Office of the Information Commissioner
Queensland

6 November 2020

Level 7
133 Mary Street
Brisbane Q 4000

PO Box 10143
Adelaide Street
Brisbane Q 4000

Phone (07) 3234 7373
www.oic.qld.gov.au

ABN: 70 810 284 665

Attention: Office of the National Data Commissioner
PO Box 6500
Canberra ACT 2600

By electronic submission

Submission re: Data Availability and Transparency Bill 2020

The Queensland Office of the Information Commissioner (OIC) welcomes the opportunity to comment on the Office of the National Data Commissioner's (ONDC) Exposure draft of the Data Availability and Transparency Bill 2020 (DATB), explanatory materials and Accreditation Framework discussion Paper (Accreditation Framework).

About the OIC

The OIC is an independent statutory body that reports to the Queensland Parliament. We have a statutory role under the *Right to Information Act 2009* (RTI Act) and the *Information Privacy Act 2009* (IP Act) to facilitate greater and easier access to information held by government agencies. We also assist agencies to understand their obligations under the IP Act to safeguard personal information that they hold.

Queensland's RTI Act recognises that government-held information is a public resource and that openness in government enhances accountability. The RTI Act represents a clear move from a 'pull' model' to a 'push model' emphasising proactive and routine release of information and maximum disclosure of information unless to do so would be contrary to the public interest.

OIC supports data sharing and release strategies and initiatives that maximise disclosure of government-held information, carefully balanced with other important public interests such as appropriately safeguarding the community's privacy.

OIC's statutory functions include mediating privacy complaints against Queensland government agencies, issuing guidelines on privacy best practice, initiating privacy education and training, and conducting audits and reviews to monitor agency performance and compliance with the RTI Act and the IP Act. Our office reviews decisions of agencies and Ministers about access to, and amendment of, information under the RTI and IP Act.

OIC's Submission

OIC acknowledges the extensive consultation undertaken by the Australian Government over a two-year period to inform development of the DATB and supporting materials.

OIC notes that some concerns, raised by stakeholders in earlier consultations, are addressed in the DATB, including:

- no compulsion to share data
- no application to open data release
- restrictions on the sharing of data for compliance, assurance, national security and law enforcement purposes;
- specific accreditation for the handling of personal information; and
- sharing of personal information of individuals is done with the consent of the individual unless it is unreasonable or impracticable to obtain their consent.

A transparent and accountable data sharing framework incorporating robust governance, oversight and privacy and data protections is critical to addressing community concerns over privacy and building social license and trust to realise the policy objectives of the DATB. The DATB needs to be sufficiently flexible to respond to privacy risks posed by the advent of new technologies such as artificial intelligence, facial recognition and data analytics. For example, further clarification may be required regarding the use of data for automated decision making and for training of artificial intelligence, including requirements around notice to individuals along the lines of the General Data Protection Regulation. Developments in this area will also need to align with any future reforms to the Commonwealth *Privacy Act*.

The recent passing of the *Privacy Amendment (Public Health Contact Information) Act 2020* by the Commonwealth Government demonstrates the importance of embedding robust privacy protections in legislation, in managing privacy risks and securing the trust of the community to realise the benefits of government services and initiatives, such as the *COVIDSafe* app**.**

Community concerns over privacy is evident from the findings of the recent Australian Community Attitudes to Privacy Survey 2020 conducted by the Office of the Australian Information Commissioner (ACAPS). The Survey found that 87% of Australians want more control and choice over the collection and use of their personal information with 70% of Australians uncomfortable with government agencies sharing their personal information with the private sector.[1]

OIC welcomes the commissioning, and publication of, two Privacy Impact Assessments (PIA's) to mitigate privacy risks and strengthen privacy safeguards, noting that the draft PIA on the Bill will be updated in response to changes to the Bill that may occur following public consultation. OIC further notes Information Integrity Solutions (IIS) made 13 recommendations in the draft PIA on the Bill to strengthen the sharing scheme, all of which were accepted, in full or in principle,[2] by the interim ONDC.

OIC also welcomes a range of transparency measures contained in the DATB including publicly available Data Sharing Agreements, annual reporting to Parliament by the ONDC on the operation of the scheme and prescribed periodic reviews of the data sharing scheme.

OIC provides the following specific comments on the draft DATB:

1. The **permitted purposes** data can be shared by data custodians with an accredited user are broadly defined, which lends itself to a potentially

[1] https://www.oaic.gov.au/assets/engage-with-us/research/acaps-2020/Australian-Community-Attitudes-to-Privacy-Survey-2020.pdf

[2] Noting that Recommendation 8, 11 and 12 were accepted 'in principle'.

wide and subjective interpretation of the purposes for which data can be shared. In accordance with the DATB, data can be shared between Commonwealth agencies, and with state and territory governments, universities and private sector entities that have been accredited.

The permitted purposes require greater clarity and narrowing to restrain improper disclosure, reduce the risk of function creep, increase community acceptance and trust, and reduce the privacy risks to individuals. This is important given that the DATB contemplates the sharing of personal information that is not de-identified. OIC further considers that there is a need for greater certainty and clarity around commercial uses. As noted previously, the community has less comfort with government agencies sharing their personal information with the private sector.

2. The DATB adopts a principles-based framework to facilitate the controlled sharing of public sector data with key aspects of the Bill to be dealt with in regulations, rules, standards and guidance materials, yet to be developed. Data Codes made by the ONDC will prescribe how entities must apply the Scheme. While OIC notes that regulations, Ministerial Rules and Data Codes are all disallowable legislative instruments, it has been OIC's consistent position that data and privacy protections and safeguards should be **entrenched in primary legislation** rather than subordinate legislation.

This provides for a level of parliamentary oversight and scrutiny of any proposed amendments that may serve to weaken privacy protections that is not available for protections prescribed in other instruments, agreements or subordinate legislation. OIC notes that the draft DATB affords some protection by providing that the Ministerial Rules cannot expand the Data Sharing Scheme, i.e. the rules can only restrict the scheme by prescribing additional precluded purposes, but they cannot expand it. However, significant and substantive matters that impact on the privacy of individuals should be included in the DATB. The effectiveness of the DATB in addressing concerns about privacy and security of data sharing is dependent on the development of a range of subordinate legislation and accompanying guidance materials, including the security, privacy, infrastructure and governance requirements accredited users are required to satisfy.

OIC is not able to provide fully informed feedback on the DATB in the absence of the details of a range of legislative instruments that are not yet available, including the security, privacy, infrastructure and governance requirements accredited users are required to satisfy.

3. While merits and judicial review is available under the DATB for decisions made by the ONDC, such as accreditation decisions, the DATB does not provide for merits review of data sharing decisions by data custodians. An individual would be restricted to challenging data sharing decisions made by data custodians through judicial review. Judicial review offers a more limited form of review and may not offer an individual access to a timely and cost-effective remedy.

As outlined in the Explanatory Memorandum (EM) existing avenues for redress in other schemes continue to be available, including where the situation involves sharing or shared data. For example, a person affected by a decision based on shared data may seek review of that decision, where legislation governing that decision sets review rights.

Given the Data Custodian makes the data sharing decision, **merits review of data sharing decisions by data custodians** should be made available under the DATB for individuals to strengthen available redress mechanisms for individuals.

4. Clause 27 of the DATB provides that all data scheme entities must be subject to the Commonwealth *Privacy Act* or comparable privacy protections. Two mechanisms are provided under the DATB for these entities to achieve **privacy coverage** for acts and practices involving personal information under the data sharing scheme.

Subclause (1)(b), allows State or Territory authorities in jurisdictions with privacy laws to be covered by those laws, where coverage is equivalent to the *Privacy Act*. To be deemed equivalent, the EM states that a jurisdictional law must provide for protection of personal information comparable to the Australian Privacy Principles, monitoring of compliance with the law, and means of recourse for individuals if their information is handled contrary to the law. The EM further states that 'at the time of drafting, New South Wales, Victoria, Queensland, Tasmania, the Australian Capital Territory and the Northern Territory may have privacy laws that satisfy subclause (1)(b).

OIC has previously raised that it is not certain whether Queensland's current privacy laws offer equivalent coverage to the *Privacy Act*. The current review of *the Privacy Act*, which may result in changed or additional privacy protections and coverage under the *Privacy Act,* is likely to pose further challenges for State or Territory jurisdictions in achieving equivalency under subclause (1)(b). It is also not clear from the current drafting how this will apply in practice i.e. what criteria will be used to determine equivalency and which body/entity will make that determination? If State and Territory jurisdictions do not agree with a finding of equivalency, what review mechanism, if any, is available? Is there a requirement for ongoing review of those jurisdictions deemed equivalent under this provision to ensure equivalency is maintained? This will be critical as privacy laws across jurisdictions continue to evolve and change.

For States and Territories without their own privacy laws (currently South Australia and Western Australia) or entities that are not already covered by the Privacy Act as 'agencies' or 'organisations', subclause 1(a) provides that these entities could use the relevant mechanism of the *Privacy Act* (sections 6E(2), 6EA, and 6F) to become subject to the *Privacy Act*. The EM notes that a State or Territory authority in other jurisdictions, including Queensland, may choose to achieve its coverage obligations under subclause (1)(a). OIC has previously noted that clauses which seek to apply the Commonwealth *Privacy Act* to State or Territory authorities potentially raises constitutional issues. OIC would welcome further clarification on the operation of subclause (1)(a) to ensure the validity of these provisions in the DATB and the interaction with existing State or Territory privacy laws for entities subject to existing laws in their respective jurisdictions.

The drafting of subclause (1)(a) and (1)(b) highlights the difficulties of a lack of national consistency in privacy laws and the risks posed to an individual's privacy due to the patchwork of privacy protections in the handling of their personal information.

5. Clause 22 of the DATB provides limited statutory authority to override other Commonwealth, State and Territory laws that restrict sharing, collection and use of public sector data. The EM notes this clause is only effective against secrecy or non-disclosure provisions, as these provisions present barriers to sharing of public sector data. The EM further notes that provisions relating to data handling and security are also not affected by this clause. **OIC strongly recommends the ONDB provide clear guidance on the operation of clause 22** to provide certainty and clarity regarding interaction with State and Territory laws, including interaction with the existing privacy frameworks in these jurisdictions.

6. OIC notes that the DATB establishes another statutory body to undertake the role of regulator of sharing of data that contains, or is derived from, personal information, adding an additional layer of complexity to the current regulatory environment.

7. There is no requirement for data containing, or derived from, personal information to be **de-identified** prior to sharing. To minimise the privacy risks to individuals, data sharing should occur on a de-identified basis, whenever practicable.

Your sincerely

Phil Green
Privacy Commissioner

Rachael Rangihaeata
Information Commissioner