [2019] QCAT 79 which involved a police officer's disclosure of Zil's residential address to her ex-husband where there was a history of domestic violence. Misuse of confidential information in cases of domestic and family violence can not only impact a person's safety and cause distress and psychological harm but, as the Impala Report detailed, may also have other wide-ranging impacts including incurring costs associated with moving to a new house; children having to change schools; and change of employment.[3]

The report by the Australian Institute of Criminology, *Counting the costs of identity crime and misuse in Australia*, *2018-19* examined the cost and impact of identity crime and misuse on the Australian economy for the 2018–19 financial year. The estimated cost of identity crime in Australia in that year (including direct and indirect costs) was $3.1 billion - 17 percent more than in 2015–16. These findings demonstrate a considerable increase in the financial losses experienced by government, law enforcement, industry and individuals through both direct and indirect costs associated with identity crime.

Recent known data breaches affected millions of Australians: Optus in September 2022, Medibank in October 2022 and Latitude Finance in March 2023. These breaches were the result of malicious attacks.[4]

While errors can occur, resulting in the unauthorised and/or unintentional disclosure of that data, there is scope to minimise the harm for affected individuals. This involves being transparent when a data breach has occurred and enabling individuals to take steps to reduce the risk of harm. For example, an individual can change passwords or be alert to identity frauds or scams. A lack of transparency concerning data breaches also has the potential to detract from the accountability of entities that handle personal information for privacy protection and diminish trust and public confidence in those entities.

Currently Queensland government agencies are not subject to any legislative requirements in the *Information Privacy Act 2009* (IP Act) requiring them to notify data breaches concerning individuals' personal information but are subject to a voluntary notification scheme under the Office of the Information Commissioner's (OIC's) *Privacy Breach Management and Notification Guideline*.[5] In a recent audit, the OIC asked all agencies subject to the IP Act to report on their planning to respond to data breaches and out of 107 respondents, 52 reported

[1] Office of the Australian Information Commissioner, https://www.oaic.gov.au/privacy/data-breaches/what-is-a-data-breach/.

[2] Tabled in the Legislative Assembly on 21 February 2020.

[3] Impala Report, p 45.

[4] Office of the Information Commissioner, *Data Breach Response Plans: Effective and responsive plans – building public confidence*, Report No. 4 to the Queensland Legislative Assembly for 2022-23

[5] Office of the Information Commissioner, *Privacy Breach Management and Notification*, https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/privacy-breach-management-and-notification.

that they had a plan for responding to data breaches.[6] While there are existing measures in place, there is not a consistent approach adopted by all Queensland government agencies.

Let the Sunshine In: A Review of culture and accountability in the Queensland public sector (Coaldrake Report)[7] recommended that citizens' privacy rights be protected by implementation of mandatory reporting of data breaches.

The objectives of Government action are to:

- ensure that there are clear, consistent requirements for Government agencies to notify individuals of data breaches by Queensland government agencies, so that individuals are able to take steps to reduce the risk of harm;
- enhance transparency, accountability and public confidence in Government agencies that handle personal information.

Privacy principles and definition of 'personal information'

The IP Act contains privacy principles governing the collection, storage, transfer, use and disclosure of personal information in the public sector. It also provides a formal mechanism for a person to apply to access or amend their own personal information.

The privacy principles are a significant regulatory mechanism in the IP Act. As noted by the Australian Law Reform Commission (ALRC), the use of a principle-based approach to the regulation of personal information in the public sector is in contrast to 'rules-based regulation' – that is, more detailed and prescriptive regulation.[8]

The privacy principles in the IP Act regulate how agencies and their contracted service providers collect, store, use and disclose personal information. An individual can make a privacy complaint if an individual believes an agency has breached its obligations under the IP Act to comply with the principles.

The IP Act contains two sets of privacy principles – the National Privacy Principles (NPPs), which apply to health agencies, and the Information Privacy Principles (IPPs), which apply to all other agencies. The Commonwealth Privacy Act contains the APPs.

There are similarities between the IPPs and the NPPs in the IP Act. The IPPs and NPPs also share similarities with the Australian Privacy Principles (APPs) in the *Privacy Act 1988* (Cth) (Commonwealth Privacy Act), with greater similarities between the APPs and the NPPs. There are also differences between all three sets of privacy principles which reflect, for example, that the APPs apply to both the public and private sector and the NPPs apply to health agencies. The definition of 'personal information' which is central to the operation of the IP Act and the Commonwealth Privacy Act differs between these two frameworks.

The existence of two similar but not identical sets of privacy principles in Queensland, which are not consistent with the APPs, has the potential to give rise to compliance costs, particularly for entities which may be subject to more than one set of privacy obligations.

Some agencies may have obligations under both the IP Act and the Commonwealth Privacy Act. The IP Act requires agencies to bind certain contracted service providers to privacy principles in the IP Act. This has the potential for contracted service providers to be subject to more than one set of privacy principles, for example if they provide services in more than one Australian jurisdiction, or contract with health agencies and non-health agencies in Queensland. The Privacy Act similarly requires Commonwealth agencies to bind contracted service providers to the APPs.

The different sets of privacy principles may also limit individuals' understanding of their privacy rights, and result in confusion for individuals dealing with both Commonwealth regulated agencies and organisations and Queensland government agencies.

[6] Office of the Information Commissioner, Annual Report 2022-23.

[7] Provided to the Premier and Minister for the Olympics and Paralympics on 28 June 2022

[8] ALRC report, For Your Information: Australian Privacy Law and Practice (ALRC Report 108, 2008), (ALRC 2008 report) pp 642 -3.

There have been a number of calls for greater consistency in approaches to privacy regulation nationally, including by the ALRC (in the Report: For Your Information: Privacy Law and Practice, 2008).[9] A large number of submissions to the ALRC inquiry called for consolidation of the IPPs and the NPPs to create a single set of privacy principles. A number of Queensland reports (including the Impala Report) have also considered whether a single set of privacy principles should be introduced.[10]

The APPs provide a higher standard of protection for 'sensitive information' which includes health related information, DNA and biometric data. They have more explicit requirement for the open and transparent handling of personal information than the IPPs and the NPPs and promote a 'privacy by design' approach, that is, it ensures that privacy and data protection compliance is included in the design of information systems from their inception. Individuals would be given the option of dealing anonymously or by pseudonym with an agency.

The objectives of Government action are to:

- reduce compliance costs for contracted service providers to Queensland Government agencies and other entities who may be subject to more than one set of privacy principles;
- enhance the standard of privacy protections for individuals;
- ensure Queensland Government agencies and their contracted service providers are held to a similar standard as Commonwealth government agencies and their contracted service providers;
- enable individuals to have a greater understanding of their privacy rights, knowing that all agencies in Queensland operate under the same privacy principles and there is increased consistency with Commonwealth arrangements.

Own motion investigation powers and modifications to privacy complaints

A primary objective of the IP Act is to provide for the fair collection and handling in the public sector environment of personal information.

The IP Act does provide the Information Commissioner, on the Commissioner's own initiative or otherwise, to conduct a review into the personal information handling practices of agencies and bound contracted service providers. However, this power can only be exercised to identify privacy related issues of a systemic nature generally, or particular grounds for the issue of a compliance notice.

The IP Act provides for a complaints mechanism which allows an individual to make a privacy complaint to the Queensland Government agency or its bound contracted service provider (in the first instance to the agency or bound contracted service provider, and following that to the OIC) if they believe that their personal information has been dealt with in a way by a Queensland Government agency or its bound contracted service provider that is not consistent with the privacy principles.

Reports have made recommendations for changes to these areas of the IP Act. In particular:

- the Impala report[11] and report on the *Review of the Right to Information Act 2009 and Information Privacy Act 2009* (Review Report)[12] recommended that own motion powers be provided to the Information Commissioner to strengthen existing powers and better identify systemic issues arising from an act or practice of an agency; and
- the Review Report[13] and the and the *Strategic Review of the Office of the Information Commissioner* (Strategic Review Report) [14] recommended changes to timeframes and requirements for privacy complaints.

The objectives of Government action, in developing appropriate responses to these recommendations are to:

- better position the OIC to investigate compliance with privacy obligations under the IP Act, and thereby lead the improvement of public sector privacy administration in Queensland;

[9] ALRC 2008 report, p 486.
[10] Impala report, recommendation 16 recommended that the IPPs and NPPs in the IP Act be amalgamated and strengthened, having regard to the APPs contained in the Privacy Act; RTI/IP Review Report, recommendation 13 referred to the potential benefits of a single set of privacy principles.
[11] Recommendation 14.1.
[12] Recommendation 19.
[13] Recommendations 17 and 18.
[14] Tabled in the Legislative Assembly on 11 May 2017, recommendation (c).

- promote consistency in the way privacy complaints are received and handled across agencies and their bound contracted service providers;
- allow for greater flexibility and the more efficient resolution of privacy complaints.

Other RTI Act and IP Act issues

The primary objective of the RTI Act is to give a right of access to information in the Government's possession or under the Government's control unless, on balance it is contrary to the public interest to give the access. This recognises that in a free and democratic society there should open discussion of public affairs, that information in in Government's possession or under the Government's control is a public resource, and that openness in government enhances accountability and participation in democratic processes.

The IP Act currently includes a similar right of access to, and amendment of, personal information.

A number of reports have made recommendations for changes to the Queensland RTI and IP frameworks to improve and clarify their operation. In particular, recommendations have been made relevant to the following areas:

- providing for a single right of access to documents, including for personal information, to be applied for under the RTI Act, with the RTI Act also to cover applications to amend personal information[15];
- making improvements to the processing of access and amendment applications under the RTI Act[16];
- modifying internal and external review processes under the RTI Act[17];
- clarifying the definition of 'public authority' under the RTI Act[18] which determines whether an entity is subject to the RTI Act;
- reducing the burden on departments and Ministers concerning disclosure logs[19], which form part of the 'push' model' where information released under an RTI application is made available for access to the public by being published on agency websites, and removing the requirements that do not provide substantive benefit to the public[20];
- ensuring that information required for publication schemes, which are a structured list of an agency's information that is readily available to the public, is not overly prescriptive or redundant and that duplication or administrative inefficiency is minimised[21]; and
- ensuring that the preparation of annual reports on the operation of the IP Act and the RTI Act do not impose an unreasonable burden on agencies and results in meaningful data being available.[22]

In broad terms, the objectives of Government action in developing appropriate responses to these recommendations and making changes to the IP Act are to:

- remove legislative duplication and unnecessary steps related to access and amendment applications;
- provide an appropriate balance between the rights of applicants and agencies;
- address lack of clarity in legislative requirements to support understanding by applicants and agencies;
- reduce administrative burden for agencies and Ministers related to disclosure logs and annual report requirements.

Entities regulated by the IP Act, and number of applications and privacy complaints

[15] Review Report, recommendation 2.

[16] Review Report, recommendations 3, 7, 11, recommendation 23.

[17] Review Report, recommendation 11.

[18] Recommendation 3(b) of the Windage report recommended that entities controlled by local councils should come within the oversight of the CC and the RTI Act.

[19] Review Report, recommendation 8.

[20] Review Report, recommendation 8.

[21] Review report, recommendation 10.

[22] Review report, recommendation 12; Strategic Review report, recommendation (d),

Agencies under the IP Act comprise of Ministers, departments, local governments and public authorities as defined under section 21 of the Act. However, they do not include some entities which are excluded by schedule 2 of the Act.

The IP Act requires an agency entering into a certain service arrangements that involve personal information to take all reasonable steps to bind the contracted service provider to comply with the privacy principles. A relevant service arrangement involves a service for the purpose of performing one or more of the contracting agency's functions. There is an exception if a contracted service provider receives funding from the contracted agency, and there is also no collection of personal information by the contracted service provider, or not giving of personal information between the parties.

Once bound, the contracted service provider assumes the privacy obligations as if it were the agency. In the event of a breach, any privacy complaint would be made against the contracted service provider. If the contracting agency *should* have taken all reasonable steps to bind the contractor and didn't, the contracting agency will be liable for any privacy breaches of the contracted service provider. However, the agency will not be liable if, despite taking all reasonable steps, it was not able to bind the contractor.

The *Right to Information Act 2009 and Information Privacy Act 2009 Annual Report 2021-22* indicated that 10,235 access applications and 70 amendment applications under the IP Act (relating to personal information) were received in 2021-22. The OIC referred 9 complaints to the Queensland Civil and Administrative Tribunal.

The OIC's *Annual Report 2022-23* indicates that the OIC finalised 125 privacy complaints, closed 34 accepted privacy complaints and resolved 14 complaints through mediation. The OIC referred 9 complaints to the Queensland Civil and Administrative Tribunal.

The OIC's *Annual Report 2022-23* indicates that the OIC received 41 voluntary notifications from agencies of privacy breaches.

Entities currently regulated by the RTI Act

Agencies under the RTI Act comprise departments, local governments, public authorities, government owned corporations and subsidiaries of government owned corporations. However, some entities are excluded from the operation of the Act (Schedule 2 of the Act). Obligations under the act also apply to Ministers and Assistant Ministers.

The *Right to Information Act 2009 and Information Privacy Act 2009 Annual Report 2021-22* indicated that 6,674 access applications under the RTI were received in 2021-22.

Proposals not within the scope of this IAS

Amendments to the RTI Act to support the Proactive Release of Cabinet documents included in the Information Privacy and Other Legislation Amendment Bill 2023 are not covered by this IAS.

What options were considered?

In view of the problems identified above, two broad options were considered:

- Status quo (no action). This involves making no changes to the IP Act maintaining the status quo. The existing voluntary scheme for mandatory data breach notification would be maintained.
- Legislated response. This involves a suite of legislative measures to achieve the objectives of government action. This option would also be supported by non-regulatory approaches such as education and training.

It is noted that the status quo already involves a non-legislated response in relation to mandatory data breach notification in the form of the OIC's voluntary scheme. Adopting a non-legislated response in relation to the other areas (privacy principles and definition of 'personal information', other privacy issues and other RTI issues) is not considered a feasible option to address the identified objectives of government action, given the existing legislative frameworks that regulate these areas.

Option 1 – Status quo (no action)

Under this option, the framework in the existing IP Act and RTI Act would be maintained. This would entail:

- not introducing a mandatory data breach notification scheme in the IP Act. The OIC's current voluntary scheme would be maintained, under which the OIC 'strongly encourages' agencies to notify affected individuals in the case of a data breach and to notify affected individuals in appropriate circumstances. The OIC's guidelines are published by the OIC, there would be no legal obligations to comply with them;
- continuing with the existing two sets of privacy principles applicable to Queensland government agencies and their contracted service providers (the IPPs, and the NPPs applying to health agencies). These would continue to operate alongside the Commonwealth APPs for organisations with an annual turnover of more than $3 million and certain other organisations, including private sector health providers and to contracted service providers of Commonwealth Government agencies;
- not introducing an own motions investigations power for the Information Commissioner or modify existing timeframes and requirements for privacy complaints; and
- not making amendments to address other IP Act and RTI Act issues and maintaining existing arrangements.

Option 2 – Legislated response

Under this option, a range of amendments to the IP Act and RTI Act would be adopted. In particular:

- a mandatory data breach notification scheme would apply to Queensland agencies in the event of an 'eligible data breach'. An eligible data breach involves unauthorised access to, or unauthorised disclosure of or a loss of personal information, where there is likely harm to an individual to whom the information relates. Agencies must take reasonable steps to contain data breaches, assess whether they are eligible data breaches, provide a statement to the Information Commissioner and notify individuals. Functions and powers would be provided to the OIC to support the scheme;
- a single set of privacy principles, based on the APPs in the Commonwealth Privacy Act, in place of the existing NPPs and IPPs, would apply to agencies and their bound contracted service providers;
- the Information Commissioner would have power to investigate, on the Commissioner's own motion, an act, failure to act or practice of an agency which may be a breach of the privacy principles or other stated obligations under the IP Act;
- arrangements for privacy complaints under the IP Act would be amended to:
  - require privacy complaints to an agency or bound contracted service provider to meet stated requirements, including being made within 12 months of the complainant becoming aware of the act, failure to act or practice the subject of the complaint;
  - allow agencies or bound contracted service providers to request extensions of time to deal with privacy complaints by agreement with the complainant;
  - allow the Information Commissioner to give a respondent written notice requiring them to give information for preliminary inquiries for a privacy complaint;
  - provide that a complainant has 20 business days to ask the Information Commissioner to refer a privacy complaint to QCAT;
- other amendments to the RTI Act and IP would be made to:
  - make changes to the processing of access and amendment applications under the RTI Act including:
    - providing for a single right of access to documents, including for personal information, to be applied for under the RTI Act, with the RTI Act also to cover applications to amend personal information;
    - clarifying the definition of 'processing period' for applications, including extending it by five business days if the only address the applicant has given the agency or Minister to be sent notices is a postal address;
    - extending the timeframe for a decision that a document or entity is outside the scope of the RTI Act from 10 business days to 25 business days;
    - providing a new exemption permitting refusal of access to a document under the RTI Act to the extent that disclosure of information is prohibited under the *Ombudsman Act 2001*;
  - modify internal and external review processes under the RTI Act to:

        - remove the right of internal review and external review to the Information Commissioner of a decision by an entity that an application is outside the scope of the Act, because the Act does not apply to an entity in relation to an entity's judicial or quasi-judicial functions;
        - allow agencies to extend the time in which agencies must make internal review decisions, either by agreement with the applicant or where third-party consultation is required;
        - provide clear authority that in undertaking an internal review, agencies may consider whether the original decision maker has taken reasonable steps to identify and locate documents applied for;
        - allow the Information Commissioner to disclose documents during an external review to third parties, to facilitate the resolution of an external review;
        - provide for a new power for the Information Commissioner to refer documents that the Information Commissioner becomes aware of during external review to an agency or Minister for decision about giving the applicant access;
        - provide a new power for the Information Commissioner to set aside one of a number of stated types of decisions and direct an agency or Minister to decide the application;
        - clarify that an agency or Minister may release documents following an informal resolution of a review;
    - clarify the definition of 'public authority' under the RTI Act or IP Act and provide clearer criteria for when an entity may be declared as a public authority under the RTI Act;
    - require departments and Ministers to be subject to the same requirements as other agencies for disclosure logs under the RTI Act and remove the requirement to include on a disclosure log an applicant's name and whether an applicant has applied on behalf of another entity;
    - require agencies to maintain publication schemes under the RTI Act which outline stated matters and publish information prescribed by regulation; and
    - transfer legislative responsibility for the preparation of annual reports from the responsible Minister to the Information Commissioner.

This option would be supported by non-regulatory approaches such as education and training, and provision of advice, assistance on the interpretation and administration of the IP Act and RTI Act. The OIC performs functions directed at improving agencies' practices in right to information and information privacy and promoting greater awareness of right to information and information privacy in the community and within government.

What are the impacts?

Option 1 – Status quo (no action)

As the status quo option, option 1 represents the base case against which option 2 is compared. As this option entails no further government action, it has no cost, produces no additional benefit. It also does not address the identified objectives of government action.

Option 2 – Legislated response

A Cost-Benefit Analysis for option 2 is presented below. The availability of quantitative information is significantly limited, meaning that it is not possible to monetise or quantify impacts to stakeholders. This means that the impacts have been assessed qualitatively, taking into account stakeholder feedback that has been provided in the consultation processes identified below.

In relation to a legislated approach for all four key components identified below, it should be noted that:

- Government has approved funding of $11.465 million over four years and $2.563 million ongoing, allocated through the State Budget 2023-2024, for the Office of the Information Commissioner (OIC) to implement the reforms;
- Consistent with its statutory role, it is anticipated the OIC will provide training (locally and regionally, online and in person) about the new obligations and requirements. OIC will similarly prepare guidelines and templates for agencies to draw from;

- A long lead time is proposed for commencement of the reforms, to allow agencies time to prepare for implementation;
- New privacy principles will only apply to contracted service providers for new contracts entered into after commencement.

These factors will assist agencies and contractors to manage the impact of the reforms.

The qualitative benefits and costs of the four key components of the legislated response are addressed below:

Mandatory data breach notification scheme

Qualitative benefits of option 2 (compared to option 1)	**Description**
Individuals – notification, receipt of recommendations and capacity to take corrective action	Requiring individuals to be notified of an 'eligible data breach' which involves risk of serious harm, including recommendations about steps they should take to mitigate this harm, would empower individuals to protect their own interests. The increased transparency and accountability will improve the confidence of individuals in dealing with agencies that handle their personal information.
Agencies/government – consistent and transparent arrangements for data breaches	There will be clear, consistently applied and transparent requirements notifying data breaches by Government agencies. Requiring notification may act as an incentive for agencies holding personal information to improve their information handling practices. Any incentive for agencies to suppress or deliberately conceal data breaches would be reduced. The increased transparency and accountability will improve the confidence of individuals in dealing with agencies that handle their personal information.
Qualitative costs of option 2 (compared to option 1)	**Description**
Individuals – potential harm resulting from notification	Notification may create alarm/concern/distress for individuals, in particular vulnerable individuals. Notifications could be sent to incorrect addresses or to deceased persons or their relatives (although this will be mitigated by provisions allowing information sharing with prescribed agencies for the purposes of checking contact details and whether persons are deceased). However, the object of an MDBN scheme is to provide information to individuals to give them the capacity to take action. While there may be a negative impact on a minority of individuals who find notification distressing, it is anticipated that in the vast majority of cases, individuals would choose to be informed about data breaches that affect them. This impact is therefore not considered significant.
Agencies – administrative costs	**Notification:** Agencies will be required to report 'eligible data breaches' to the OIC following an assessment and notify individuals in accordance with legislative requirements. The existence of a voluntary MDBN scheme

	currently being run by the OIC means that many agencies will be familiar with similar requirements. While there may be impacts for agencies which do not comply with the voluntary scheme, the impact for agencies currently complying will not be great**.** **Publication and documentation:** Agencies will need to update existing, data breach policies and procedures, or prepare new ones. Notification of data breaches on websites will be required in some instances. OIC will assist agencies in relation to these tasks, potentially developing template documents for agencies to adopt and modify for their own requirements. **Education:** Agencies will need to understand the details of legislated requirements and communicate to staff, and conduct or participate in training and awareness activities. Again, OIC will assist agencies in their understanding of requirements, so that key staff are able to provide information and advice to their colleagues/executive. **Purchasing:** Information technology and legal services may be required to comply with the assessment obligations, and obligations more generally. OIC advice, training and guidelines may mitigate the need to procure such services. **Record keeping**: Agencies will need to maintain internal registers and be able to demonstrate compliance with obligations. **Enforcement:** Agencies will need to cooperate with reviews, audits, own motion investigations and inspections related to obligations**.** **Other:** Potential increased insurance costs a consequence of perceived risk. Expected increase in privacy complaints will need to be managed. Overall, there will be some impact for agencies in implementing the reforms, particularly in the initial stages. However, it is anticipated that assistance from the OIC will ameliorate this impact. The lead time for implementation will allow agencies to undertake tasks within an extended timeframe. Commencement by proclamation will further assist with preparedness. These impacts will be more significant for local councils, particularly for regional, rural, remote and First Nations councils. Further deferral, by 12 months, of commencement of the MDBN scheme for local councils will further assist.
OIC	Increase in activity resulting from notifications and compliance, enforcement, training and other support functions (funded). Expected increase in privacy complaints will need to be managed. Supporting ICT systems will be required. While there will be significant impacts on OIC in assisting agencies to implement these reforms, OIC is being funded to undertake these tasks.

Single set of privacy principles

Qualitative benefits of option 2 (compared to option 1)	**Description**

Individuals – improved privacy protections	Improved standards of protection for individual's personal information, and increased confidence of individuals in dealing with agencies and bound contracted service providers that handle their personal information. Enable individuals to have a greater understanding of their privacy rights through increased consistency with Commonwealth arrangements. Individuals will know that personal information held by all Queensland agencies is subject to the same set of privacy principles (rather than the IPPs and NPPs which currently apply) and that these principles are more aligned with those that apply to personal information held by Commonwealth agencies.
Agencies/government – simplification and improved standards	For some agencies, alignment with Commonwealth privacy principles will provide benefits in drafting the terms of their commercial arrangements, particularly those that provide services in more than one Australian or other jurisdiction/s and in dealing with Commonwealth government departments and agencies.
Contracted service providers – reduced duplication	Reduce administrative costs (see below) for contracted service providers to Queensland government agencies in complying with more than one set of privacy principles.
OIC	Capacity to leverage existing guidance for APPs issued by the Office of the Australian Information Commissioner. No need to produce/maintain guidance, deal with queries or process complaints relating to two different sets of privacy principles.
Qualitative costs of option 2 (compared to option 1)	**Description**
Individuals	No costs identified.
Agencies – administrative costs	**Notification:** Agencies will need to review collection notices and information on their websites in relation to new QPPs. It is anticipated that OIC will assist agencies in understanding new requirements, and potentially produce guidelines or templates which will assist them. **Publication and documentation:** There will be new requirements to prepare and publish a QPP privacy policy including information about the kind of information the agency holds, how the agency collects and holds personal information, how individuals may access and seek correction of information. Again, it is anticipated that OIC will assist agencies in their understanding of the new requirements. Agencies will then be required to apply this knowledge to their own organisational needs. **Education:** Agencies will need to ensure staff are aware of new policies, procedures and systems to ensure compliance with the QPPs. While it is expected that most agencies will need to provide some in-house advice and awareness to their colleagues/executive, it is expected that training provided by OIC in relation to new requirements will be available to those with key responsibilities (eg Privacy Officers). **Purchasing:** Legal services may be required by agencies to ensure compliance with the new QPP. As noted above, the availability of training by OIC may also reduce the need for legal advice

	Record keeping: Existing requirements about record keeping will continue. Agencies will be required to more actively consider which information should be retained. **Enforcement:** Agencies will need to cooperate with reviews, audits, own motion investigations related to the new obligations**.** These impacts will be more significant for local councils, particularly for regional, rural, remote and First Nations councils. **Overall, there will be some impact for agencies in implementing the reforms, particularly in the initial stages. However, it is anticipated that assistance from the OIC will ameliorate this impact. The lead time for implementation will allow agencies to undertake tasks within an extended timeframe.**
Contracted service providers – administrative costs	**Notification:** Entities will need to review collection notices and information on their websites in relation to new QPPs. Where entities are already compliant with the APPs, there will be a lower impact. **Publication and documentation:** There will be new requirements to prepare and publish a QPP privacy policy including information about the kind of information the agency holds, how the agency collects and holds personal information, how individuals may access and seek correction of information. Where entities are already compliant with the APPs, there will be a lower impact. **Education:** Entities who do not already comply with obligations under the Commonwealth Privacy Act will need to ensure their staff are aware of new obligations. **Purchasing:** Legal services may be required by entities to ensure compliance with the new QPPs. **Record keeping**: Existing requirements about record keeping will continue. Entities will be required to more actively consider which information should be retained in the performance of their contracts. **Enforcement:** Contracted service providers will need to cooperate with reviews, audits, own motion investigations related to the new obligations**.** Overall, there will be some impacts for contracted service providers in implementing the reforms, particularly those which are not subject to the Commonwealth Privacy Act. Contracted service providers will be able to access OIC publications and assistance. As the new privacy principles will only apply to new contracts entered into after commencement, contracted service providers will have choice and control in deciding whether to enter into contracts with agencies and thereby becoming bound by the new privacy principles.
OIC	Increase in activity resulting from compliance, enforcement, training and other support functions (funded). OIC has however been funded to provide these activities.

Own motion investigation powers and modifications to privacy complaints

Qualitative benefits of option 2 (compared to option 1)	**Description**

Individuals and the community	Enabling investigation of compliance with privacy obligations under the IP Act will promote better compliance and improve information privacy administration. The confidence of individuals in dealing with agencies that handle their personal information will be improved. Clearer obligations concerning privacy complaints to relevant entities will apply.
Agencies	There will be more flexibility for agencies to request extensions in time to deal with privacy complaints.
Contracted service providers	There will be more flexibility for bound contracted service providers to request extensions in time to deal with privacy complaints.
OIC	Capacity to support the purpose of the IP Act through own motion investigations will be increased. Being able to compel agencies and bound contracted service providers to provide information for preliminary inquiries for own motion investigation will assist in effectively carrying out this function.
QCAT	The reduced timeframe for a complainant to ask the Information Commissioner to refer a privacy complaint to QCAT (may result in fewer referrals).
Competition impacts	No benefits identified.
Qualitative costs of option 2 (compared to option 1)	**Description**
Individuals and the community	The reduced timeframe to ask the Information Commissioner to refer a privacy complaint to QCAT may limit potential for resolution.
Agencies – administrative costs	**Enforcement:** Agencies may be compelled to provide information for preliminary inquiries for own motion investigation. **Education:** Agencies will need to understand the details of legislated requirements and communicate to staff, and conduct or participate in training and awareness activities.
Contracted service providers – administrative costs	**Enforcement:** Contracted service providers may be compelled to provide information for preliminary inquiries for own motion investigation. **Education:** Contracted service providers will need to understand the details of legislated requirements and communicate to staff, and conduct or participate in training and awareness activities.
OIC	Increase in activity resulting from own motion investigations. However, OIC has been funded for this task.
QCAT	No costs identified.
Competition impacts	Contracted service providers may have reduced incentives to contract with agencies due to potential to be subject to investigations

Other RTI Act and IP Act issues

Qualitative benefits of option 2 (compared to option 1)	Description
Individuals and the community	More streamlined processes for applications for access and amendment, through matters such as: • removal of mandatory forms; • access applications being under one Act; and • removal of requirements to provide evidence of identity for agents
Agencies	More streamlined processes for applications for access applications will reduce time spent by agencies in dealing with applications – for example, decision letters will be shorter because there will be no need to cross-refer to provisions in the IP Act
OIC	Amendments will resolve some ambiguities and provide some clarification, reducing the need to provide guidance and assistance to agencies.
QCAT	No appreciable benefits identified.
Qualitative costs of option 2 (compared to option 1)	**Description**
Individuals and the community	No costs identified
Agencies – administrative costs	**Publication and documentation:** Agencies will be required to revise their processes, procedures, websites and systems to meet new requirements. **Education:** Agencies will need to understand the details of legislated requirements and communicate to staff. As noted above, OIC will assist in providing guidance on these tasks.
OIC	Delivery of training, advice, guidelines etc to transition to new arrangements
QCAT	Will be required to understand and apply new legislative provisions if matters reach the QCAT Appeal Tribunal

Who was consulted?

Two consultation processes, including a public process, were conducted to inform the Review Report, which was tabled in 2017.

On 24 June 2022 the Consultation paper—Proposed changes to Queensland's Information privacy and right to information framework (Public Consultation Paper) was released. The Public Consultation Paper sought feedback from the general public and key stakeholders on key privacy reforms and a number of reforms to enhance and clarify the operation of the IP Act and the RTI Act.

On 27 June 2022 the Agency Consultation Paper was released – to seek input from agencies subject to the IP Act on the benefits and likely administrative impacts of a MDBN scheme and a single set of privacy principles.

In August 2023, a draft Bill was released for targeted consultation with key stakeholders.

Agency Consultation Paper – impacts identified.

Feedback was received from the following agencies:21 departments, 10 statutory agencies, 7 council entities (5 councils and 2 peak local government bodies)and 4 universities.

Further, in-depth consultation was undertaken with the OIC in relation to the financial and resource impacts of overseeing a MDBN scheme..

Assessments of the impacts on agencies were classified according to the following scale:

- HIGH IMPACT - Financial impacts identified including need for funding for FTEs and/or system (IT) changes required
- MEDIUM – Administrative burden as a result of preparing to implement and comply with the scheme, including reallocation of staff to support planning and implementation.
- LOW – No significant impacts identified other than the need to review policies and procedures, some education of staff
- NOT KNOWN -insufficient information to be able to assess

Agencies were not asked directly to quantify any resource impacts as a result of implementation of a mandatory DBN scheme or the QPPs. Therefore, any assessment of high impacts (i.e. financial impacts identified) may have been greater if agencies had been asked directly to quantify any resource impacts.

MDBN impacts: Most agencies (71%) identified low to medium impacts. Medium impacts included primarily administrative burden as a result of preparing to implement and comply with the scheme, including reallocation of staff to support planning and implementation. Whereas low impact included no significant impacts identified other than the need to review policies and procedures, some education of staff. A number of agencies acknowledged the preparation of guidelines by OIC that they would apply and adopt.

Approximately t26% of agencies surveyed identified a high impact (i.e. financial impacts, including need for funding for staff and/or system (IT) changes required.

New privacy principle impacts: Of the agencies surveyed, 55% identified medium or low impacts as a result of the introduction of a single set of privacy principles. Of those agencies that identified medium to low impacts it was still recognised that implementation of a new set of privacy principles would require a significant amount of administrative work including: updating policies, procedures, websites, training and awareness raising.
Some agencies also indicated the need to conduct external consultation with stakeholders and external bodies (including unions and professional associations), conduct a review of contractual arrangements, standing offer arrangements and overseas transfer arrangements.

Approximately 40% of agencies identified a high impact (i.e. financial impacts, including need for funding for staff and/or system (IT) changes). Of those that indicated higher impacts (i.e. the need for funding and/or dedicated staff) impacts also included the need to have new dedicated staff for implementation, new dedicated privacy officers on an ongoing basis.

Impacts of other changes: The Agency Consultation paper did not ask about the impact of RTI Act changes, or IP Act changes other than the change to the QPPs. However, these changes have generally been supported through other consultation rounds, including those outside of government.

What is the recommended option and why?

On balance, it is considered that a legislated response (which also involves a combined regulatory and non-regulatory approach) is the most effective approach to achieving the objectives of government action.

Impact assessment

	First full year	First 10 years**
Direct costs – *Compliance costs**	Not assessed	Not assessed
Direct costs – *Government costs*	Not assessed	Not assessed - however, funding of $11.465 million over four years and $2.563 million ongoing from has been provided to the (OIC) to implement the reforms

Signed

Jasmina Joldić PSM
Director-General
Department of Justice and Attorney-General
Date: 6 October 2023

Yvette D'Ath MP
Attorney-General and Minister for Justice
Minister for the Prevention of Domestic and Family Violence
Leader of the House
Date: 7 October 2023