Information Privacy and Other Legislation Amendment Bill 2023

Explanatory Notes

Short title

The short title of the Bill is the Information Privacy and Other Legislation Amendment Bill 2023 (the Bill).

Policy objectives and the reasons for them

The policy objectives of the Bill are to:

- make key changes to Queensland's information privacy framework to better protect personal information and provide appropriate responses and remedies for data breaches and misuse of personal information by agencies; and
- make changes to Queensland's information privacy and right to information frameworks to clarify and improve their operation; and
- make legislative amendments to support the operation of the administrative scheme which will provide for the proactive release of Cabinet documents (the proactive release scheme).

Information privacy and right to information reforms

The Bill implements or responds to recommendations for legislative change to Queensland's information privacy and right to information frameworks from a number of reports including:

- the report on the *Review of the Right to Information Act 2009 and Information Privacy Act 2009* (Review Report), tabled in the Legislative Assembly on 12 October 2017[1];
- the Crime and Corruption Commission (CCC)'s report, *Operation Impala, A report on misuse of confidential information in the Queensland public sector* (Impala report), tabled in the Legislative Assembly on 21 February 2020[2];
- the CCC's report, *Culture and Corruption Risks in Local Government: Lessons from an investigation into Ipswich City Council* (Windage Report), tabled in the Legislative Assembly on 4 August 2018[3];
- the *Strategic Review of the Office of the Information Commissioner* (Strategic Review Report), tabled in the Legislative Assembly on 11 May 2017[4]; and

[1] Recommendations 2, 3, 7 ,8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, and 23(i)-(iv) and (vi)-(xi).
[2] Recommendations 10, 12, 14(1) and 16.
[3] Recommendation 3(b).
[4] Recommendations (c) and (d).

- *Let the sunshine in: Review of culture and accountability in the Queensland public sector* (the Coaldrake Report), provided to the Premier and Minister for the Olympics and Paralympics on 28 June 2022[5].

The Bill also makes additional clarifications and improvements to information privacy and right to information frameworks that have been identified, including in response to judicial decisions and to suggestions made by stakeholders as part of consultation on the proposed information privacy and right to information reforms.

Amendments to support the proactive release scheme

The proactive release scheme, as recommended by the Coaldrake Report, will be an administrative scheme implemented via amendment to the Cabinet Handbook. This approach is consistent with the New Zealand proactive release scheme. While legislation is not required to enable the scheme, a small number of amendments are included in the Bill to support the simple operation of a proactive release scheme. Amendments to the *Right to Information Act 2009* (the RTI Act) are intended to:

- ensure that the publication of documents under a proactive release scheme does not alter the exempt status of redacted information and of other Cabinet-related documents currently taken to be comprised exclusively of exempt information under the RTI Act;
- ensure Ministers have appropriate protection from civil liability; and
- protect public interest immunity.

Achievement of policy objectives

Information privacy and right to information reforms

To achieve its objectives, the Bill will amend the *Information Privacy Act 2009* (the IP Act) and the RTI Act to:

- align the definition of 'personal information' in the IP Act with the definition in the *Privacy Act 1988* (Cth) (Commonwealth Privacy Act) (recommendation 14 of the Review Report and recommendation 16(2) of the Impala Report);
- adopt a single set of privacy principles in the IP Act, based on the Australian Privacy Principles (APPs) in the Commonwealth Privacy Act and referred to as the Queensland Privacy Principles (QPPs), in place of the National Privacy Principles (NPPs) applying to health agencies and the Information Privacy Principles (IPPs) applying to all other agencies (recommendation 13 of the Review Report and recommendation 16 of the Impala Report);
- establish a mandatory data breach notification (MDBN) scheme applicable to agencies (recommendation 12 of the Impala Report and recommendation 10 of the Coaldrake Report, following on from recommendation 13 of the Review Report);
- provide enhanced powers and functions for the Information Commissioner including:
    - a power to investigate, on the Information Commissioner's own motion, an act, failure to act or practice of an agency which may be a breach of

[5] Recommendation 10.

the privacy principles or other stated obligations under the IP Act (recommendation 19 of the Review Report and recommendation 14(1) of the Impala Report);
    - new functions and regulatory powers in relation to compliance with the new MDBN scheme;
- make improvements to access and amendment applications and the processing of these 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 (recommendation 2 of the Review Report);
    - removing requirements for applications to be in the approved form (recommendation 23(iii) and (iv) of the Review Report);
    - removing requirements for agents to provide evidence of identity in all cases (recommendation 23(vi) of the Review Report);
    - clarifying the definition of 'processing period' for applications (recommendation 23(i) of the Review Report), 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 (recommendation 23(viii) of the Review Report);
    - 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 (recommendation 23(ii) of the Review Report);
    - removing the mandatory requirements for agencies and Ministers to give an applicant a schedule of relevant documents (recommendation 3 of the Review Report), and charges estimate notice (CEN) where no charges apply, and clarifying that applicants are limited to two CENs and that any narrowing of a second CEN would not require a third CEN to be issued (recommendation 23(vii) of the Review Report);
    - 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 (recommendation 11 of the Review Report);
    - 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 (recommendation 23(ix) of the Review Report);
    - provide for a new power for the Information Commissioner to refer documents that the 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 (recommendation 23(x) of the Review Report);
- clarify the definition of 'public authority' and provide clearer criteria for when an entity may be declared as a public authority under the RTI Act (in response to recommendation 3(b) of the Windage Report) or IP Act;
- enhance arrangements for privacy complaints under the IP Act so that:
    - privacy complaints to an agency or bound contracted service provider, are required to meet stated requirements (recommendation 16 of the Review Report), including being made in writing and within 12 months of the complainant becoming aware of the act, failure to act or practice the subject of the complaint;
    - allow respondents to request extensions of timeframes for privacy complaints by agreement with the complainant, and allow a complainant to make a complaint to the Information Commissioner after they receive a written response from an agency or bound contracted service provider without having to wait for 45 business days to expire (recommendation 17 of the Review Report and recommendation (c) of the Strategic Review Report);
    - allow the Information Commissioner to give a respondent written notice requiring them to give information to a preliminary inquiry;
    - provide that a complainant has 20 business days to ask the Information Commissioner to refer a privacy complaint to the Queensland Civil and Administrative Tribunal (QCAT) (in response to recommendation 18 of the Review Report);
- require departments and Ministers to be subject to the same requirements as other agencies for disclosure logs under the RTI Act (recommendation 8 of the Review Report), 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 (recommendation 9 of the Review Report);
- require agencies to maintain publication schemes under the RTI Act which outlines stated matters and publish information prescribed by regulation (recommendation 10 of the Review Report);
- transfer legislative responsibility for the preparation of annual reports from the responsible Minister to the Information Commissioner (recommendation 12 of the Review Report and recommendation (d) of the Strategic Review Report); and
- make a number of other additional clarifications and improvements.[6]

The Bill will also amend the Criminal Code offence of computer hacking and misuse in section 408E to improve its operation and clarity, having regard to the underlying issues forming the basis of recommendation 10 of the Impala Report.

[6] These include amendments to address recommendations 7, 15, 20 and 23(xi) of the Review Report and other matters.

Amendments to support the proactive release scheme

The proactive release of Cabinet documents will officially publish Cabinet information. Cabinet documents (i.e. Cabinet submissions and Cabinet decisions) will not necessarily be published in full, rather there will be redactions where sensitive information should be removed for legislative, commercial or other reasons. This is consistent with practice in New Zealand.

Following an access application under the RTI Act, an agency or Minister may refuse access to all or part of a document to the extent the document comprises exempt information. There is a reasonable expectation that the act of redaction under the proactive release scheme should not change the redacted information's status as exempt information under the RTI Act. However, as proactive release is an entirely novel reform in the Australian context and given the already complex nature of decision-making under the RTI Act, legislative amendments will provide clarity, both for applicants and decision makers, under the RTI Act that the official publication of Cabinet documents, including under the proactive release scheme, does not alter the exempt status of redacted information and of other Cabinet-related documents currently taken to be comprised exclusively of exempt information under the RTI Act.

The Coaldrake Report did not consider the potential impact of a proactive release scheme in Queensland and future claims of public interest immunity. There is a heightened risk that the existence of a proactive release scheme would lead to courts, tribunals or other bodies conducting extra-curial, inquisitorial or investigative proceedings or processes placing less weight on Cabinet confidentiality when considering future claims of public interest immunity. The principles of collective Ministerial responsibility and Cabinet confidentiality remain foundations of Westminster systems of government. An amendment to the RTI Act seeks to protect these foundations by requiring an assessment of the public interest relevant to whether a common law or statutory rule prevents the production or disclosure of information in connection with Cabinet, publication by Cabinet of information (which would include publication under the proactive release scheme) must be disregarded.

The Coaldrake report did not consider the implications of proactive release for potential Ministerial civil liability. There is a risk in any proactive release scheme of inadvertent disclosure of information. Such disclosure could lead to legal action against individuals or the State. For employees of public sector entities, there is already a broad civil liability protection in the *Public Sector Act 2022*, but no similar protection is provided to Ministers who may authorise release of information in good faith under or connection with the proactive release scheme. The amendment therefore extends civil liability protections to Ministers to cover the proactive release of Cabinet documents. Consistent with the approach under the *Public Sector Act 2022*, liability instead attaches to the State.

Commencement

The Bill, when enacted, will commence on a day to be fixed by proclamation.

Alternative ways of achieving policy objectives

There is no alternative method of achieving the policy objectives as the objectives require amendments to legislation.

Estimated cost for government implementation

Information privacy and right to information reforms

The amendments to give effect to the information privacy and right to information reforms, in particular the MDBN scheme and the introduction of a single set of privacy principles, will have resource impacts on agencies.

These reforms will impact on the Office of the Information Commissioner (OIC) due to its statutory responsibility to provide education, training and guidance in relation to the RTI Act and IP Act and its new regulatory and statutory functions including the oversight of the MDBN scheme, own motion powers, and the transfer of annual reporting requirements from DJAG to the OIC. The OIC has been allocated $11.465 million over four years, and $2.563 million ongoing, through the State Budget 2023-24 for operational implementation, development of an ICT solution and training and awareness activities.

Implementation of the reforms by other agencies and entities subject to the IP Act and RTI Act, which include local councils and universities, will have resourcing impacts and costs will be absorbed by those agencies and entities. The resourcing of OIC to undertake education and training will assist agencies and entities to implement the reforms. Phased commencement, including a 12-month delay to implement the MDBN scheme for local councils, will provide a longer period for these councils to transition to the new MDBN and mitigate the immediate resourcing impact.

The amendments to section 408E of the Criminal Code are not expected to have any significant impacts for departments, the courts, the QPS or the Director of Public Prosecutions.

Amendments to support the proactive release scheme

The proactive release scheme will be the first of its kind in Australia. To the extent that cost implications can be ascertained, an initial $10.137 million over four years was allocated through the State Budget 2023-24 for whole-of-government implementation of the proactive release scheme. This funding includes $6.073 million for the Department of the Premier and Cabinet to manage and coordinate the scheme across government, to manage implementation of ICT systems to support proactive release and for seven additional FTE to support the proactive release scheme. It also includes $4.064 million over four years for the Department of Justice and Attorney General to implement the proactive release scheme within its agency.

The proactive release scheme will be kept under review and any additional costs identified will be brought to the Cabinet Budget Review Committee for further consideration.

Consistency with fundamental legislative principles

The Bill is generally consistent with fundamental legislative principles (FLPs) in the *Legislative Standards Act 1992* (LS Act). Aspects of the Bill that raise potential FLP issues, and the justifications for any breaches, are addressed below.

Rights and liberties of individuals

The FLPs include requiring that legislation has sufficient regard to the rights and liberties of individuals – section 4(2)(a) of the *Legislative Standards Act 1992* (LS Act)).

Rights and liberties dependent on administrative power – decision by a judicial or quasi-judicial entity that an application is outside the scope of the RTI Act

The Bill includes amendments to 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 its judicial or quasi-judicial functions. This potentially departs from the FLP that legislation should make rights and liberties, or obligations, dependent on administrative power only if the power is subject to appropriate review (section 4(3)(a) of the LS Act). It also potentially abrogates established statutory review rights.

These amendments are justified on the basis that they are needed to preserve judicial independence and clarify the position for users of the RTI Act, consistent with a series of decisions, (including *Carmody v Information Commissioner & Ors* [2018] QCATA 14) which highlighted the importance of the separation of powers and judicial independence when applying the RTI Act. The right of appeal to the QCAT Appeals Tribunal on a question of law for these decisions is retained which provides a safeguard for applicants.

Consistency with natural justice – timeframes for internal review decisions under the RTI Act and privacy complaints

The Bill includes an amendment to the RTI Act to allow agencies and Ministers to extend the time in which they must make internal review decisions, either by agreement with the applicant or where third-party consultation is required. This may be seen to potentially depart from the FLP that legislation should be consistent with the principles of natural justice (section 4(3)(b) of the LS Act) by allowing a longer period for agencies and Ministers to make internal review decisions, potentially to the detriment of an applicant seeking such a decision. It also abrogates existing statutory rights to internal review decisions within a timeframe that does not accommodate such extensions.

Procedural fairness involves a flexible obligation to adopt fair procedures that are appropriate and adapted to the circumstances of a particular case. The amendment is justified to ensure that there is sufficient time to conduct third-party consultation which is an important aspect of the processing RTI access and amendment applications, noting that otherwise any extension of time specifically requires the applicant's consent. Extending this timeframe to allow for third-party consultation ensures that rights of

third parties are protected and may benefit the applicant in some situations such as where additional documents that were not processed as part of the original application have been located at internal review and need to be considered.

The Bill also includes amendments to the IP Act to:

- provide that a complainant has 20 business days to ask the Information Commissioner to refer a privacy complaint to QCAT for hearing from the day the Commissioner gives written notice that the Information Commissioner does not believe the complaint can be resolved by mediation, or mediation is attempted but is not successful;
- require a privacy complaint to an agency or bound contracted service provider to be made within 12 months of the complainant becoming aware of the act or practice the subject of the complaint.

These may be seen to potentially depart from the FLP that legislation should be consistent with the principles of natural justice (section 4(3)(b) of the LS Act). It also abrogates existing statutory rights of a complainant to seek referral to QCAT or make a complaint to an agency or bound contracted service provider without such a time limit.

The amendments are justified on the basis that they are needed to provide more certainty for respondents and applicants about the status of complaints, and ensure that referrals to QCAT are made within a timely manner. For referrals to QCAT, the Information Commissioner would have discretion to extend the timeframe if reasonable all in the circumstances. For privacy complaints to an agency or bound contracted service provider, the respondent may agree to a longer period if satisfied that the extension is reasonable. The amendments therefore provide sufficient flexibility to ensure fairness to an applicant.

Abrogation of established statutory rights – processing period for applications under the RTI Act

The Bill includes an amendment to the RTI Act to provide that the definition of processing period for an access or amendment application is extended by five business days if, at the time the application complies with all relevant application requirements, the only address the applicant has given the agency or Minister to be sent notices is a postal address. This abrogates existing statutory rights of applicants to decisions within a processing period that does not accommodate such extensions.

The amendment is needed to accommodate the additional time taken for postal delivery, which is beyond the control of the agency or Minister, and to address the longer postal delivery times that have arisen in recent years. While it is important that applicants receive timely decisions, the amendment is justified on the basis that it is necessary to provide fairness to agencies and Ministers and reduce the risk of deemed decisions arising due to a factor which is outside their control.

The Bill also includes amendments to exclude entities established by letters patent from the application of the RTI Act and the IP Act. This abrogates existing statutory rights under those Acts to these entities.

Entities established by letters patent are mainly religious and charitable organisations. The amendment is needed to provide consistency with the core purpose of the RTI Act (which is for a right of access to information in the government's possession or under the government's control), and to alleviate the administrative burden on such entities complying with RTI Act obligations, including dealing with access applications, publishing disclosure logs and maintaining publication schemes.

The amendments are needed to provide consistency with the core purpose of the IP Act, which is to provide for the fair collection and handling in the public sector environment of personal information, and to also alleviate the administrative burden of such entities in complying with the IP Act obligations, including with the privacy principle requirements.

Consequences proportionate and relevant to the actions to which they are applied – criminal offences

The Bill includes new offences in the IP Act for:

- failure by an authorised officer to return their identity card within 15 business days after the office ends, unless they have a reasonable excuse (new section 66) – maximum penalty of 10 penalty units;
- failure by an agency to take all reasonable steps to facilitate entry by an authorised officer on a date and time consented to or stated in a notice (new section 68)– maximum penalty of 100 penalty units; and
- failure by a person to give reasonable help to an authorised officer to exercise powers unless they have a reasonable excuse (new section 71) – maximum penalty of 100 penalty units.

The Bill expands the scope of section 160 of the IP Act, which provides an offence with a maximum penalty of 100 penalty units, for a failure by a 'relevant entity' to comply with a compliance notice given by the Information Commissioner, which means that it applies to bound contracted service providers as well as agencies.

The Bill expands the scope of section 186 of the IP Act, which provides an offence, with a maximum penalty of 100 penalty units, for giving information to the Information Commissioner, or a member of staff of the OIC, that the person knows is false or misleading particular, so that it also applies to information given to an authorised officer.

The penalty level for an offence, including whether it is proportionate to the level of seriousness of the offence and consistent with other similar offences, is relevant to whether the offence has sufficient regard to the rights and liberties of persons who may be subject to it.

The penalties for new and amended offences under the IP Act are proportionate and relevant to the actions to which they apply, taking into account comparable existing offences, including those already within the IP Act. The penalties are sufficiently high to deter non-compliance and thereby support the effectiveness of the IP Act in achieving its objectives, and allow the functions and powers of the Information Commissioner and authorised officers to be performed and exercised with appropriate assistance from agencies and relevant persons.

The amendments to section 408E of the Criminal Code include an increase in the maximum penalty for the simpliciter offence in subsection (1) from two years to three years imprisonment and reclassify the offence as a misdemeanour. These amendments are designed to address concerns raised by the CCC in its Impala Report that the current penalties for section 408E do not adequately reflect the serious nature of deliberate breaches of the public's privacy by public officers. The higher maximum penalty of three years imprisonment is considered justified on the basis of the demonstrated need for deterrence and to meet community expectations. Reclassifying the offence as an indictable offence will also have the consequence that there will no longer be a time limit on commencing a prosecution. The CCC in its Impala Report highlighted that one of the challenges in applying section 408E was that in some cases charging under the offence becomes statute barred. The classification of this offence as a misdemeanour is consistent with the approach taken for other similar Criminal Code offences used to prosecute corruption and abuse of office (see Chapter 13 of the Criminal Code).

Reversal of onus of proof and appropriate defences to liability – criminal offences

Offences in new sections 66 and 71 of the IP Act (see above) allow for a 'reasonable excuse' for failure to comply. This potentially departs from the FLP that legislation should not reverse the onus of proof in criminal proceedings without adequate justification (section 4(3)(d) of the LS Act).

The inclusion of 'reasonable excuse' in these offences acknowledges that there are likely to be range of matters that are peculiarly within the knowledge of the defendant and that the defendant would be better positioned than the prosecution to meet the evidential burden. It ensures liability would not be unjustly imposed, given the unpredictability of situations likely to arise.

The Bill includes amendments to the IP Act and RTI Act so that the Information Commissioner or a member of staff of the OIC will not be liable for an offence for disclosing information that they obtained in performing functions under the IP Act or RTI Act where that disclosure is required to lessen or prevent a serious threat to life, health or safety. This is intended provide an appropriate defence to ensure that such persons are not liable in those limited circumstances involving such serious threats to life, health or safety, acknowledging that in those limited circumstances the public interest is better served in allowing disclosure than preventing it.

Power to enter premises – monitoring and investigation relating to the MDBN scheme

The Bill includes amendments which allow for an authorised officer to enter into an agency's place of business or another place it occupies if they have consented to entry, or into an agency's place of business or another place it occupies if consent has not been provided but particular notice requirements have been satisfied.

Conferral of power to enter premises only with a warrant issued by a judge or judicial officer is relevant to whether legislation has sufficient regard to rights and liberties of individuals (section 4(3)(e) of the LS Act)).

The purpose for the amendments allowing entry by authorised officers is to observe a demonstration of data handling systems and practices of the agency, or inspect a document that is relevant to the systems, policies and practices of the agency, that relate to compliance with obligations under the MDBN scheme. The functions of an authorised officer are to monitor and investigate whether an occasion has arisen for the exercise of the Information Commissioner's powers that relate to compliance with the MDBN scheme. In viewing the systems and practices, the OIC would gain practical insights and understanding that they would not otherwise be able to obtain through the use of other existing powers.

The amendments are limited in their scope and do not authorise the search and seizure of property. An authorised officer must be issued with an identity card and must produce them when exercising a power. A place of business, for an agency, does not include a part of the place where a person resides. Requirements to provide reasonable help to an authorised officer are subject to a reasonable excuse where there may be self-incrimination, would result in the disclosure of information that is the subject of legal professional privilege or would result in the disclosure of confidential information in contravention of a law. In addition, documents or information obtained by an authorised officer are subject to an immunity so that evidence of these documents or information, or other evidence directly or indirectly derived from the documents or information, is not admissible against the individual in any proceeding to the extent it tends to incriminate the individual or exposes them to penalty.

The amendments are justified on the basis that they are needed to support the effective operation of the MDBN scheme by allowing for the monitoring and investigation of compliance with the scheme and thereby contribute to its effectiveness.

Abrogation of established statutory and common law rights – public interest immunity

The Bill includes an amendment to the RTI Act which provides that the publication by Cabinet of any information or a decision to officially publish Cabinet information on a regular basis must be disregarded when a decision is being made in a proceeding or process about whether a common law or statutory rule prevents the production or disclosure of information in connection with Cabinet because the production or disclosure would be contrary to the public interest.

This amendment potentially alters the operation of existing common law and statutory rules, and therefore it may abrogate existing common law and statutory rights arising from the application of those rules. However, the amendment does not seek to create a restriction per se. Rather, it seeks to maintain the status quo in terms of how the public interest immunity operated prior to the introduction of the proactive release scheme.

The amendment is justified on the basis that it is necessary to ensure that the publication of Cabinet information does not lead to courts, tribunals and other entities placing less weight on the considerations underpinning the convention of Cabinet confidentiality when assessing a claim for public interest immunity in processes or proceedings. It is intended to clarify that the publication of information by Cabinet does not derogate from an assessment of public interest privilege that previously attached to the Cabinet documents prior to the proactive release scheme.

Immunity from proceeding – civil liability for Ministers

The Bill includes an amendment which provides that a Minister does not incur civil liability as a result of, or in connection with, disclosing information under a publication scheme or other administrative scheme in good faith. If liability is prevented from attaching to a Minister, the liability attaches instead to the State. This potentially departs from the FLP that legislation should not confer immunity from proceeding or prosecution without adequate justification (section 4(3)(h) of the LS Act).

The amendment is justified on the basis that conferral of immunity from civil liability for a Minister as a result of, or in connection with, disclosing information under a publication scheme in good faith is a reasonable and appropriate protection provided to Ministers who may be involved in such disclosure of information under a publication scheme, such as through official publication by a decision of Cabinet of information contained in a Cabinet document or publishing of information on a department's website. There is already a broad civil liability protection in the *Public Sector Act 2022*, for employees of public sector entities engaging in conduct in an official capacity but no similar protection is provided to Ministers. Importantly, the protection is available only if disclosure is in good faith, and if liability is prevented from attaching to a Minister, the liability will instead attach to the State. This ensures that there is still potential recourse against the State that is available to persons seeking to make a civil liability claim in relation disclosure under a publication scheme.

Abrogation of existing statutory right – continuation of offences

The Bill includes an amendment which provides that a proceeding for an offence against former section 185 of the IP, which prohibits a person from knowingly deceiving or misleading a person exercising powers under the IP Act in order to gain access to a document containing person's personal information, or an offence against section 187, which concerns failing to give information, produce a document or attend before the Information Commissioner, in relation to a chapter 3 document, may be continued and started, and the person may be convicted of and punished for the offence, as provisions of the Amendment Act amending or omitting these sections had not commenced. The section applies despite section 11 of Criminal Code which provides that a person cannot be punished for doing or omitting to do an act unless the act or omission constituted an offence under the law in force when it occurred and when the person is charged. This abrogates an existing statutory law right provided by that section.

The continuation of proceedings and convictions and punishments for these offences is justified on the basis that the offences are in effect for the same conduct under provisions with continued effect under the RTI Act, and the amendment merely ensures that any conduct that occurred under the former IP Act continues to be subject to these offences.

Privacy rights and other human rights

The right to privacy and other human rights are relevant to consideration of whether legislation has sufficient regard to individuals' rights and liberties. Amendments which

limit the right to privacy and the justification for these limitations are addressed in the Statement of Compatibility with Human Rights for the Bill.

Institution of parliament

The FLPs include requiring that legislation has sufficient regard to the institution of Parliament – section 4(2)(b) of the LS Act.

Appropriateness of delegation of legislative power – QPP codes

The Bill includes amendments related to the approval of QPP codes which are written codes of practice about information privacy, approved by regulation, which state how one or more of the Queensland privacy principles (QPPs) are to be applied or complied with by agencies that are bound by it. A QPP code may also impose additional requirements to those imposed by a QPP, to the extent that they are not inconsistent with a QPP. The development of a draft QPP code can be initiated by an agency or the Information Commissioner and publication and invitation of submissions is required on the draft code. A draft QPP code must be endorsed by the Minister and the QPP code will only take effect if approved by regulation. This may be seen to potentially depart from the FLP that a delegation of legislative power should only be made in appropriate cases and to appropriate persons (section 4(4)(a) of the LS Act).

The purpose of the QPP code arrangement is to provide individuals with transparency about how their information will be handled and ensure consistency across those entities that a QPP code is applied to. QPP codes will not lessen the privacy rights of an individual provided for in the IP Act. The focus of the QPP codes is expected to be of a practical and operational nature which would not be appropriately suited to be dealt with in primary legislation. In these circumstances, any departure from the FLP is justified.

Appropriateness of delegation of legislative power – Guideline for permitted general situations

The Bill includes amendment related to the preparation and approval of a guideline about the collection, use or disclosure of personal information to assist an entity locate a person who has been reported as missing. The preparation of a guideline is initiated by an agency or the Information Commissioner, and publication and invitation of submissions is required on the draft guideline. A draft guideline must be endorsed by the Minister and the guideline will only take effect if approved by regulation. This may be seen to potentially depart from the FLP that a delegation of legislative power should only be made in appropriate cases and to appropriate persons (section 4(4)(a) of the LS Act).

The purpose of the arrangements for guidelines is to allow the Information Commissioner to development guidelines would not be appropriately suited to be dealt with in primary legislation. In these circumstances, any departure from the FLP is justified.

Appropriateness of delegation of legislative power – Extension of assessment period under the MDBN scheme

The Bill includes a provision which allows an agency that is satisfied that an assessment of a known or suspected eligible data breach will take longer than 30 days to extend the period within which it must be completed. The agency must, before the end of the 30-day period give written notice to the Information Commissioner providing information about the extension and the Information Commissioner may ask the agency to provide further information or updates about progress. This may be seen to potentially depart from the FLP that a delegation of legislative power should only be made in appropriate cases and to appropriate persons (section 4(4)(a) of the LS Act).

The amendment is justified on the basis that it is needed to provide sufficient flexibility to allow agencies to undertake a fulsome assessment of a data breach, and acknowledging that there may be significantly complex matters involved leading to an agency being best placed to determine how long an assessment may take if not possible to achieve within 30 days taking into consideration factors including resourcing. It is a requirement to provide a statement to the Information Commissioner as soon as practicable after a belief is formed that there is an eligible data breach and there are powers for the Information Commissioner to seek information from an agency concerning a data breach which will allow for information to be sought concerning potentially unwarranted delays by an agency in conducting an assessment.

Appropriateness of delegation of legislative power – Waivers of modifications of privacy principle requirements and MDBN scheme obligations

The Bill includes a provision which allows an agency to apply to the Information Commissioner for an approval that waives or modifies obligations under the MDBN scheme applying to both the agency. This expands the existing provision which allows an agency to apply for an approval that waives or modifies and agency's obligation to comply with the privacy principles. This may be seen to potentially depart from the FLP that a delegation of legislative power should only be made in appropriate cases and to appropriate persons (section 4(4)(a) of the LS Act).

The Information Commissioner may give an approval only if the Commissioner is satisfied that the public interest in the agency's compliance with the relevant obligations is outweighed by the public interest in waiving or modifying the obligation. The ensure that this mechanism has sufficient regard to the institution of Parliament, the tabling of the approval in the Legislative Assembly is required and approval will be subject to disallowance, as if it were subordinate legislation. The amendment is justified on the basis that it is necessary to provide flexibility in balancing the interests of protection of individual's personal information against other emerging public interests.

Appropriateness of delegation of legislative power – Corporations legislation displacement

The Bill includes provisions which will allow a regulation to be made prescribing a provision of the RTI and IP to be a Corporations legislation displacement provision for the purposes of section 5G of the *Corporations Act 2001*. These provisions may potentially depart from the following FLPs:

- whether the Bill allows the delegation of legislative power only in appropriate cases and to appropriate persons (LS Act, s 4(4)(a)); and
- whether any regulation declaring a displacement provision will contain only matter that is appropriate to SL (LS Act, s 4(5)(c)).

The amendments are justified on the basis that they are necessary to provide flexibility to ensure that if a corporation is prescribed in the future to be a public authority under the RTI Act or IP Act, consideration can be given at that time to provisions of the Corporations legislation which should be displaced to give effect to provisions in the Acts. Section 5G of the *Corporations Act 2001* provides that if a State law declares a provision of a State law to be a Corporations legislation displacement provision, any provision of the Corporations legislation with which the State provision would otherwise be inconsistent does not apply to the extent necessary to avoid the inconsistency.

Consultation

Information privacy and RTI reforms

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.

A consultation draft of a Bill containing amendments to give effect to information privacy and RTI reforms was released for targeted consultation with key stakeholders in August 2023.

The majority of measures contained in the Bill will implement or address recommendations for legislative change from the reports noted above, which were also subject to separate consultation processes.

Amendments to support the proactive release scheme

No public consultation has been conducted on the amendments required to support a proactive release scheme. As this is an administrative scheme being implemented via amendment to the Cabinet Handbook, the amendments are considered technical in nature to support the scheme and are minor in their impact.

Consistency with legislation of other jurisdictions

The Bill is specific to the State of Queensland, and is not uniform with or complementary to legislation of the Commonwealth or another state or Territory.

The single set or privacy principles has been developed to be consistent, as far as possible, with the current Australian Privacy Principles under the Commonwealth Privacy Act, but adapted as appropriate for Queensland agencies.

Notes on provisions

Part 1 Preliminary

Clause 1 provides that, when enacted, the Bill will be cited as the *Information Privacy and Other Legislation Amendment Act 2023* (the Amendment Act).

Clause 2 provides for commencement of the Amendment Act, other than part 6 and schedule 1, part 1, on a day to be fixed by proclamation. The clause also provides that section 15DA of the *Acts Interpretation Act 1954*, which provides for automatic commencement of postponed law that has not commenced within one year of its assent, does not apply to the Amendment Act.

Part 2 Amendment of Criminal Code

Clause 3 provides that part 2 amends the Criminal Code. A note alerts readers to a further amendment to the Criminal Code in schedule 1, part 2 to the Bill.

Clause 4 amends section 408E (Computer hacking and misuse) of the Criminal Code to:

- omit the heading for section 408E and replace it with the new heading, 'Misuse of a restricted computer';
- reclassify the simpliciter offence under subsection (1) as a misdemeanour and increase the maximum penalty for this offence to three years imprisonment; and
- amend the definition of benefit under subsection (5) to clarify that a benefit need not be pecuniary (consistent with the definition of detriment).

Clause 5 inserts new part 9, chapter 108 (Transitional provision for Information Privacy and Other Legislation Amendment Act 2023) which contains new section 760. This section provides that section 408E of the Criminal Code as in force before commencement continues to apply if an act or omission constituting an offence against section 408E happened before commencement, whether the proceeding for the offence is started before or after the commencement.

Part 3 Amendment of Information Privacy Act 2009

Clause 6 provides that part 3 amends the *Information Privacy Act 2009* (IP Act). A note alerts readers to further amendments to the IP Act in schedule 1, part 2 to the Bill.

Clause 7 amends the long title of the IP Act to remove reference to the Act providing a right of access to, and amendment of personal information. These matters will be dealt with under the *Right to Information Act 2009* (RTI Act).

Clause 8 amends section 3 (Object of Act) to omit content relating to right of access to or amendment of personal information. These matters will be dealt with under the RTI Act.

Clause 9 omits section 4 (Act not intended to prevent other accessing or amendment of personal information) and section 5 (Relationship with other Acts requiring access to or amendment of personal information). This is consequential to the omission of chapter 3 of the IP Act.

Clause 10 replaces section 7 (Relationship with other Acts prohibiting disclosure of information) to reflect the omission of chapter 3 of the IP Act, and to provide that QPPs 6.1 and 6.2(d) and the permitted health situation mentioned in section 5 of schedule 4 do not override any law with respect to assisted and substituted decision-making, including, for example, the *Guardianship and Administration Act 2000* and the *Powers of Attorney Act 1998.*

Clause 11 omits section 9 (Relationship with Right to Information Act) which related to access applications made under the RTI Act that could have been made under the IP Act. This is consequential to the omission of chapter 3 of the IP Act.

Clause 12 replaces section 12 (Meaning of *personal information*), section 13 (Meaning of a *document* of an agency for ch 3) and section 14 (Meaning of a *document* of a Minister for ch 3) with new sections 12 and 13. New section 12 (Meaning of *personal information*) provides for a new meaning of personal information consistent with the definition in section 6 (Interpretation) of the *Privacy Act 1988* (Cth). The new definition refers to information or an opinion about an identified individual, or an individual who is reasonably identifiable from the information or opinion, whether or not the information or opinion is true, and whether or not the information or opinion is recorded in a material form. New section 13 (Meaning of *held* or *holds* in relation to personal information) provides the personal information is 'held' by a relevant entity, or the entity 'holds' personal information, if the personal information is contained in a document in the possession, or under control, of the relevant entity. This definition is consistent with the definition of "holds" in section 6 (Interpretation) of the *Privacy Act 1988* (Cth).

Clause 13 replaces section 15 (Meaning of *document* otherwise) to provide a new definition of 'document' which reflects the omission of chapter 3 and the use of the terminology 'privacy principle requirements'.

Clause 14 replaces section 16 (Meaning of *document to which the privacy principles do not apply*) so that the section heading and the section use the terminology 'privacy principle requirements'.

Clause 15 omits section 17 (Meaning of *agency* for ch 3) which is no longer needed due to the omission of chapter 3 of the IP Act.

Clause 16 makes consequential amendments to section 18 (Meaning of *agency* otherwise) to reflect the omission of chapter 3 of the IP Act and the use of the terminology 'privacy principle requirements' and to incorporate the definition of 'entity to which the privacy principle requirements do not apply' into the section.

Clause 17 omits section 19 (Meaning of *entity to which the privacy principles do not apply*) to reflect its incorporation into section 18.

Clause 18 makes consequential amendments to section 20 (Special provision about application of Act other than ch 3 to a Minister) and the section heading to reflect the omission of chapter 3.

Clause 19 amends section 21 (Meaning of *public authority*) to more clearly provide that an entity over which government is in a position to exercise control is a separate type of entity that may be prescribed by regulation to be a public authority for the Act. The clause also provides that an entity may be declared by regulation to be a public authority in relation to only a part of its functions. The clause also provides that a public authority does not include an entity established by letters patent.

Clause 20 amends section 23 (What it means to *disclose* personal information and to *use* personal information) to omit subsection (1) which limits the section's application for the privacy principles, which is no longer needed due to the omission of chapter 3 of the IP Act.

Clause 21 replaces section 24 (Meaning of *control* of a document), which is no longer needed due to the definitions in new section 13, and section 25 (References to IPPs and NPPs) with new section 24. New section 24 (References to doing an act or engaging in a practice) provides that, in the IP Act, a reference to doing an act or engaging in a practice in contravention of a requirement includes a reference to a failure to act or failure to engage in a practice in contravention of a requirement.

Clause 22 replaces section 26 (Information Privacy Principles) to provide that each Queensland privacy principle is set out in schedule 3 to the IP Act, and that a reference to a QPP followed by a number is a reference to the provision of schedule 3 having that number.

Clause 23 amends section 27 (Agencies to comply with IPPs) to require an agency, other than an APP entity, to comply with the QPPs. An APP entity is an agency that is required to comply with the Australian Privacy Principles under the *Privacy Act 1988* (Cth). The clause also updates the note under section 27(1) to alert readers to section 20 for the application of the IP Act in relation to a Minister.

Clause 24 amends section 28 (Noncompliance with particular IPPs) to update the heading to refer to QPPs and provide that an agency is not required to comply with QPP 6 or QPP 10.2 in relation to an individual's personal information where the individual has previously published or given that information for the purpose of publication. 'Publish' for personal information, means publish information by way of television, newspaper, radio, internet or other form of communication.

Clause 25 amends section 29 (Special provision for law enforcement agencies) to provide that a law enforcement agency is not subject to QPP 3.6, 5, 6 or 10.1 if the law enforcement agency is satisfied on reasonable grounds that non-compliance with the QPP is necessary for particular activities, functions or responsibilities stated in the section.

Clause 26 omits chapter 2, part 2 (Compliance with NPPs), in view of the adoption of the QPPs.

Clause 27 replaces the heading for chapter 2, part 3 (Transfer of personal information outside Australia) with 'Part 2 Disclosure of personal information outside Australia'. Part 3 of the chapter 2 becomes part 2 of chapter 2.

Clause 28 amends section 33 (Transfer of personal information outside Australia) so that the section refers to 'disclosure' of an individual's personal information to an entity outside Australia, rather than 'transfer' of such information. The amendments also update references to the IPPs and the NPPs with references to the QPPs.

Clause 29 replaces the heading to part 4 of chapter 2 (Compliance with parts 1 to 3 by contracted service providers) to be part 3 of chapter 3 'Compliance with parts 1 and 2 and s 41 by contracted service providers' to reflect the amended content of this part. Part 4 of chapter 2 becomes part 3 of chapter 2.

Clause 30 amends the section heading for section 35 (Binding a contracted service provider to privacy principles) to use the terminology 'privacy principle requirements'. The clause also amends the section to refer to an agency taking all reasonable steps to ensure that the contracted is required to comply with parts 1, 2 and section 41.

Clause 31 amends the section heading for section 36 (Bound contracted service provider to comply with privacy principles) and subsection 36(3) to use the terminology 'privacy principle requirements'. The clause also amends the section to refer to a contracted service provider being required to comply with parts 1, 2 and section 41.

Clause 32 amends section 38 (Personal information relevant to portfolio responsibilities) so that it refers to the QPPs rather than the IPPs or NPPs.

Clause 33 replaces chapter 3 (Disclosure and amendment by application under this Act) with: new chapter 3 (QPP codes and guideline for permitted general situations). Applications for access or amendment to documents containing an individual's personal information will now be covered by the RTI Act. New chapter 3 contains new sections 40 to 43 (regarding QPP codes) and new sections 44 to 45 (regarding guidelines for permitted health situations). The clause also inserts new chapter 3A (Mandatory notification of data breaches) which contains new sections 46 to 74.

New section 40 (QPP codes) provides that a QPP code is a written code of practice about information privacy, approved by regulation, that states how one or more QPPs are to be applied or complied with. A QPP code must state the agencies that are bound by it, or a way of determining the agencies that are bound by it. A QPP code may also impose additional requirements to the extent they are not inconsistent with a QPP. A QPP code expires on the day that is five years after it is approved or the stated day for expiry, whichever is earlier.

New section 41 (Agencies must comply with QPP codes) provides that an agency must not do an act, or engage in a practice, that contravenes a QPP code that is in effect and binds the agency.

New section 42 (Preparing QPP codes) provides that the Information Commissioner or agency may prepare a draft QPP code or draft amendment of a QPP code and submit the draft to the Minister for endorsement. The section also provides for steps that the

Information Commissioner or agency must carry out before the draft code or amendment is submitted to the Minister. An agency must also notify the Information Commissioner immediately after publishing a draft QPP code or draft amendment of a QPP code.

New section 43 (Approval of QPP codes or amendments of QPP codes) provides that if a draft QPP Code or draft amendment of QPP code is submitted by an agency to the Minister for endorsement, the Minister must ask the Information Commissioner for submissions about the draft. The Minister must decide to endorse or refuse to endorse the draft having regard to any submissions made by the Information Commissioner and any other relevant matter. If the Minister endorses the draft, the Minister must recommend to the Governor in Council the making of a regulation approving the QPP code or amended QPP code, and QPP code or amended QPP code takes effect following approval by regulation on the day prescribed by regulation. The Information Commissioner must, as soon as practicable after a regulation approving a QPP code or amended QPP code is made, publish the code or amended code on the Information Commissioner's website.

New section 44 (Preparing guideline) provides that the Information Commissioner may prepare a draft guideline about the collection, use or disclosure of personal information to assist an entity locate a person who has been reported as missing, and submit the draft to the Minister for endorsement. However, before the Information Commissioner submits the draft guidelines to the Minister, the commissioner must publish the draft on the commissioner's website and invite the public to make submissions in accordance within a stated period of at least 20 business days, and consider submissions.

New section 45 (Approval of guideline) provides that if a draft guideline is submitted to the Minister under section 44, the Minster must decide to endorse or refuse to endorse the draft. If the Minister endorses the draft, the Minister must recommend to the Governor in Council the making of a regulation approving the guideline, and the guideline takes effect following approval by regulation on the day prescribed by regulation, and expires 5 years after it takes effect. The Information Commissioner must, as soon as practicable after a regulation approving a guideline is made, publish the guideline on the information commissioner's website.

New section 46 (Application of chapter), in new chapter 3A (Mandatory notification of data breaches), provides that new chapter 3A applies in relation to personal information other than information in a document to which privacy principle requirements do not apply, but does not apply to an agency that is an APP entity under the *Privacy Act 1988* (Cth).

New section 47 (Meaning of *eligible data breach*) provides for the circumstances in which an eligible data breach occurs in relation to personal information held by an agency. The circumstances are where there is a data breach involving unauthorised access to, or unauthorised disclosure of personal information, which is likely to result in serious harm to an individual to whom the information relates, or a data breach involving loss of personal information where unauthorised access to, or disclosure of information is likely to occur and if it was to occur would be likely to result in serious harm to an individual to whom the information relates. Regard must be had to stated matters in considering whether serious harm would be likely to result.

New section 48 (Obligations of agencies in relation to data breaches) applies in relation to a data breach of an agency that the agency that knows or reasonably suspects is an eligible data breach. The agency must immediately take all reasonable steps to contain the data breach and if the data breach is not known to be an eligible data breach, assess whether there are reasonable grounds to believe the data breach is an eligible data breach. The assessment must be completed within 30 days after the suspicion was formed, which may be subject to extension under new section 49, and during the assessment the agency must take, or continue to take, all reasonable steps to contain the data breach and take all reasonable steps to mitigate the harm cause by the data breach. The agency must also notify another agency if the agency is aware that the data breach may affect them. If all of the personal information the subject of the data breach also the subject of a data breach of one or more other agencies, and at least one of the other agencies has undertaken to conduct the assessment, the agency need not conduct an assessment.

New section 49 (Extension of period for assessment by agency) allows for extension of the period in which as assessment is required to be conducted by an agency where the agency is satisfied that the assessment cannot reasonably be conducted within 30 days. The agency must start the assessment and notify the Information Commissioner of the extension, and the Information Commissioner may ask for updates about progress.

New section 50 (Application of part) provides that chapter 3A, part 3 (Notifying eligible data breaches) applies if an agency reasonably believes that there has been an eligible data breach of the agency. However, chapter 3A, part 3, division 2 does not apply in relation to the agency to the extent an exemption applies to the agency under chapter 3A, part 3, division 3.

New section 51 (Agency must give statement about eligible data breach to information commissioner) provides for the preparation and giving of a statement to the Information Commissioner which includes stated information, to the extent it is reasonably practicable.

New section 52 (Further information to be provided) provides that if it is not reasonably practicable to include any information a statement given to the Information Commissioner, the agency must take all reasonable steps to provide the information to the Commissioner as soon as practicable.

New section 53 (Agencies must notify particular individuals) provides for the circumstances in which an agency must notify an individual whose personal information has been accessed, disclosed or lost or otherwise each ‘affected individual’, and the information that must be included in the notice. If notifying individuals is not reasonably practicable, the agency must publish information in a notice on an accessible agency website for a period of at least 12 months and the Information Commissioner must publish information on the Commissioner’s website about how to access the notice for a period of at least 12 months.

New section 54 (Particular agencies may collect, use and disclose relevant personal information for notification) provides for a regulation that may prescribe a disclosing agency that is able to disclose relevant personal information to another agency, and a

receiving agency (that it is subject of an eligible data breach as identified in the section 54(4)) that may disclose relevant personal information to, and collect and use relevant personal information from, a disclosing agency. The provision may only be relied upon if it is reasonably necessary for the purpose of confirming the name and contact details of a notifiable individual or whether a notifiable individual is deceased. If a disclosing agency may enter into an arrangement and charge a fee under an Act for the provision of personal information, the agency may do so under that Act in relation to the personal information that may be disclosed.

New section 55 (Exemption – investigations and proceedings), in chapter 3A, part 2, division3, provides that an agency need not comply with chapter 3A, part 2, division 2 (Notification) to the extent complying with that division is likely to prejudice an investigation that could lead to the prosecution of an offence or proceedings before a court or tribunal.

New section 56 (Exemption – eligible data breach of more than 1 agency) provides that an agency need not comply with chapter 3A, part 3, division 2 (Notification) in relation to an eligible data breach where the breach is an eligible data breach of one or more other agencies which the agency is not required assess, and another agency is required to comply with chapter 3A, part 3, division 2 in relation to the data breach.

New section 57 (Exemption – agency has taken remedial action) provides that the agency need not comply with section 53 in relation to an eligible data breach to the extent the data breach is no longer likely to result in serious harm to any individual. This will apply where the agency takes action to mitigate the harm caused by the data breach and as result of the action taken serious harm is no longer likely to result, or there is no authorised access to, or disclosure of information for a data breach involving the loss of personal information.

New section 58 (Exemption – inconsistency with confidentiality provision) provides that an agency need not comply with chapter 3A, part 2, division 2 (Notification) in relation to an eligible data breach to the extent the compliance would be inconsistent with a provision of an Act or the Commonwealth or a State that prohibits or regulates the use or disclosure of the information.

New section 59 (Exemption – serious risk of harm to health or safety) provides that an agency need not comply with chapter 3A, part 2, division 2 (Notification) in relation to an eligible data breach to extent of compliance would create a serious risk of harm to an individual's health or safety. If an agency relies on the section, the agency must give notice to the Information Commissioner containing stated information.

New section 60 (Exemption – compromise to cybersecurity) provides that an agency need not comply with section 53 in relation to an eligible data breach if compliance is likely to compromise or worsen the agency's cybersecurity, or lead to further data breach of the agency. If an agency relies on the section, the agency must give a notice to the Information Commissioner containing stated information and must review the application of the exemption each month and give the Commissioner a summary of the review.

New section 61 (Information commissioner may direct agency to give statement and make recommendations), in chapter 3A, part 4 (Role of information commissioner), allows the Information Commissioner to direct an agency, if the Commissioner reasonably suspects a data breach of an agency may be an eligible data breach, to prepare and give a statement providing stated information, and may recommend that the agency notify individuals as if the suspected data breach were an eligible data breach in stated circumstances.

New section 62 (Functions), in chapter 3A, part 5, provides that the functions of an authorised officer are to monitor and investigate whether an occasion has arisen for the exercise of the Information Commissioner powers that relate to an agency's compliance with chapter 3A.

New section 63 (Appointment) provides that the Information Commissioner may, by instrument in writing, appoint an appropriately qualified person as an authorised officer.

New section 64 (Identity cards) provides that the Information Commissioner must issue an identity card to each authorised officer which complies with stated requirements.

New section 65 (Production or display of identity card) provides that an authorised officer must produce and display their identity card in exercising a power in relation to a person in the person's presence, other than when the person has entered a place under new section 67(1)(b), unless it is not practicable to comply.

New section 66 (Return of identity card) provides that the person must return their identity card to the Information Commissioner within 15 business days after their office as an authorised officer ends, unless the person has a reasonable excuse. Failure to comply is an offence with a maximum penalty of 10 penalty units.

New section 67 (General power to enter places occupied by agency), in division 2, provides for the circumstances in which an authorised officer may enter a place occupied by an agency. The agency must have consented to the entry (under new section 68) or the place must be the agency's place of business and is open for carrying on the business or otherwise open for entry.

New section 68 (Information commissioner must give written notice of entry) provides that the Information Commissioner must, by written notice containing stated information, ask the agency to the consent to an authorised officer entering a place in stated circumstances. If an agency's principal officer does not consent, an authorised officer may enter on a stated reasonable date at a stated reasonable time. If notice is given to an agency, the agency must take all reasonable steps to facilitate entry by an authorised officer on the date or time consented to or stated. Failure to comply is an offence with a maximum penalty of 100 penalty units.

New section 69 (General powers), in division 3 (powers of authorised officers after entering places) provides for powers of the authorised officer to require a person with the necessary skills or knowledge to demonstrate the data handling systems and practices, or inspect documents that is relevant to the systems policies and practices of the agency that relate to its compliance with chapter 3A and remain at the place for the time necessary to achieve the purpose of the entry.

New section 70 (Power to require reasonable help) provides that if an authorised officer enters a place occupied by an agency under section 67, the authorised officer may require a person to give the authorised officer reasonable help to exercise their power, but must give the person an offence warning.

New section 71 (Offence to contravene help requirement) provides that a person of whom a requirement is made under section 70(1) must comply with the requirement unless the person has a reasonable excuse. It will not be a reasonable excuse for a person not to comply if the document or information is required to be held or kept by the individual under this Act. Failure to comply is an offence with a maximum penalty of 100 penalty units.

New section 72 (Agency must keep register), in part 6 (Miscellaneous), requires an agency to keep a register of eligible data breaches of the agency. The register must include stated information for each eligible data breach and if it is not practicable to include it in the register, the agency must record it as soon as it is reasonably practicable to do so.

New section 73 (Agency must publish data breach policy) provides than an agency must prepare and publish a policy about how it will respond to a data breach, including a suspected eligible data breach. The policy must be published on an accessible agency website.

New section 74 provides for evidential immunity for individuals who give information to an authorised officer under sections 69(1) or 70(1). Evidence of the information, and other evidence directly or indirectly derived from the information, is not admissible against the individual in any proceeding to the extent it tends to incriminate the individual, or expose the individual to penalty, in the proceeding, unless it is about the false or misleading nature of the information or anything in which the false or misleading nature of the information is relevant evidence.

Clause 34 amends section 134 (Information commissioner not subject to direction) to remove a reference to section 137 which is omitted, and to provide that the Information Commissioner is not subject to direction by any person about the priority to be given to audits and privacy complaints, in addition to investigations and reviews which are already specified.

Clause 35 amends section 135 (Performance monitoring and support functions) to:

- include investigations (on the Information Commissioner's own initiative), if the Commissioner is satisfied on reasonable ground that an act or practice may contravene the privacy principle requirements or an agency's obligations under chapter 3A, as functions of the commissioner;
- include new functions of the Information Commissioner for monitoring and auditing relevant entities' compliance with the Act;
- include new functions related to QPP codes;
- update the reference to issuing guidelines to refer to new section 138;
- update terminology to refer to 'privacy principle requirements';
- make changes to the functions, consequential to the omission of chapter 3 of the IP Act,;

- include a new function reporting to the Speaker, if the Commissioner considers it appropriate, on the findings of a reportable matter (namely a review, investigation or audit) including reporting any recommendations to the relevant entity on the subject of the reportable matter.

Clause 36 amends section 136 (Decision-making functions) to provide that the functions of the Commissioner include waiving or modifying an obligation of agencies to comply with the privacy principle requirements, an obligation of an agency to comply with chapter 3A, part 2 or 3 or section 72 or 73.

Clause 37 omits section 137 (External review functions) which is no longer needed due to the omission of chapter 3 of the IP Act.

Clause 38 replaces section 138 (Guidelines under Right to Information Act) to provide that the Information Commissioner may issue a guideline about any matter relating to the Commissioner's functions. The section provides examples of guidelines that may be made and clarifies the relationship with the Information Commissioner's power to make guidelines under the RTI Act.

Clause 39 amends the heading for chapter 4, part 5 (Waiving or modifying privacy principles obligations in the public interest) to refer to 'particular obligations' rather than 'privacy principles obligation's. This reflects the amendments to section 157.

Clause 40 amends section 157 (Waiver or modification approval) to provide that a relevant entity may apply to the Information Commissioner for an approval that waives the privacy principle requirements, or for an agency, chapter 3A, part 2 or 3 or section 72 or 73. The clause also amends the section heading to reflect its content.

Clause 41 amends section 158 (Compliance notice) so that the Information Commissioner may give a relevant entity a compliance notice in relation to stated relevant obligations (currently compliance notices are limited to agencies for the privacy principles), and clarifies that it extends to acts or practices in contravention of a relevant obligation.

Clause 42 amends section 159 (Extension of time for compliance) so that it applies to a relevant entity that is given a compliance notice and such a relevant entity may ask the Information Commissioner to extend the time within which it must take the action stated in the notice.

Clause 43 amends section 160 (Agency must comply with notice) so that it applies to a relevant entity rather than being limited to an agency. The section heading is also amended.

Clause 44 amends section 161 (Application to Queensland Civil and Administrative Tribunal for review of decision to give compliance notice) so that it applies to a relevant entity rather than being limited to an agency.

Clause 45 amends section 162 (Parties to QCAT proceeding) so that the relevant entity given a compliance notice is a party to application to review the decision to give the notice and any review by QCAT of the decision.

Clause 46 amends section 163 (How QCAT may dispose of review) to make it clear that the decision subject to the review is a decision to give a relevant entity a compliance notice.

Clause 47 replaces section 164 (Meaning of *privacy complaint*) with new section 164 and new section 164A.

New section 164 (Meaning of *privacy complaint*) provides that a privacy complaint is a complaint by an individual about an act or practice engaged in by a relevant entity in relation to personal information that may be a breach of the relevant' entity's obligation to comply with the privacy principle requirements or, for an agency, chapter 3A, part 2 or 3. However, a privacy complaint does not include a complaint to the extent that it relates to stated types of personal information.

New section 164A (Response period for privacy complaints) provides that the response period for a privacy complaint made to a relevant entity is a period of 45 business days after the day the privacy complaint is received by the relevant entity, extended by any further specified period during which the relevant entity may continue to consider the privacy complaint in addition to the period of 45 business days. The relevant entity may continue to consider the privacy complaint after the period of 45 business days ends, provided that the relevant entity has asked for a further specified period and the complainant has not refused a request for an extension, the relevant entity has not received notice that the complainant has made a privacy complaint to the Information Commissioner or the further specified period requested ends.

Clause 48 amends section 166 (Requirements for privacy complaint) to clarify in the section heading that the section relates to complaints to the Information Commissioner; and to require that a complaint must give particulars of the act, or practice the subject of the complaint. The section also requires a complainant to have made a privacy complaint to the relevant entity under new section 166A before making a complaint to the Information Commissioner and either not consider the relevant entity's response to be adequate or not receive a response within the response period.

Clause 49 inserts new section 166A (Requirements for privacy complaint to relevant entity) which provides for new requirements for privacy complaints to a relevant entity. The complaint must be in writing, state an address to which the entity must respond to the complaint, give particulars of the act or practice the subject of the complaint, and be made within 12 months after the complainant becomes aware of the act or practice the subject of the complaint, subject to extension by the relevant entity. The section also provides that the entity must give reasonable help to the complainant to put the complaint in writing.

Clause 50 amends section 168 (Information commissioner may decline to deal with or to deal further with complaint) to provide that the Information Commissioner may decline to deal with a privacy complaint, or part of it, if 12 months have elapsed since the earlier of the last day of the response period for the complaint under new section 164A or the day the relevant entity responds.

Clause 51 inserts new section 173A (Confidentiality of mediation) which provides that things said or done in the course of mediation of a privacy complaint are not admissible in criminal, civil or administrative proceedings unless the complainant and the respondent for the complaint agree.

Clause 52 amends section 175 (Advice to parties) to provide that that written notice which must be given to the complainant and the respondent for a privacy complaint must advise that the complainant may ask the Information Commissioner to refer the privacy complaint to QCAT under section 175A.

Clause 53 inserts new section 175A (Complainant's request for referral to Queensland Civil and Administrative Tribunal) which provides that, within 20 business days after the date of the notice given under section 175, the complainant may, by written notice, ask the Information Commissioner to refer the privacy complaint to QCAT. The Information Commissioner may, if asked by the complainant, extend the period if the Commissioner is satisfied that doing so is reasonable in the circumstances. If the period is extended, the Information Commissioner must give a written notice to the complainant and the respondent for the privacy complaint stating the new period.

Clause 54 amends section 176 (Referral to Queensland Civil and Administrative Tribunal) to require the Commissioner to refer the privacy complaint to QCAT within 20 business days after receiving the written notice under section 175A.

Clause 55 amends section 178 (How QCAT may dispose of complaint) to amend the orders that QCAT may make after the hearing of a privacy complaint referred to QCAT. These may include an order that the breach the subject of the complaint, or part of the complaint, has been substantiated, together with one or more stated orders.

Clause 56 amends section 179 (Access – protection against actions for defamation or breach of confidence) to make consequential amendments to remove references to 'access authorised by a decision-maker' and 'giving of access' as a result of the omission of chapter 3. The provision also updates terminology to refer to 'privacy principle requirements'.

Clause 57 omits section 180 (Publication – protection against actions for defamation or breach of confidence) as a result of the omission of chapter 3.

Clause 58 replaces section 181 (Access – protection in respect of offences) to remove reference to access authorised by a decision-maker under chapter 3 and remove reference to document including a chapter 3 document. These references are no longer required due to the omission of chapter 3.

Clause 59 omits section 182 (Publication – protection in respect of offences) as a result of the omission of chapter 3.

Clause 60 amends section 183 (Protection of agency, information commission etc. from personal liability) to remove reference to a decision-maker under chapter 3 as a result of the omission of chapter 3.

Clause 61 amends section 185 (Unlawful access) to omit subsection (2) as a result of the omission of chapter 3.

Clause 62 amends section 186 (False or misleading information) to provide a new definition of 'official' for the purposes of the section which includes an authorised officer, and expand the scope of the offence by referring to officials.

Clause 63 replaces section 187 (Failure to produce documents or attend proceedings) to remove a reference to section 116 (which is omitted) and to clarify that it is a reasonable excuse for a person to fail to give information if complying with the requirement might tend to incriminate the person or expose the person to penalty unless information is in a document required to be kept by the person under the Act.

Clause 64 amends section 188 (Disclosure or taking advantage of information) to update language to be gender neutral and provide that a person who is or has been the Information Commissioner or member of staff of the OIC is not prevented from disclosing information where necessary to lessen or prevent a serious threat to the life, health or safety of an individual or to public health or safety.

Clause 65 omits chapter 7, part 1 (Archival documents) which is longer required due to the omission of chapter 3.

Clause 66 amends section 193 (Reports of information commissioner) to allow the Information Commissioner to make a report to the Speaker on matters relating to the outcome of a review, investigation, or audit of an agency or the performance of the Information Commissioner's functions.

Clause 67 replaces section 194 (Report to Assembly on Act's operation) to require the Information Commissioner to prepare a report on the operation of the Act for each financial year, which must include details of the matters prescribed by regulation and may be included as part of a report the Information Commissioner prepared under the RTI Act. The report must be given to the parliamentary committee, and the chair must table it within three sitting days after the committee receives it. An agency or Minister will be required to give the Information Commissioner the information prescribed by regulation about the operation of the Act in relation to that agency or Minister as soon as practicable after the end of each financial year.

Clause 68 amends section 195 (Functions of parliamentary committee) to remove the function relating to the statistical information for the report under the RTI Act. This is consequential to the omission of chapter 3.

Clause 69 amends section 196 (Power of person acting for another person) to remove reference to access or amendment applications and to move definitions of 'child' and 'parent', which are currently in chapter 3, to the section. These amendments are consequential to the omission of chapter 3.

Clause 70 inserts new section 196A (Information Commissioner may make preliminary inquiries) which provides that the Information Commissioner may make preliminary inquiries of any person for the purpose of determining whether to investigate an act or practice on the commissioner's own initiative or otherwise under section 135(1)(a)(ii).

Clause 71 amends section 197 (Power of information commissioner for compliance notices and privacy complaints) to expand its application so that it applies if the Information Commissioner is satisfied on reasonable grounds that a person has information relevant to: a review under section 135(1)(a)(i); an investigation under section 135(1)(a)(ii); an audit under section 135(1)(b)(iii); or preliminary inquiries the commissioner is making of the respondent for the privacy complaint under section 167. The section heading is also updated to reflect the expanded scope of the section.

Clause 72 replaces section 199 (Contents of prescribed written notice) which is no longer required due to the omission of chapter 3, with new sections 199 and 199A.

New section 199 (Exchange of information) allows the Information Commissioner to enter into an information-sharing arrangement with a prescribed agency. The information-sharing arrangement may only relate to information that assists the Information Commissioner and the prescribed agency perform its functions, and authorises the asking for, the receipt and disclosure of information despite another Act or law.

New section 199A (Corporations legislation displacement) provides that a regulation may declare a provision of the IP Act that applies in relation to a prescribed corporation (within the meaning of the Corporations Act that is declared under section 21(1)(c) to be a public authority for the IP Act) to be a Corporations legislation displacement provision for the purposes of section 5G of the Corporations Act. The regulation may be declared to apply in relation to the whole of the Corporations legislation or a particular provision of the Corporations legislation or all prescribed corporations or a particular prescribed corporation.

Clause 73 inserts new chapter 8, part 3 (Transitional provisions for *Information Privacy and Other Legislation Amendment Act 2023*) which contains new sections 215 to 225.

New section 215 provides definitions of ‘amendment Act’, ‘former’ and ‘former IP Act’ for the purposes of chapter 8, part 3.

New section 216 (Existing bound contracted service providers) provides that if, immediately before the commencement, an entity was a bound contracted service provider required to comply with former chapter 2, part 1 or 2 and part 3 under former chapter 36, these provisions continue to apply to the contracted service provider in relation to personal information it holds under the service arrangement and the act applies as if a reference to the privacy principle requirements were a reference to the requirement to comply with those provisions. A contracted service provider and agency may agree to vary the service arrangement to require the contracted service provider to comply with chapter 2, parts 1, and 2 and section 41, and if this occurs, section 216 stops applying.

New section 217 (Existing access and amendment applications) provides that the former IP Act continues to apply to applications or purported applications made under former chapter 3, but not finalised (as defined in the section) before the commencement. A note also alerts readers to section 206Q of the RTI Act.

New section 218 (Continued protection for giving access to or publishing chapter 3 documents) provides that if a chapter 3 document (within the meaning of the former IP Act) is accessed or published before the commencement or under section 217, former sections 179 and 181 continue to apply in relation to the authorising or the giving of access as if the amendment act had not been enacted. Former sections 180 and 182 also continue to apply in relation to the publication of a chapter 3 document as if the Amendment Act had not been enacted.

New section 219 (Delayed application of ch 3A to local governments) provides that chapter 3A does not apply to an agency that is a local government until the day that is one year after commencement.

New section 220 (Existing approvals under former s 157) provides that a waiver or modification approval given under former section 157 lapses on the commencement of this section.

New section 221 (Existing compliance notices under s 158) provides that an agency must comply with a compliance notice given to it by the Information Commissioner before the commencement where the time for compliance had not ended before the commencement.

New section 222 (Information commissioner may issue compliance notice for failure to comply with former IP Act) provides that the Information Commissioner may give a compliance notice under section 158 in relation to an act or practice if, before the commencement, an agency had done an act or engaged in a practice in contravention of a requirement to comply with the privacy principles under the former IP Act and the Information Commissioner had not yet given a compliance notice to the agency, and the act or practice also constitutes a contravention of the privacy principle requirements.

New section 223 (Privacy complaints about act or practice of relevant entity not yet made before commencement) provides that a privacy complaint that could have been made under former chapter 5, part 1 that had not been made immediately before commencement may be made under former chapter 5, which continues to apply in relation to the complaint as if the Amendment Act had not been enacted.

New section 224 (Privacy complaints made but not finalised before commencement) provides that former chapter 5 continues to apply in relation to a privacy complaint or apart of the privacy complaint that was made or referred to the Information Commissioner as if the Amendment Act had not been enacted. The section also states the circumstances in which the privacy complaint is considered finalised for the purposes of the section.

New section 225 (Continuation of sections 185 and 187 for chapter 3 documents) provides that a proceeding for an offence against former section 185 or 187 committed in relation to a chapter 3 document by a person before the commencement may be continued or started, and the person may be convicted of and punished for the offence, as if the Amendment Act, sections 61 and 63 had not commenced. This applies despite section 11 of the Criminal Code and does not limit section 20 of the *Acts Interpretation Act 1954*.

New section 226 (Report to Assembly on Act's operation) provides that new section 194 does not apply, and former section 194 continues to apply in relation to the financial year ending before the commencement if the report for the financial year has not been tabled in the Assembly under former section 194, as if the Amendment Act had not been amended.

Clause 74 replaces schedule 3 (Information Privacy Principles) and schedule 4 (National Privacy Principles).

Schedule 3 – Queensland Privacy Principles

New schedule 3 (Queensland Privacy Principles) sets out the QPPs, with which an agency, other than an APP entity, must comply. The QPPs generally align with the APPs in the Commonwealth Privacy Act, with some adaptations appropriate for Queensland agencies. Some of the APPs (and provisions of the APPs) apply only to organisations (as defined by the Commonwealth Privacy Act) or to certain Commonwealth agencies.

APPs (and provisions of the APPs) which are not relevant to the regulation of information privacy by Queensland agencies have not been adopted in the QPPs. Where an APP (or a provision of an APP) has not been adopted in the QPPs, the QPPs include a note referring to the relevant APP (or provision).

QPPs 7, 8 and 9 are not substantive QPPs but refer to Commonwealth APPs which are not relevant to the handling of information by Queensland public sector agencies. APP 7 regulates direct marketing. APP 8 regulates cross-border disclosure of personal information and APP 9 regulates the adoption, use or disclosure of government-related identifiers (for example, Medicare numbers and driver's licence numbers). Notes are included to alert readers where APPs in the Commonwealth Privacy Act have not been adopted in the IP Act.

Part 1 - Consideration of personal information privacy

1 QPP 1 - open and transparent management of personal information

The object of QPP 1 is to ensure agencies manage personal information in an open and transparent way.

Under QPP 1.2, an agency must take reasonable steps to implement practices, procedures and systems relating to the agency's functions and activities that will ensure compliance with the QPPs or a QPP code that binds the agency, and enable the agency to deal with inquiries or complaints from individuals about the agency's compliance with the QPPs and any QPP code binding the agency.

QPP 1.3 requires an agency to have a clearly expressed and up-to-date privacy policy (the QPP privacy policy) about the management of personal information by the agency.

QPP 1.4 sets out the information that must be included in the agency's QPP privacy policy. This information must include: the kinds of personal information the agency collects and holds; how the agency collects and holds personal information; the

purposes for which the agency collects, holds, uses and discloses personal information; how an individual may access personal information about the individual that is held by the agency, and seek correction of the information; how an individual may complain about a breach of the QPPs, or any QPP code that binds the agency and how the agency will deal with the complaint; whether the agency is likely to disclose personal information to entities outside Australia; if the agency is likely to disclose personal information to entities outside Australia, the countries in which the recipients are likely to be located (if it is practicable to state those countries in the policy).

Under QPP 1.5, an agency must take reasonable steps to make its privacy policy available to the public free of charge, and in an appropriate form. An example of how an agency may achieve this is by publishing its privacy policy on the agency's website.

Under QPP 1.6, if a person requests a copy of the agency's QPP privacy policy in a particular form, the agency must take reasonable steps to give the person a copy in that form.

2 QPP 2 - anonymity and pseudonymity

QPP 2.1 provides that individuals must have the option of not identifying themselves, or using a pseudonym, when dealing with an agency in relation to a particular matter.

Under QPP 2.2(a), QPP 2.1 will not apply, if, in relation to a matter, the agency is required or authorised under an Australian law, or a court or tribunal order, to deal with individuals who have identified themselves.

Under QPP 2.2(b), QPP 2.1 will also not apply, if, in relation to the matter, it is impracticable for the agency to deal with individuals who have not identified themselves or who have used a pseudonym.

Part 2 - Collection of personal information

3 QPP 3 - collection of solicited personal information

Under QPP 3.1, an agency must not collect personal information, other than sensitive information, unless the information is reasonably necessary for, or directly related to, one or more of the agency's functions or activities.

An editor's note advises that the equivalent APP includes a provision (APP 3.2) which applies only to certain private sector entities and has therefore no been adopted as a QPP.

QPP 3.3 provides for the collection of 'sensitive information', which is defined in schedule 5. An agency must not collect sensitive information about an individual unless:

- the individual consents to the collection of the information and the information is reasonably necessary for, or directly related to, one or more of the agency's functions or activities; or
- QPP 3.4 applies in relation to the information.

An editor's note advises that the equivalent APP includes a provision applying to certain private sector entities (APP 3.3(a)(ii)) and has not been adopted as a QPP.

QPP 3.4 applies in relation to sensitive information about an individual in the circumstances outlined in QPP 3.4 (a) to QPP 3.4 (d).

QPP 3.4(a) applies where the collection of the information is required or authorised under an Australian law or a court or tribunal order.

QPP 3.4(b) applies where a permitted general situation exists in relation to the collection of the information by the agency.

An editor's note refers the reader to schedule 4, part 1 (permitted general situations).

QPP 3.4(c) applies where the agency is a health agency and a permitted health situation exists in relation to the collection of the information by the agency

An editor's note refers the reader to schedule 4, part 2 (permitted health situations).

QPP 3.4(d) applies where the agency is a law enforcement agency and the agency reasonably believes that the collection of the information is reasonably necessary for, or directly related to, one or more of the agency's functions or activities.

The definition of 'law enforcement agency' is in schedule 5 (as amended by clause 75 of the Bill).

An editor's note advises that the equivalent APP includes a provision applying to the Commonwealth Immigration Department and non-profit organisations. These provisions are not relevant to the IP Act and are not included in QPP 3.4.

QPP 3.5 provides that an agency must collect personal information only by lawful and fair means.

QPP 3.6 provides that an agency must collect personal information about an individual only from the individual, unless QPP 3.6(a) or (b) apply.

QPP 3.6(a) applies where either:

- the individual consents to the collection of the information from someone other than the individual; or
- the agency is required or authorised under an Australian law, or a court or tribunal order to collect the information from someone other than the individual.

QPP 3.6 (b) applies where it is unreasonable or impractical for an agency to collect personal information about an individual only from the individual.

QPP 3.7 provides that QPP 3 applies to the collection of personal information that is solicited by an agency.

'Solicit', for schedule 3, is defined in schedule 5.

4 QPP 4 - dealing with unsolicited personal information

Under QPP 4.1, if an agency receives personal information and the agency did not solicit the information, the agency must, within a reasonable period after receiving the information, decide whether or not the agency could have collected the information under QPP 3 if the agency had solicited the information.

Under QPP 4.2 the agency may use or disclose the personal information for the purpose of making the decision under QPP 4.1.

QPP 4.3 provides that, if the agency decides it could not have collected the personal information, and if the information is not contained in a public record, the agency must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure the information is de-identified.

Under QPP 4.4, if QPP 4.3 does not apply in relation to the personal information, QPPs 5 to 13 apply in relation to the information as if the agency has collected the information under QPP 3.

5 QPP 5 - notification of the collection of personal information

QPP 5 sets out the obligation for an agency to ensure that an individual is notified of certain matters when it collects that individual's personal information.

QPP 5.1 provides that at or before the time, or if that is not practicable, as soon as practicable after an agency collects personal information about an individual, the agency must take steps, if any, that are reasonable in the circumstances to notify the individual of the matters mentioned in QPP 5.2 that are reasonable in the circumstances, or otherwise ensure that the individual is aware of those matters.

QPP 5.2 states the matters for QPP 5.1 are:

- the identity and contact details of the agency;
- if the agency collects the personal information from someone other than the individual, or the individual may not be aware that the agency has collected the personal information – the fact that the agency collects or has collected the information, and the circumstances of that collection;
- if the collection of the personal information is required or authorised under an Australian law, or a court or tribunal order—the fact that the collection is required or authorised, including the name of the Australian law, or details for the court or tribunal order, that requires or authorises the collection;
- the purposes for which the agency collects the personal information;
- the main consequences, if any, for the individual if all or some of the personal information is not collected by the agency;
- any other agency or entity, or the kinds of any other agencies or entities, to which the agency usually discloses personal information of the kind collected by the agency;
- that the QPP privacy policy of the agency contains information about how the individual may access the personal information about the individual that is held by the agency and seek the correction of the information;

- that the QPP privacy policy of the agency contains information about how the individual may complain about a breach of the QPPs, or any QPP code that binds the agency, and how the agency will deal with the complaint;
- whether the agency is likely to disclose the personal information to entities outside of Australia;
- if the agency is likely to disclose the personal information to entities outside of Australia—the countries in which the recipients are likely to be located if it is practicable to state those countries in the notification or to otherwise make the individual aware of them.

Part 3 – Dealing with personal information

6 QPP 6- use or disclosure of personal information

QPP 6 sets out the circumstances in which agencies may use or disclose personal information.

QPP 6.1 provides that if an agency holds personal information about an individual that was collected for a particular purpose (the primary purpose) the agency must not use or disclose the information for another purpose (the secondary purpose) unless:

- the individual has consented to the use or disclosure of the information; or
- QPP 6.2 applies in relation to the use or disclosure of the information.

QPP 6.2 provides that QPP 6 applies in relation to the use or disclosure of personal information about an individual if the circumstances in QPP 6.2 (a), (b), (c), (d), (e), (f) or (g) apply.

QPP 6.2(a) applies where the individual would reasonably expect the agency to use or disclose the information for the secondary purpose and the secondary purpose is

- if the information is sensitive information—directly related to the primary purpose; or
- if the information is not sensitive information—related to the primary purpose.

QPP 6.2(b) applies where the use or disclosure of the information is required or authorised under an Australian law or a court or tribunal order;

QPP 6.2(c) applies where a permitted general situation exists in relation to the use or disclosure of the information by the agency (see schedule 4, part 1 of the Bill);

QPP 6.2(d) applies where the agency is a health agency and a permitted health situation exists in relation to the use or disclosure of the information by the agency (see schedule 4, part 2).

QPP 6.2(e) applies if an agency reasonably believes that the use of disclosure of the information is reasonably necessary for one or more enforcement-related activities conducted by a law enforcement agency.

QPP 6.2(f) applies if the Australian Security Intelligence Organisation (ASIO) has asked the agency to disclose the personal information; an ASIO officer or employee authorised in writing by the director-general of ASIO has certified in writing that the

personal information is required in connection with the performance by ASIO of its functions, and the disclosure is made to an ASIO officer or employee authorised in writing by the director-general of ASIO to receive it.

QPP 6.2(f) reproduces an exception not included in the APPs but that is included in IPP 11(1)(ea) which permits disclosure by an agency to ASIO. While the APPs do not include a specific exception permitting disclosure of personal information to ASIO, the Privacy Act provides that acts and practices of intelligence agencies (including ASIO) are exempt from the Privacy Act.

QPP 6.2(g) applies if the use or disclosure is necessary for research, or the compilation or analysis of statistics, it does not involve the publication of all or any of the personal information in a form that identifies any individual, it is not practicable to obtain the express or implied agreement of each individual the subject of the personal information before the use or disclosure; and if the personal information is disclosed to another entity, the agency is satisfied on reasonable grounds that the relevant entity will not disclose the personal information to another entity. The does not correspond to an APP and is specific for Queensland agencies.

An editor's note alerts the reader that the QPPs do not contain an equivalent to APP 6.3 - APP 6.3 provides that an agency will be allowed to disclose biometric information or templates if the recipient is a law enforcement agency and the disclosure is conducted in accordance with the guidelines made by the Information Commissioner.

QPP 6.4 requires the agency to take reasonable steps to de-identify the information before using or disclosing the information under QPP 1 or QPP 2. This sub-principle reproduces a requirement in NPP 9(4) in the NPPs that applied to health agencies. QPP 6.4 provides for an equivalent requirement to APP 6.4 applying to health agencies which collect health information for certain research purposes under the permitted health situations in schedule 4, part 2 of the Bill. APP 6.4 provides that if an APP entity is an organisation and collects health information about an individual for certain research purposes under section 16B(2) of the Commonwealth Privacy Act (the permitted health situations), that entity must take such steps as are reasonable in the circumstances to de-identify that information before it uses or discloses the information under APP 6.1 or 6.2.

QPP 6.5 provides that if an agency uses or discloses personal information because it is reasonably necessary for an enforcement related activity conducted by, or on behalf of, a law enforcement agency, the agency must make a written note of the use or disclosure.

An editor's note alerts the reader that APP 6.6 and 6.7 have not been adopted. APP 6.6 applies to an APP entity that is a body corporate, which collects personal information from a related body corporate. QPP 6 does not include this provision.

APP 6.7 applies to organisations, not agencies. APP 6.7 provides that APP 6 does not apply to the use or disclosure of personal information for the purposes of direct marketing or to government related identifiers (because these matters are specifically dealt with elsewhere in the APPs). QPP 6 does not include this provision.

An editor's note alerts the reader that APP 7 has not been adopted into the IP Act as it applies to direct marketing by organisations. The editor's note also alerts the reader that QPP6 is relevant to the use or disclosure of personal information for the purposes of direct marketing.

An editor's note alerts the reader that APP 8 has not been adopted into the IP Act. Section 33 of the IP Act, which relates to the disclosure of an individual's personal information by an agency to an entity outside Australia, are included in the privacy principle requirements.

An editor's note alerts the reader that APP 9 has not been adopted into the IP Act as it applies to the adoption, use and disclosure of government-related identifiers (e.g. Medicare card numbers, tax file numbers) used by organisations.

Part 4 - Integrity of personal information

10 QPP 10 - quality of personal information

QPP 10 sets out the obligation for an agency to take reasonable steps to ensure that the personal information it collects, uses and discloses meets certain quality requirements.

QPP 10.1 provides than agency must take reasonable steps to ensure that the personal information the agency collects is accurate, up-to-date and complete.

QPP 10.2 provides that an agency must take reasonable steps to ensure the personal information the agency uses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

11 QPP 11-security of personal information

QPP 11 sets out an agency's obligations relating to the protection and destruction or de-identification of personal information it holds.

QPP 11.1 requires an agency which holds personal information to take reasonable steps to protect personal information from misuse, interference or loss, and from unauthorised access, modification or disclosure.

QPP 11.2 provides that, if an agency holds personal information about an individual and the agency no longer needs the information for a purpose for which the information may be used or disclosed by the agency under the QPPs, and the information is not contained in a public record, and the agency is not required under an Australian law, or a court or tribunal order, to retain the information, the agency must take reasonable steps to destroy the information or to ensure the information is de-identified.

Part 5 - Access to, and correction of, personal information

12 QPP 12 - access to personal information

QPP 12.1 provides that if an agency holds information about an individual, the agency must, on request by the individual, give the individual access to the information.

QPP 12.2 provides that if an agency is required or authorised to refuse to give the individual access to the personal information under the RTI Act, or another law in force in Queensland which provides for access by people to documents, then, the agency is not required to give access to the extent to the agency is required or authorised to refuse to give access.

An editor's note alerts the reader that QPP 12 does not include provisions equivalent to APP 12.3 to 12.10.

13 QPP 13 - correction of personal information

QPP 13.1 provides that if an agency holds personal information about an individual, and either the agency is satisfied that having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading, or the individual requests the agency to correct the information, the agency must take reasonable steps to correct the information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading.

An editor's note alerts the reader that QPP 13 does not include provisions equivalent to APP 13.2 and 13.3.

If an agency refuses to correct personal information in response to an individual's request, QPP 13.4 will provide a mechanism for individuals to request that a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading be associated with the information. The agency must take reasonable steps to associate the statement with the information so that it is apparent to users of the personal information.

An editor's note alerts the reader that APP 13.5 is noted adopted.

QPP 13.6 provides that an agency need not comply with QPP 13.1 in relation to a request made to the agency to correct personal information if the agency is required or authorised to refuse to correct or ament the information under the RTI Act or another Act regulating the amendment of information. QPP 13.6 applies in relation to Queensland agencies and does not correspond to an APP.

Schedule 4 – Permitted general situations and permitted health situations

New schedule 4 (Permitted general situations and permitted health situations) describes permitted general situations and permitted health situations for schedule 5.

Part 1 – Permitted general situations

Section 1 (Collection, use or disclosure) provides that a permitted general situation exists in relation to the collection, use or disclosure by an agency of personal information. In order for the situation to apply, one following must apply:

- it is unreasonable or impracticable to obtain the individual's consent, and the agency reasonably believes that the collection, use or disclosure is necessary to

lessen or prevent a serious threat to the life, health or safety of an individual or to public health or safety;

- the agency has reason to suspect that unlawful activity or misconduct of as serious nature, that the relates to the agency's functions or activities, is being or may be engaged in and the agency reasonably believes that the collection, use or disclosure is necessary to take appropriate action;
- the agency reasonably believes that the collection, use or disclosure is reasonably necessary to assist an entity to locate a person who has been reported as missing, and complies with a guideline in effect under chapter 3, part 2;
- the collection use or disclosure is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim; or
- the collection, use or disclosure is reasonably necessary for the purposes of a confidential alternative dispute resolution process.

Part 2 – Permitted health situations

Section 2 (Collection – provision of a health service) specifies two permitted health situations in relation to the collection of health information about an individual by a health agency. In the first situation, collection of the information must be necessary to provide a health service to the individual, and either be authorised or required under an Australian law, or the individual would reasonably expect to collect the information for that purpose. In the second situation, the information is a family or social medical history or other relevant information about the individual or another individual, necessary for providing a health service to the individual or another individual, and is collected from the person receiving the health service or a responsible person for the individual.

Section 3 (Collection – research etc.) specifies a permitted health situation in relation to the collection of health information about an individual by a health agency. Collection of the information must be necessary for research or analysis of statistics relevant to public health or public safety or compilation or analysis of statistics relevant to public health or public safety, or the management, funding or monitoring of the health service. It must also be the case that the purposes cannot be served by collection of information that does not identify the individual or from which the individual's identity cannot be reasonably ascertained, it is impracticable for the health agency to seek consent to the collection, and the information is collected as authorised or required under Australian law, by a designated person with the approval of the relevant chief executive or in accordance with relevant chief executive's guidelines.

Section 4 (Use or disclosure – research etc.) provides that a permitted health situation exists in relation to use or disclosure of health information about an individual by a health agency. Use or disclosure of the information must be necessary for research or compilation of statistics or analysis of statistics relevant to public health or public safety. It must also be the case that it is impracticable for the health agency to obtain the individual's consent before the use or disclosure, the use or disclosure is conducted in accordance with the relevant chief executive of the health department for this purpose. For disclosure, the health agency must also reasonably believe that the entity receiving the health information will not disclose the health information or personal information derived from the health information.

Section 5 (Disclosure – responsible person for an individual) provides that a permitted health situation exists in relation to disclosure of health information about an individual by a health agency that provides a health service to the individual. The recipient of the information must be a responsible person for an individual who is physically or legally incapable of giving consent to the disclosure or physically cannot communicate consent. A health professional providing the health service for the organisation must be satisfied the disclosure is necessary to provide appropriate care or treatment of the individual or the disclosure is made for compassionate reasons. The disclosure must not be contrary to any wish expressed by the individual of which the health professional is aware, or could reasonably be expected to be aware. The disclosure is also limited to the extent necessary for the stated purposes.

Clause 75 amends schedule 5 (Dictionary) to omit definitions which are no longer required, insert new definitions relevant to new and amended provisions, and amend the definitions of 'consent', 'health information', 'health professional,' and 'law enforcement agency'.

Part 4 Amendment of Ombudsman Act 2001

Clause 76 provides that Part 4 amends the *Ombudsman Act 2001*

Clause 77 amends s 16 (What Ombudsman may not investigate) to provide that the ombudsman must not investigate administrative action taken by the Information Commissioner in the performance of the commissioner's functions under section 135 or section 136 of the IP Act.

Part 5 Amendment of Right to Information Act 2009

Clause 78 provides that Part 5 amends the RTI Act and provides a note alerting readers to the amendments in schedule 1, part 2.

Clause 79 amends the long title of the RTI Act to include reference to rights 'relating to' government and other information. This reflects the inclusion of matters from chapter 3 of the IP Act, including rights to amendment of personal information, into the RTI Act.

Clause 80 amends section 3 (Object of Act) to add a primary object of the Act to include the giving of the right of amendment of personal information in the government's possession or under the government's control unless, on balance, it is contrary to the public interest to allow the information to be amended. The amendment is consequential to the omission of chapter 3 of the IP Act and the inclusion of access applications for an individual's personal information into chapter 3 of the RTI Act and amendment applications for an individual's personal information in new chapter 3A of the RTI Act.

Clause 81 replaces section 4 (Act not intended to prevent other publication or access) and section 5 (Relationship with other Acts requiring publication or access) with new sections 4 (Act not intended to prevent other publication, access or amendment) and 5 (Relationship with other Acts requiring access, amendment or publication). These new sections incorporate content from replaced sections 4 and 5 of the RTI Act and omitted sections 4 and 5 of the IP Act so that the sections are expanded to also deal with access

and amendment applications for an individual's personal information. Terminology is also updated to reflect changes to the IP Act which refers to 'privacy principle requirements' rather than privacy principles.

Clause 82 replaces section 8 (Relationship with Information Privacy Act) to provide that the Information Privacy Act is intended to operate subject to provisions of the RTI Act regulating the accessing and amendment of personal information. A note refers to section 7 of the IP Act.

Clause 83 amends section 14 (Meaning of *agency*) to amend the note under section 14(2) to alert readers to the effect of section 26 and new section 78G.

Clause 84 amends section 16 (Meaning of *public authority*) to: provide that an entity declared to be a public authority for the RTI Act must be declared under new section 16A; and provide that a public authority does not include an entity established by letters patent.

Clause 85 inserts new section 16A (Declaration of entities to be public authorities) to provide that an entity may be declared by regulation to be a public authority for the RTI Act. To recommend the making of a regulation declaring an entity to be a public authority, the Minister must be satisfied that the entity is: supported directly or indirectly by government funds or other government assistance; the entity is an entity over which government is in a position to exercise control; or is established or is given public functions under an Act. The Minister must also consider it to be in the public interest for the entity to be prescribed as a public authority, having regard to stated matters. The section also provides that an entity may be declared by regulation to be a public authority in relation to only part of the entity's functions.

Clause 86 replaces section 18 (Meaning of *processing period, revision period* and *transfer period*) with new section 18 (Meaning of *processing period*) which provides for a single definition of 'processing period' for an access or amendment application to an agency or Minister. The processing period is a period of 25 business days from the 'valid application day' on which the application complies with all relevant application requirements for the application, extended by each additional period for a stated circumstance. The stated circumstances have been modified to:

- include extensions for the prescribed consultation period under new section 78O;
- provide that the processing period is extended by five business days if the only address to be sent notices given by the applicant, by the valid application day (on which an access or amendment application complies with all relevant application requirements), is a postal address;
- provides for the period to be extended by a relevant further period if the agency or Minister asks the applicant for a further specified period under section 18(2));
- provide that where an applicant is given a charges estimate notice (other than a charges estimate notice stating that charges will be waived) the additional period will end on the earlier of the day the applicant confirms an application or a changed application, or the day the applicant is given notice of a decision to waive charges.

The section also inserts a new definition of 'valid application day' for an access or amendment application as being the day on which the application complies with all relevant application requirements under section 33(8) or 78K(8).

Clause 87 inserts new Chapter 1, part 3 (Effect of publication by Cabinet on public interest immunity) into the RTI Act, which contains new section 18A. New section 18A applies in relation to a decision being made in a proceeding or process about whether a common law or statutory rule prevents the production or disclosure of information in connection with Cabinet because the production or disclosure would be contrary to the public interest. In the making of the decision, the following matters must be disregarded in assessing the public interest:

- the publication by Cabinet of any other information contained in the document that contains the information;
- the publication by Cabinet of any other Cabinet information; and
- a decision by Cabinet to officially publish Cabinet information on a regular basis.

The section defines 'Cabinet information' as information contained in a document mentioned in Schedule 3, section 2(3) of the RTI Act, and 'proceeding or process' includes any extra-curial proceeding, or inquisitorial or investigative process carried out under an Act, and provides examples of this.

New section 18A is intended to require the existence of the proactive release 'scheme' to be disregarded in deciding claims of public interest immunity in proceedings or processes, so that the administrative proactive release of Cabinet documents is not intended to, and does not abrogate or derogate from, the public interest privilege that previously inhered in Cabinet documents, but for the 'scheme'. It is also intended that the publication of some information in a Cabinet document (which would otherwise be subject to public interest immunity) does not affect the application of public interest immunity to other information contained in the document.

Clause 88 replaces section 21 (Requirement for publication scheme) to include new stated requirements for a publication scheme that must be published by an agency, other than a prescribed entity under amended section 16. The agency must, as far as it is reasonably practicable, publish the scheme on an accessible agency website, or if not reasonably practicable to publish part of the scheme in that way, publish information about how a person may access that part. The scheme must publish information about the agency that is prescribed by regulation to the extent the information is held by the agency. There will no longer be guidelines published by the Minister on the Minister's website concerning the publication scheme.

Clause 89 inserts new section 22A (Civil liability of Minister for disclosing information). Section 22A(1) provides that a Minister does not incur civil liability as a result of, or in connection with, disclosing information under a publication scheme or other administrative scheme in good faith. The section includes publishing information on a department's website, and official publication by a decision of Cabinet of information contained in a Cabinet document as examples of disclosing information. New section 22A(1) provides that if section 22(1) prevents liability attaching to the Minister, the liability attaches instead to the State. A note refers readers to section 269

of the *Public Sector Act 2002* in relation to the civil liability of prescribed persons engaging in conduct in an official capacity.

New section 22A intends to protect Ministers from civil liability for actions undertaken in good faith in relation to the proactive release of Cabinet documents, similar to that afforded to public servants under the *Public Sector Act 2022*.

Clause 90 amends section 24 (Making access application) to:

- replace the requirement for an access application to be in the approved form with a requirement for it to be in writing, but also continue to allow it to be in the approved form;
- remove requirements to state whether access is sought for the benefit or use of the document by the applicant or another entity and, if applicable, to name the other entity;
- remove the requirement for evidence of the identity for an agent acting for an applicant to be provided;
- remove the requirement for evidence of identity for the application and evidence of the agent's authorisation for an application for access to a document containing personal information of the applicant to be provided within 10 business days after making the application, but rather treat this on the same basis as other application requirements;
- provide that no application fee is payable for an application by an individual for access to a document if the only document applied for contains the applicant's personal information, and if an application fee is paid for such an application it must be refunded as soon as practicable.

Clause 91 amends section 26 (Access application may not be made to commissioner) to include that an access application cannot be made or transferred to the OIC in addition to the Information Commissioner, the RTI commissioner or the Privacy Commissioner, and provide that the making or transfer of an access application to the OIC is not prohibited if an access application was made to the OIC by a person who is or was a staff member of the OIC in relation to the person's personal information.

Clause 92 amends section 32 (Application outside scope of Act) to:

- make the section apply where a person makes an application, rather than where they purport to make an application;
- specify that part of an application may be decided under the section, and provide that the entity must consider the part of an application that is not subject to a decision under the section;
- make consequential amendments to reflect the changes to section 26;
- provide that an entity must give prescribed written notice of a decision to the applicant within 25 business days after the application or part application is received; and
- insert a note alerting readers to the effect of section 119(2), section 1(a) in schedule 4A and relevant definitions in schedule 5.

Clause 93 amends section 33 (Noncompliance with application requirement) to:

- clarify that for subsection (3), the Agency or Minister must consult with an applicant with a view to making any changes or doing any other thing necessary

to make an application in a form complying with all relevant application requirements, including for example, by paying the application fee;
- require the agency or Minister to provide advice and help, to the extent that it would be reasonable to expect the agency or Minister to do so, to help the applicant to make an application in a form complying with all relevant application requirements; and
- make consequential amendments to reflect changes to section 24 and numbering changes.

Clause 94 omits section 34 (Application for personal information) which concerns access applications that could have been made under the IP Act. This section is no longer required due to the omission of chapter 3 of the IP Act.

Clause 95 amends section 35 (Longer processing period) to omit section 35(4) and the note under it. This is consequential to amendments made to section 18.

Clause 96 amends section 36 (Schedule of relevant document and charges estimate notice) to:
- remove references to schedules of relevant documents;
- remove the requirement to provide a charges estimate notice if a processing charge or access charge is not payable in relation to an application;
- provide that an applicant is taken to have withdrawn their access application if they do not confirm or withdraw a narrowed access application in stated circumstances;
- make consequential changes to the details that need to be included in a charges estimate notice, and other consequential changes.

Clause 97 amends section 38 (Transfer of application) to:
- provide than an 'application' includes a purported application for the purposes of the section;
- provide for modified application of the section if an application is made to an agency for access to two or more documents where at least one of those documents is in another agency's possession;
- clarify the wording in sections 38(5) and (6) in relation to documents that do not contain personal information of the applicant;
- make changes to numbering.

Clause 98 amends section 43 (Previous application for same documents) to remove references to a first access application that an applicant makes under the IP Act, remove references to an internal review, an external review or a proceeding under the IP Act, make consequential amendments in view of the amendments to section 36 of the RTI Act and make consequential amendments to numbering.

Clause 99 amends section 46 (Deemed decision on access application) to clarify that refunds of application fees under the section are only relevant for an application for which the applicant paid an application fee.

Clause 100 amends section 49 (Contrary to public interest) to clarify that for subsection (3), an agency or Minister may identify any factor that is irrelevant to deciding whether, on balance, disclosure of the information would be contrary to the
public interest that applies in relation to the information (an irrelevant factor), including, for example, any factor mentioned in schedule 4, part 1..

Clause 101 amends section 54 (Notification of decision and reasons) to remove reference to section 78 (which is omitted) and specify additional details that must be stated in a prescribed written notice to an applicant for an access application which is subject to deletion of personal information of a child under section 75A or the deletion under section 75B of relevant healthcare information of the applicant.

Clause 102 omits section 78 (Disclosure logs – departments and Ministers). This section is no longer required as departments and Ministers will be subject to general requirements in amended section 78A.

Clause 103 amends section 78A (Disclosure logs – other agencies) so that it applies to an agency or Minister, including the section heading, and reflects the changes to section 78B.

Clause 104 amends section 78B (Requirements about disclosure logs) to omit the requirement in section 78B(1) for an agency to comply with guidelines published by the Minister, make consequential amendments to reflect the omission of section 78, and expand the section's application to an agency or Minister.

Clause 105 inserts new chapter 3A (Amendment of personal information) which contains new sections 78C to 78W. This is consequential to the omission of chapter 3 of the IP Act.

New section 78C (Right to amend personal information in particular documents) provides for a right of an individual to amend documents of an agency or Minister to the extent they contain the individual's personal information if they are inaccurate, incomplete, out of date or misleading. This generally reflects the content in section 41 of the IP Act, but the notes are updated to reflect the amended sections.

New section 78D (Other ways of amending personal information) provides that personal information may be amended other than by application under chapter 3A. This is generally consistent with the content of section 42 of the IP Act, as it relates to amendment of personal information, which is omitted..

New section 78E (Making amendment application) provides for an individual to apply to an agency or Minister for amendment of any part of the individual's personal information contained in the document that the individual claims is inaccurate, incomplete out of date or misleading. This contains similar content to section 44 of the IP Act which is omitted, but is adjusted to:

- replace the requirement for an access application to be in the approved form with a requirement for it to be in writing, but also continue to allow it to be in the approved form;
- remove the requirement for evidence of the identity for an agent acting for an applicant to be provided;

- remove the reference to evidence of identity for the application and evidence of the agent's authorisation for an application for access to a document containing personal information of the applicant to be provided within 10 business days after making the application, but rather treat this on the same basis as other application requirements.

New section 78F (Making amendment applications for children) provides for an amendment application to be made for a child by the child's parent. This is similar to the content of section 45 of the IP Act (which is omitted), as it relates to amendment applications, with references in the note adjusted to refer to the equivalent provisions in the RTI Act rather than the IP Act, and definitions of 'child' and 'parent' to refer to section 25 of the RTI Act.

New section 78G (Amendment application may not generally be made to OIC etc.) provides that amendment applications may not be made or transferred to the OIC, the Information Commissioner, the RTI commissioner or the Privacy Commissioner, and provides that the making or transfer of an amendment application to the OIC is not prohibited if an amendment application was made to the OIC by a person who is or was a staff member of the OIC. This is similar to section 46 of the IP Act, which is omitted, but has been adjusted for consistency with section 26 of the RTI Act.

New section 78H (Decision-maker for application to agency) provides for who must deal with an amendment application to an agency, and provides for delegation and cross delegation of the power to deal with the application. This reflects the content of section 50 of the IP Act, as it relates to amendment applications, which is omitted, with references in the note also adjusted to refer to the equivalent provisions in the RTI Act rather than the IP Act.

New section 78I (Decision-maker for application to Minister) provides that an amendment application to a Minister may be dealt with by the person the Minister directs. This reflects the content of section 51 of the IP Act, as it relates to amendment applications, which is omitted, with references in the note also adjusted to reflect equivalent provisions in the RTI Act rather than the IP Act.

New section 78J (Application outside the scope of Act) provides for how an amendment application or part of an amendment application that an entity decides is outside the scope of the RTI Act is dealt with. This reflects the content of section 52 of the IP Act, as it relates to amendment applications, which is omitted, but makes additional amendments for consistency with section 32 of the RTI Act.

New section 78K (Non-compliance with application requirement) provides for how a purported amendment application which does not comply with all the relevant application requirements is to be dealt with by an agency or Minister. This reflects the content of section 53 of the IP Act, as it relates to amendment applications, which is omitted, but also include additional amendments for consistency with section 33 of the RTI Act.

New section 78L (Transfer of amendment application) provides for the agency to which an amendment application has been made to transfer the application to another agency. This reflects the content of section 57 of the IP Act, as it relates to amendment

applications, which is omitted, but has been updated for consistency with section 38 of the RTI Act.

New section 78M (Pro-amendment bias in deciding to deal with applications) specifies the Parliament's intention concerning the pro-amendment bias in deciding to deal with amendment applications. This reflects the content of section 58 of the IP Act, as it relates to amendment applications, which is omitted, with references updated to refer section 78N of the RTI Act.

New section 78N (Effect on agency's or Minister's functions) provides for stated circumstances in which an agency or Minister may refuse to deal with an amendment application (or multiple amendment applications by the applicant) due to an effect on the performance of the agency's or Minister's functions. This broadly reflects the content of section 60 of the IP Act, which is omitted. Amendment applications ill only be considered together if there are two or more applications by the same applicant for the purposes of applying the section.

New section 78O (Prerequisites before refusal because of the effect on functions) provides for the circumstances in which an agency or Minister may refuse to deal with an amendment application under section 78O. This reflects the content of section 61 of the IP Act, as it relates to amendment applications, which is omitted, with references updated to refer to section 78N of the RTI Act.

New section 78P (Previous application for same documents) provides that an agency may refuse to deal an amendment application in stated circumstances where there has been a previous amendment application for the same documents. This reflects the content of section 63 of the IP Act, as it relates to amendment applications, which is omitted, however, the section is also has updated references to equivalent sections in the RTI Act.

New section 78Q (Considered decision on amendment application) provides for requirements for an agency of Minister to make a considered decision about an amendment application and provide written notice to the person. This reflects the content of section 70 of the IP Act, which is omitted, with a reference updated to refer to section 78T of the RTI Act.

New section 78R (Deemed decision on amendment application) specifies when an agency or Minister is taken to have made a deemed decision refusing to amend a document. This reflects the content of section 71 of the IP Act, which is omitted.

New section 78S (Grounds on which amendment may be refused) specifies grounds on which amendment of a document may be refused. This reflects the content of section 72 of the IP Act, which is omitted.

New section 78T (Notification of decision and reasons) provides for notification by an agency or Minister of a decision on an amendment application. This reflects the content of section 73 of the IP Act, which is omitted.

New section 78U (Amendment of document by alteration or notation) provides for amendment of a document by alteration or requirements for notation to information. This reflects the content of sections 74 and 75 of the IP Act, which are omitted.

New section 78V (Particular notations required to be added) provides requirements for particular notations if the agency or Minister refuses to amend a document in stated circumstances. This reflects the content of section 76 of the IP Act, which is omitted, with section and part references updated to refer to relevant sections of the RTI Act.

Clause 106 inserts a heading to new chapter 3B (Review and other matters).

Clause 107 renumbers chapter 3, part 8 as chapter 3B, part 1 (Internal review).

Clause 108 amends section 79 (Definitions for part 8) to amend the section heading and refer to the new definition of 'internal review processing period' in section 82A.

Clause 109 amends section 80 (Internal review) to refer to chapter 3B, part 2 and update references to include relevant provisions concerning amendment applications. The clause also amends section 80 to provide that in addition to making a new decision as if the reviewable decision had not been made, an internal reviewer may review whether the agency or Minister has taken reasonable steps to identify and locate documents applied for by the applicant.

Clause 110 amends section 81 (Decisions that may not be reviewed) to expand the scope of the section to include amendment applications.

Clause 111 inserts new sections 82A (Meaning of *internal review processing period*) which provides that the internal review processing period, for an internal review application, is the period of 20 business days from the valid application day for the application, extended by each additional period for a stated circumstance. The additional periods are: five business days if the only address to be sent notices given by the applicant, by the valid application day (on which an access or amendment application complies with all relevant application requirements), is a postal address; 10 business days if the application involves consultation with a relevant third party; and a another stated period if the agency or Minister ask the applicant for a further specified period under section 82A(2).

The section also inserts a new definition of 'valid application day' for an internal review application as the day on which the application complies with all relevant application requirements under section 82.

Clause 112 amends section 83 (When internal review application to be decided) to provide that if an agency or Minister does not decide an internal review application and notify the applicant of the decision within the internal review processing period, the agency's principal officer or the Minister is taken to make a decision affirming the decision.

Clause 113 renumbers the heading for chapter 3, part 9 (External review) as chapter 3B, part 2 (External review).

Clause 114 inserts new sections 86A and 86B.

New section 86A (External review during processing period) applies if an agency or Minister has asked the applicant for an access or amendment application for a further specified period to consider the application under section 18(2), the processing period for the application disregarding the further specified period has ended, the further specified period has not ended and the agency has not given the applicant written notice of a decision on the application. The section provides that the applicant may apply for external review as if the processing period for the application does not include the further specified period and the agency's principal officer or Minister has made a deemed decision which the applicant has been given written notice of at the end of that processing period. The section specifies what occurs if the applicant applies for external review and the Act will apply in relation to the deemed decision in the same way as it applies to a deemed decision under section 46 or 78R, subject to stated changes.

New section 86B (External review during internal processing period) applies if an agency or Minister has asked an applicant for internal review for a further specified period to consider the applicant's internal review application under section 82A(2), the internal review processing period for the application disregarding the further specified period has ended, the further specified period has not ended and the agency has not given the applicant written notice of a decision on the application. The section provides that the applicant for internal review may apply for external review as if the processing period for the application does not include the further specified period and the agency's principal officer or Minister has made a decision affirming the original decision at the end of the internal review processing period which the applicant has been given written notice of at the end of that processing period. The section specifies what will occur if the applicant applies for external review, and the Act will apply in relation to the decision taken to have been made in the same way it applies to a decision under section 83(2), subject to stated changes.

Clause 115 amends section 93 (Applications where decision delayed) to expand the scope of the section to include amendment applications and to make it clear that the Information Commissioner may allow an agency or Minister further time to deal with the access or amendment application subject to conditions which may include a condition that the applicable access charge must be reduced or waived.

Clause 116 inserts new section 94A (Agency or Minister authorised to give access to documents) to provide that if an agency or Minister agrees to give access to a document or part of a document, to a participant in an external review, the agency or Minister is authorised to give access to the document or part to the participant, and the external review continues as if the review did not apply in relation to the document or part.

Clause 117 replaces section 102 (Requiring a search) to provide that in the conduct of an external review of a relevant reviewable decision, the information commissioner may require the agency or Minister to conduct a particular search, or to conduct searches, for a document. Relevant reviewable decision is defined as a reviewable decision mentioned in section 1(e), (h) or (k) of schedule 4A.

Clause 118 amends section 105 (Additional powers) to expand the powers that the Information Commissioner has in the conduct of an external review apply to amendment applications.

Clause 119 inserts new section 105A (Referral of particular documents relating to external review to agency or Minister) to allow the Information Commissioner, on external review of a decision relating to an access application and after consulting with the agency or Minister, to refer a document the Commissioner has become aware of to an agency or Minister if the Commissioner believes the document may not have been considered by the agency or Minister in making the decision that is the subject of the external review. To exercise the power, the Commissioner must consider referral of the document be a more efficient and effective way for a decision to be made about access to the document than the Commissioner making the decision, and must consider it reasonably likely that the agency would be able to make a decision about whether access is to be given to the document that is satisfactory to the access applicant. On the referral, a new access application is taken to have been made by the applicant on the day of the referral, and the external review continues as if the review did not apply in relation to the document. No application fee or other charges are payable by the access applicant in relation to that new access application, and evidence of identity and evidence of agent's authorisation (if the same agent is acting) need not accompany the new application.

Clause 120 amends section 107 (Information commissioner to ensure proper disclosure and return of documents) to add a relevant third party under section 107A to the list of people to whom the Commissioner is permitted to disclose a document which is the subject of the decision being reviewed.

Clause 121 inserts new section 107A (Information commissioner may give document to third party to obtain views) to permit the Information Commissioner to give a relevant third party access to a document that is the subject of an external review where disclosure of the document may reasonably be expected to be of concern to that third party. The Information Commissioner may give access to the document to obtain the third party's views about whether the document is a document to which the RTI Act does not apply or the information is exempt information or contrary to public interest information, and may inform the applicant that if the Commissioner decides, on the external review, to give access to the document, access may also be given to the document under a disclosure log. If the disclosure may reasonably be expected to be of concern to a third party but for the fact that the person is deceased, access may be given to the person's representative as if they were the relevant third party. The commissioner must notify the agency or Minister for the decision about the giving of the access.

Clause 122 amends section 110 (Decision on external review) to add that, after the Information Commissioner has conducted an external review of a decision, the Commissioner may make a written decision setting aside the decision and giving a direction under new section 110A.

Clause 123 inserts new section 110A (Direction to decide whether access to be given) which applies in relation to an external review of a relevant decision (as defined in the section) made by an agency or Minister in relation to an access application if the Information Commissioner:

- would otherwise have decided to set aside the relevant decision and make a decision in substitution under section 110(c);
- believes it would be more efficient and effective for the agency or Minister to consider whether access is to be given to the subject documents than to make a decision in substitution; and
- believes that if the agency or Minister were to consider whether access is to be given to the subject documents, it is reasonably likely the agency or Minister would be able to make a decision that is satisfactory to the access applicant.

The Information Commissioner may, after consulting with the agency or Minister about stated matters, set aside the relevant decision and notify the agency or Minister that the decision has been set aside and direct the agency or Minister to decide whether access is to be given to the subject documents as if the ground for making the relevant decision did not apply in relation to the documents. A new access application is taken to have been made on the day that is 21 business days after the Information Commissioner gives notice to the agency or Minister, no application fee is payable and evidence of identity and evidence of agent's authorisation (if the same agent is acting) need not accompany the new application.

Clause 124 amends section 113 (Disciplinary action) to provide that the section applies where there is evidence that a person subject to a direction of a Minister under section 78I relating to amendment applications, fix a minor drafting issue and make consequential amendments in view of the changes to section 16 and the insertion of new section 16A.

Clause 125 replaces the heading for chapter 3, part 10 (Vexatious applicants) to refer to chapter 3B, part 3.

Clause 126 amends section 114 (Vexatious applicants) to expand the scope of the section to apply to amendment actions and amendment applications.

Clause 127 renumbers chapter 3, part 11 to refer to chapter 3B, Part 4 (References of questions of law and appeals).

Clause 128 amends section 119 (Appeal to Queensland Civil and Administrative Tribunal on a question of law) to provide that a person affected by a judicial function decision may appeal to the appeal tribunal against a judicial function decision and to require a notice of appeal for such a decision to be served on the entity that made the decision. The amendments also clarify that the participants in an external review, other than the Information Commissioner, are parties to the appeal and remove reference to the appeal being by way of rehearing.

Clause 129 amends section 131 (Performance monitoring functions) to omit reference to chapter 3 of the IP Act which is omitted.

Clause 130 amends section 178 (Failure to produce documents or attend proceedings) to clarify that it is a reasonable excuse for a person to fail to give information or produce a document if would tend to incriminate the person or expose the person to a penalty.

Clause 131 amends section 179 (Disclosure or taking advantage of information) to use gender neutral language and provide that a person who is or has been the Information Commissioner or member of staff of the OIC is not precluded from disclosing information where necessary to lessen or prevent a serious threat to the life, health or safety of an individual or to public health or safety.

Clause 132 amends section 184 (Reports of Information Commissioner) to provide that the Information Commissioner may make a report to the Speaker on matters relating to the performance of the commissioner's functions, including matters relating to a particular external review.

Clause 133 replaces section 185 (Report to Assembly on Act's operation) to provide that an agency or Minister must give the Information Commissioner information prescribed by regulation about the operation of the Act during a financial year and the Information Commissioner must prepare a report on the operation of the Act which includes details of matters prescribed by regulation. The chair of the parliamentary committee must table the report in the Assembly within three sitting days after the committee receives the report.

Clause 134 inserts new section 191A (Corporations legislation displacement) which provides that a regulation may declare a provision of the RTI Act that applies in relation to a prescribed corporation (within the meaning of the Corporations Act that is declared under section 16A to be a public authority for the RTI Act) to be a Corporations legislation displacement provision for the purposes of section 5G of the Corporations Act. The regulation may be declared to apply in relation to the whole of the Corporations legislation or a particular provision of the Corporations legislation, or all prescribed corporations or a particular prescribed corporation.

Clause 135 inserts new chapter 7, part 9 (Transitional provisions for Information Privacy and Other Legislation Amendment Act 2023) which contains new sections 206J to 206S.

New section 206J (Definitions for part) provides definitions of 'amendment Act', 'former', 'former IP Act, and 'new' for the purposes of new part 9 of chapter 7.

New section 206K (Existing access applications) provides for how an application or purported application under former chapter 3 that has not been finalised before commencement is to be treated. The RTI Act as in force from time to time before the commencement continues to apply as if the amendment Act had not been enacted, however, the section is subject to sections 206L.

New section 206L (Disclosure logs) provides that new chapter 3, part 7, division 2 applies in relation to an access application, regardless of when the application was made, and a reference to a publication of information or a document in a disclosure log under section 78A is taken to include a reference to publication of the information or document in a disclosure log under former section 78.

New section 206M (Refusal to deal with access application – previous application for same documents) provides that for new section 43, a first application may be an access application under the former IP Act and specifies how stated references in new section 43

are to be taken. The section also includes definitions of 'corresponding former IP Act provision' and 'former IP Act review' for the purposes of the section.

New section 206N (Refusal to deal with amendment application – previous application for same documents) provides that in new section 78P, a reference to a first application is taken to include a reference to an amendment application under the former IP Act. If a first application under 78P is an amendment application under the former IP Act, a reference in section 78P to a provision of this Act is taken to be a reference to the corresponding former IP Act provision, a reference in 78P to a review is taken to be a former IP Act review.

New section 206O (Existing delegations or sub-delegations under former IP Act relating to amendment applications) provides that a delegation or sub-delegation made under section 50 of the former IP Act, which is still in effect immediately before commencement, continues to have effect for amendment applications under new section 78H.

New section 206P (Existing directions under former IP Act relating to amendment applications) provides that a direction relating made by a Minister under section 51 of former IP Act, which is still in effect immediately before commencement, continues to have effect for amendment applications under new section 78I.

New section 206Q (Performance monitoring functions) provides former section 131 of the RTI Act continues to apply in relation to an existing review in relation to the operation of the former IP Act, chapter 3, and the operation of the former IP Act, chapter 3 under section 217 of the IP Act, where a review was started before commencement but a report about its outcome has not been given to the parliamentary committee before commencement.

New section 206R (Report to Assembly on Act's operation) provides that new section 185 does not apply, and former section 185 continues to apply in relation to financial year ending before the commencement if the report for the financial year has not been tabled in the Assembly under former section 185, as if the Amendment Act had not been amended.

Clause 136 amends section 2 of Schedule 3 (Exempt information) to insert new section 2(3A). Section 2(3A) declares that, to remove any doubt, a document mentioned in schedule 3, section 2(3)(a) (Cabinet submissions) or Schedule 3, section 2(3)(f) (Cabinet decisions):

- is not comprised exclusively of exempt information if some information in the document has officially published by decision of Cabinet; but
- continues to be comprised of exempt information to the extent information in the document has not been published.

New section 2(3A) also declares that a document mentioned in schedule 3, section (3)(b) to (e) or (g) (that is, Cabinet briefing notes, Cabinet agendas, notes of discussion in Cabinet, Cabinet minutes, and drafts of these things as well as drafts of Cabinet submissions and Cabinet decisions) is taken to be comprised exclusively of exempt information despite any publication of a document mentioned in schedule 3, section 2(3)(a) (Cabinet submissions) or Schedule 3, section 2(3)(f) (Cabinet decisions).

Clause 137 amends section 12(1) in Schedule 3 (Information disclosure of which prohibited by Act) to include information the disclosure of which is prohibited by section 92 of the *Ombudsman Act 2001* as exempt information.

Clause 138 amends schedule 4 (Factors for deciding the public interest) to insert notes to alter readers to the effect of section 47(3)(b) and that factors for deciding the public interest may include factors other than the factors mentioned in schedule 4.

Clause 139 inserts new schedule 4A (Reviewable decisions) which provides items for the definition of 'reviewable decision' in schedule 5 which refers to a decision mentioned in schedule 4A. Section 1 in schedule 4A refers to stated decisions relating to access applications. Section 2 in schedule 4 refers to stated decisions related to amendment applications.

Clause 140 amends schedule 5 (Dictionary) to omit definitions which are no longer required and provide new definitions of 'amendment application', 'considered decision' decision-maker', 'deemed decision', 'evidence of identity', 'internal review processing period', 'judicial function decision', 'narrow', 'personal information' and 'reviewable decision'. Consequential changes are also made to the definitions of 'appeal tribunal', 'judicial member' and 'privacy commissioner'.

Part 6 Other amendments

Clause 141 provides that Schedule 1 amends the legislation it mentions.

Schedule 1, part 1 makes amendments to the *Information Privacy Regulation 2009* and the *Right to Information Regulation 2009* to refer to 'copy' instead of 'photocopy', to ensure that there is flexibility to provide certified copies of documents that are not necessarily photocopies. These amendments commence on assent.

Schedule 2, part 2 makes the following amendments to commence by proclamation:

- the *Auditor-General Act 2009*, to update the note to section 72A(2) to refer to QPP 6.2(b) in schedule 3 of the IP Act, rather than sections 10(1)(c) and 11(1)(d) of the IPPs;
- the *Brisbane Olympic and Paralympic Games Arrangements Act 2021*, for consistency with amended section 33 of the IP Act;
- the *City of Brisbane Act 2010*, to refer to the amended heading for section 408E of the Criminal Code;
- the *Coal Mining Safety and Health Act 1999*, to omit a reference to chapter 3 of the IP Act which is omitted;
- the *Corrective Services Act 2006*, to omit a reference to chapter 3 of the IP Act which is omitted;
- the Criminal Code, to refer to the amended heading for section 408E of the Criminal Code;
- the *Domestic and Family Violence Protection Act 2012*, to update a reference to the information privacy principles to the QPPs, and to update a cross-reference to section 7 of the IP Act;
- the *Energy and Water Ombudsman Act 2006*, to update a reference from any IPP to any QPP;
- the *Explosives Act 1999*, to omit a reference to chapter 3 of the IP Act which is omitted;
- the *Hospital and Health Boards Act 2011*, to update a reference from chapter 2, part 4 to chapter 2, part 3 of the IP Act;

- the *Information Privacy Act 2009*, to update terminology to refer to 'Queensland privacy principles', 'privacy principle requirements' and 'QPPs' and reflect the amended definition of 'public record';
- the *Introduction Agents Act 2001*, to omit a reference to chapter 3 of the IP Act which is omitted;
- the *Legal Profession Act 2007*, to omit a reference to chapter 3 of the IP Act which is omitted;
- the *Local Government Act 2009*, to refer to the amended heading for section 408E of the Criminal Code;
- the *Mining and Quarrying Safety and Health Act 1999*, to omit a reference to chapter 3 of the IP Act which is omitted;
- the *Partnership Act 1891*, to omit a reference to chapter 3 of the IP Act which is omitted;
- the *Path to Treaty Act 2023*, to make consequential changes reflecting the omission of chapter 3 of the IP Act;
- the *Police Powers and Responsibilities Act 2000*, to refer to the amended heading for section 408E of the Criminal Code;
- the *Public Guardian Act 2014*, to omit a reference to chapter 3 of the IP Act which is omitted;
- the *Public Health Act 2005*, to update a reference from chapter 2, part 4 to chapter 2, part 3 of the IP Act;
- the *Public Sector Act 2022*, to update the note to section 177(3) to include section 134 of the IP Act as not subject to direction by a chief executive;
- the *Queensland Future Fund (Titles Registry) Act 2021*, to omit reference to section 126 of the IP Act which is omitted and update a note to refer to relevant QPPs;
- the *Right to Information Act 2009*, to make a number of minor and consequential amendments; and
- the *Tourism Service Act 2003*, to omit a reference to chapter 3 of the IP Act which is omitted.