FSC

FINANCIAL SERVICES COUNCIL

Exposure Draft: Data Availability and Transparency *Bill* 2020

FSC Submission

November 2020

1. About the Financial Services Council

The FSC is a leading peak body which sets mandatory Standards and develops policy for more than 100 member organisations in one of Australia's largest industry sectors, financial services.

Our Full Members represent Australia's retail and wholesale funds management businesses, superannuation funds, life insurers, financial advice licensees and licensed trustee companies. Our Supporting Members represent the professional services firms such as ICT, consulting, accounting, legal, recruitment, actuarial and research houses.

The financial services industry is responsible for investing $3 trillion on behalf of more than 15.6 million Australians. The pool of funds under management is larger than Australia's GDP and the capitalisation of the Australian Securities Exchange and is the fourth largest pool of managed funds in the world.

2. Background and Introductory Comments

We thank you for the opportunity of providing a submission on the *Data Availability and Transparency Bill 2020* Exposure Draft (**DATB**).

We have reviewed the DATB and the:

1. *Data Availability and Transparency Bill 2020* Exposure Draft Consultation Paper; and
2. Privacy Impact Assessment "**PIA**) – Draft *Data Availability and Transparency Bill 2020* for the Office of the National Data Commissioner (**NDC**), Department of the Prime Minister and Cabinet.

We understand the broad intent of the *Data Availability and Transparency Bill 2020* (**DATB**) to reduce the need for individuals to provide the same and/or similar data to multiple Government agencies. This is particularly the case for individuals who are vulnerable and/or disadvantaged, such as those dealing with the death of a loved one and those facing financial difficulties.

However, we have considered the key risks that increased access to data by Government agencies may pose and the operational controls that should be implemented to mitigate those risks and protect the data shared and accessible as a result of the implementation of the DATB into legislation.

We note that Government departments and agencies would only be able to share data for three purposes:

- to deliver Government services;
- to help develop Government policies; and
- for research and development.

We note that the DATB ensures that data is only shared if prescribed conditions are met including the following safeguards:

- an accreditation framework;
- data sharing purposes;
- data sharing principles; and
- data sharing agreements.

We note that the DATB specifically excludes sharing information for the purposes of law enforcement, compliance, assurance, national security and targeted commercial marketing.

We consider that Government departments and agencies will need to review their current operational processes and both their financial and human resources to protect the personal and sensitive information that they transmit and hold. We would expect that Government departments and agencies would review their current operational processes and resources in alignment with the following:

1. *Privacy Act* 1988 (Cth) (**Act**) and the 13 *Australian Privacy Principles*;
2. Guidelines published by the Office of the Australian Information Commissioner (**OAIC**) regarding the protection of personal information; and
3. Surveys published by the OAIC regarding individual and community expectations regarding privacy and information security.

We consider that the current volume and extent of personal and sensitive information held by Government departments and agencies is already attractive to cyber criminals, state actors and organisations involved in big data and artificial intelligence (**AI**) and that the threats regarding access to that information will increase exponentially as a result of the implementation of the provisions within the DATB.

We anticipate the privacy and cyber security teams within Government departments and agencies would be increased in line with the increased risks to ensure that adequate resources and support teams can quickly and efficiently identify and remediate any issues regarding the security of information transmitted between and held by Government departments and agencies as a result of the implementation of the provisions within the DATB.

As such, the financial services industry would expect Government departments and agencies to significantly increase their:

- IT security/cyber funding and resources to implement appropriate operational controls, detection and testing around IT security; and
- IT security/cyber and privacy teams with appropriate skills and experience to manage the increased risks and threats.

We have set out some more detailed comments on the PIA recommendations below.

3. Specific Comments on the 13 Recommendations in the PIA

Recommendation 1: Align accreditation requirements with APP 1 and give regard to OAIC advice on privacy governance and management

We agree with this recommendation and the commentary in the PIA pertaining to this recommendation. However, further clarity is needed on whether or not accreditation is an ongoing process or a one-off event. The period of accreditation should be limited to a specific timeframe before re-accreditation is required; alternatively, there could be a process where ongoing accreditation is subject to a regular independent assurance process.

It is not clear from the DATB if there will be penalties for Government departments and agents and individuals accountable for privacy and data security in those entities if data is acquired and/or transferred in contravention of the relevant provisions, such as if there is no current accreditation. To deter non-compliance with the provisions of the DATB, we would expect that penalties would apply to relevant entities and individuals in cases where the contravention was deliberate or negligent and the impact of the contravention has or could result in harm to one or more individuals impacted by the contravention. The provisions of the Notifiable Data Breach regime, within s26 of the Act could be considered in this regard.

Recommendation 2: Ensure that accreditation involves regular assurance that standards are being met

We agree with this recommendation but have some concerns regarding the frequency and scope of the assurance function. A review may be necessary of the current resources and regulatory powers of the OAIC and NDC to ensure that these entities will be able to effectively monitor and enforce compliance with the provisions of the DATB.

Recommendation 3: Draft DATB to effectively exclude sharing for compliance and assurance purposes

We believe it is prudent to agree with this recommendation and the commentary in the PIA pertaining to ensuring that compliance and assurance is an excluded purpose and having law enforcement related activities regulated by dedicated law.

However, we note that a similar concept should be included in the draft DATB for those entities (including, FSC members) who are required to notify and submit data to a number of Government agencies and regulators in respect of, but not limited to the following legal requirements:

- reporting of significant breaches of the law or Australian Financial Service Licence obligations to ASIC pursuant to section 912D of the *Corporations Act* 2001 (Cth) (**Corporations Act**);
- reporting of significant breaches by a registrable superannuation entity of its licence condition to APRA pursuant to section 29JA of the *Superannuation Industry (Supervision) Act* 1993 (Cth);
- provision of data or statement to ASIC under a Notice of Direction pursuant to section 912C (1) of the Corporations Act);

- provision of information or documents under the *Australian Securities and Investments Commission Act* 2001, (**ASIC Act**);
- reporting to APRA and the OAIC in respect to breaches of Prudential Standard CPS234 and the Act;
- responding to information requests relating to work, health and safety practices as a result of COVID-19;
- the provision of information and/or data to the Human Rights Commission relating to potential breaches of anti-discrimination legislation; and
- other regulatory and legal reporting obligations (**Legislative Provisions**).

The extent and nature of the data and information provided under these Legislative Provisions are predominately commercially sensitive and may contain personal and sensitive information concerning clients and customers. In some circumstances, information may be provided to these regulators that contains legally privileged communications and is only provided to the regulator under a mechanism that allows non-waiver of that privilege or is provided on a voluntary basis to that regulator due to the nature of request where the provider of information is willing to provide, voluntarily, privileged information to the regulator but not in any other circumstances.

In our view, further protections should be included in the draft DATB to cater for provision of information and data under these Legislative Provisions (or voluntarily to regulators as described above). We note that the draft DATB does attempt to cater for such protections where information is provided under legal professional privilege (sub-section 17 (3) (a) (iii)) and commercial information (sub-section 17 (3) (b)) is provided. However, there is an onus on the provider to demonstrate that sharing the data contravenes or infringes that subsection or founds an action by that party in contract. There is a subjective element to this test and allows differing interpretation as to what constitutes a breach or infringement.

Further, the commercially sensitive information is submitted under Legislative Provisions (or sometimes voluntarily to a regulator) and is not submitted under an agreement or contract which contains a right to confidence. This poses a risk where no duty of confidence arises (other than to the extent arising under provisions of the ASIC Act, such as section 127 of the.

There are other protective mechanisms such as section 56 of the *Australian Prudential Regulation Act* 1988 (**APRA Act**) which contains general secrecy provisions for the protection of certain information or documents disclosed to it; however, we note that the draft explanatory memorandum at paragraph 13 confirms that the draft DATB will override the Commonwealth and State laws that prevent sharing of information, if the draft DATB sharing requirements are met. It would be prudent to obtain clarity regarding what laws the DATB will override and whether that will impact the APRA Act, ASIC Act, or the Memorandum of Understanding between the two regulators.

Accordingly, in order to ensure certain information and data submitted to regulators is not shared inappropriately, the draft DATB should include the following:

- data and information submitted to ASIC and APRA under the above Legislative Provisions (or voluntarily where requested by a regulator but not under a statutory notice) is listed as a precluded purpose and contained in sub-section 15 (2). The first limb of the draft DATB is therefore not satisfied; and/or
- ASIC and APRA to be listed as precluded entities in section 11 and sub-section 17 (2); and/or
- Information and data submitted to government regulators to comply with a notice, direction or relevant financial services laws is excluded under sub-section 17 (3).

This addition would make it sufficiently clear and mitigate risk of legally privileged and commercially sensitive information being shared inappropriately. The provisions should accommodate the *voluntary* provision of information to a regulator (commonly provided to regulators without a statutory notice) – such information should also be excluded (or subject to the same protections, and conditions for sharing, as for information provided under notice or compulsion).

Recommendation 4: Articulate meaning of permitted purposes in Explanatory Memorandum

Greater clarity regarding permitted purposes would be welcomed by the financial services industry and the wider community. In addition to the requirement that "data must be reasonably necessary" we consider that a materiality test could be introduced to ensure that there is transparency around data sharing. Customers of financial services entities may have concerns if, say, FSC members report data to one Government department and/or agency, which is subsequently provided to another Government department and/or agency. An example may be where data is provided in order to comply with a regulatory request for information, or to report a breach of AFSL licence conditions. We note that, wherever permissible, members provide statistical data in aggregate, rather than personally identifiable information about specific customers. However, we also note that Government departments and agencies hold a great deal of information about individuals and it may be possible to identify and/or reidentify one or more specific individuals from the various data sets shared by Government departments and agencies.

Recommendation 5: Provide guidance on the ethics process in appropriate circumstances and

Recommendation 6: Provide guidance on how consent operates in the Data Sharing Scheme

We agree with the principles of these recommendations and the PIA commentary pertaining to these recommendations. We note that our customers are unlikely to expect their information to be shared between Government departments and agencies and that the scope of the consent that they provide our members to provide financial services would not specifically extend to the disclosure of their information from the financial services provider to one or more Government departments and agencies. The APP Privacy Policies of FSC members generally will refer to disclosing information to law enforcement agencies and regulators; however, these would be unlikely to reference the further disclosure of that information between Government

departments and agencies. We think it is unlikely that clients and customers would "join the dots" here. We have assumed that where a financial services entity provides information about customers to one agency, that it could be shared (under the proposed legislation) with a range of other agencies (other than perhaps the ATO). This requires further consideration and consumer education by the Government.

We note the commentary in item 3.7 of the PIA that "the loss of data through negligent sharing practices, or poor transparency of records about who shared data and for what reasons, further erodes public trust in the Government's ability to keep data safe." The commentary continues "Without appropriate oversight, data security can be neglected, misused, or mishandled." We consider that due to the rapid rate of technological advances and the value of data sets for commercial purposes, Government departments and agencies should conduct regular reviews and updates of their current operational processes to collect, transmit and secure data. We consider that Government departments and agencies should have frequent audits and assurance reviews on their data security with input from appropriately experienced and skilled privacy, IT security and cyber security experts. These audits and reviews (which should be independent of the agency sharing or receiving the information) should occur regularly and should include, but not be limited to, the following items:

- The privacy management framework of the relevant Government department or agency;
- The APP Privacy Policy of the relevant Government department or agency;
- The process to identify, remediate and report data breaches;
- The Data Breach Response Plan of the relevant Government department or agency;
- The process to transmit data between Government departments and agencies;
- The financial, operational and staffing resources available to the relevant Government department or agency to meet its relevant legal and regulatory obligations pertaining to privacy and data security; and
- A review of any privacy and data related complaints received by the relevant Government department or agency.

We consider that audits and reviews of this type should occur more frequently than the three-year timeframe specified under Recommendation 8. We would expect that different Government departments and agencies would have different levels of IT and privacy related resources and operational controls based on their size and the type and extent of personal and sensitive information that they collect, manage, disclose and secure to carry out their specific functions. As such, we consider that the information security arrangements and the adequacy of resourcing for Government departments and agencies, pertaining to information security and privacy, should be reviewed at three specific points:

- Prior to the DATB receiving Royal Assent/commencing;
- At the end of the first year after the DATB commences; and
- Periodically, e.g. on a rolling three-year basis.

We consider that there is a risk of widespread data sharing amongst Government departments and agencies to lead to the reidentification of previously de-identified and/or anonymous data. This risk increases exponentially with the number of data sets available to entities, with information about the contact details of one or more individuals being less of a threat to the privacy of those individuals, than sensitive information including information about health,

lifestyle and finances. We consider that it would be imprudent to assume that de-identified data is safe data without robust operational controls in place to reduce the risk of re-identification, particularly by cyber criminals, state agents and organisations involved in big data, AI, marketing and digital platforms.

Recommendation 7: Specify 'privacy' in the NDAC's advisory function

We consider that additional protections for sensitive information should be clearly articulated in the data sharing legislation due to the risk of harm to individuals as a result of the unauthorised access, loss, misuse, interference and unauthorised disclosure of sensitive information such as health, lifestyle and financial information entrusted to financial services providers by our customers.

Recommendation 8: Review effectiveness of the NDC support and staffing model in first statutory review of the Act and

Recommendation 9: Develop and publish a regulatory action plan

Refer to earlier comments regarding the resourcing and assurance function of both the OAIC and NDC and the frequency of audits and reviews set out in our response to Recommendation 6.

Recommendation 10: Individuals to have access to simple arrangements for addressing privacy complaints and issues and

Recommendation 11: Measure and report on individuals interaction with the scheme

It may be relevant to reference the expectations of individuals regarding the handling of their information in the most recent OAIC survey.

Recommendation 12: Allow for shortening the period for review of the Act and make reviews public

See Other Comments below.

Recommendation 13: Conduct public awareness campaign about the Data Sharing Scheme

No additional comments.

4. Other Comments

Given the risk of inappropriate data use or access and the importance of protecting the privacy of individuals and commercially sensitive information of organisations, we submit that the legislation and its operation be subject to an **initial independent review** within two years of commencement. The initial review should include whether any safeguards and protections require amendment or strengthening, and whether the extent of sharing data between Government departments and agencies needs to be wound back (or ceased) in light of experience or use of the data (such as whether there has been any cyber-hacking, or inappropriate access or use of the data shared). Input into the initial independent review should be obtained from OAIC, as a mandatory requirement.

Given the importance of security of information shared, the effect and operation of the Bill should also be subject to **independent periodic reviews** every two years, with the independent periodic review reported to, and tabled in, Parliament. Input on the independent periodic reviews also should be obtained from OAIC.

Further, the Bill should require reporting to Parliament, in Annual Reports of the agency sharing the information **and** the Government department or agency receiving the information under the Bill, on:

- what information has been shared (under the legislation),
- by which Government department or agency;
- to which Government department or agency;
- for what purpose;
- whether there has been any use or access of the data other than for permitted purposes under the legislation;
- whether the shared information has been compromised, accessed or used by persons not authorised under the legislation; and
- any complaints (whether or not sharing is compliant with the legislation) relating to the sharing, use of, or access to the data.

Reporting on the matters above to Parliament provides transparency and accountability that the extensive use and access to data meets community expectations and is also consistent with the protections in the Bill.

FSC members are entrusted with the personal and sensitive information of millions of individuals accessing financial services products, including their contact details, medical information and financial information. FSC members understand the importance of protecting the privacy and security of that information and the responsibility to identify incidents, breaches and areas for improvement. FSC members have a comprehensive understanding of both the OAIC and their customers' expectations regarding our information handling practices. FSC Privacy Working Group members are interested in developments in Australian privacy laws and would be appreciative of the opportunity to directly engage with Treasury, the OAIC and NDC on any proposed reforms.

[redacted]