6 November 2020

The Office of the National Data Commissioner (ONDC)
Department of the Prime Minister and Cabinet
PO Box 6500
Canberra ACT 2600

By upload

Dear Sir/Madam

Re: Consultation on the Data Availability and Transparency Bill 2020

AFMA supports the need for a more consistent approach by Government agencies and departments to the sharing and use of data.

However, we have serious concerns about the approach described in the Bill, notably the lack of effective exclusions, protections and insufficient explication of the principles that should exclude classes of data from potential sharing.

The result of these shortcomings we believe includes risks to the integrity and functioning of the regulatory system, a risk of undermining the legitimacy of Government data collection, and unquantifiable increased risks to personal and business privacy.

In response to these shortcomings AFMA:

- endorses a number of restrictions on the types of data that can fall within scope for 'sharing' or release, these include regulatory data, compulsorily acquired data, and data regarding vulnerable customers;
- notes our support for much more work being done to set up the principles which must be independently assessed as being adhered to before data can be released from current structures; and
- we also propose a framework approach to empower data subjects that is consistent with the Government's CDR scheme and the emergence of data as a valuable property with associated rights.

We find the controls proposed in the Bill to be weak and at risk of being ineffective. In particular the allowed purposes offer few limitations. Even where restrictions are nominally put in place for 'enforcement related purposes' the exception to these restrictions are broad.

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7900 Email: secretariat@afma.com.au

The framework of allowing Government agencies to form their own determinations on whether risks are managed is an inappropriate and insufficient approach to data management that is unlikely to produce consistent, reliable outcomes and does not sufficiently empower firms that supply data or data subjects. The alternate contractual arrangements approach also appears unworkable.

AFMA notes a number of concerns in relation to the proposed legislation including the framework approach which does not make an allowance for private data to be held in trust by the Government. This is inconsistent with the approach the Government has taken in the Consumer Data Right, where data is framed as belonging to the consumer and held in trust by business, subject to the control (within limits) of the consumer. We support such an approach for business data.

We note concerns around the need for the management of data subject to confidentiality and intellectual copyrights, and greater clarity on which data is to be considered confidential for data holders. Significantly there is no general prohibition against the release of information that could be reasonably likely to identify an individual or organisation.

There is insufficient clarity on the obligations of custodians under the Privacy Act and the conflicts with the "unreasonable or impracticable to seek their consent" test. AFMA supports consistent application of the Privacy Act to custodians. AFMA also raises concerns about whether data about vulnerable customers has sufficient protections under the legislation.

We understand the Government is moving to rapidly introduce and implement the scheme but we encourage a more measured and careful approach to building the structures that will manage data as they will have important long-term implications for Australia. As the PIA notes there is the possibility of constructing a regime that produces good outcomes within the proposed legislation, but we share concerns that too much is being left to implementation and the good intent of those that use the scheme.

Our concerns are elaborated further below.

We trust our comments are of assistance. For further information please contact me via the Secretariat.

Your sincerely

Damian Jeffree

Senior Director of Policy

Need for improved approach to data release

AFMA is aware of the need for improved processes as we have been disappointed by the proposed approach to data sharing by APRA in its consultations on the confidentiality of data.

APRA's enabling legislation has a clear framework for protecting the confidentiality of data supplied to it for reporting purposes, protecting essentially all documents and information produced for prudential purposes with significant penalties (including for custodians) unless carved out by the legislation. APRA has proposed [1] to make by determination data items from the quarterly authorised deposit-taking institution performance statistics forms, as well as the main forms used for QPEX, to be non-confidential from the time of receipt by APRA. It would also make all remaining data in all quarterly forms non-confidential after three years. More recently it has proposed to take a more staged approach[2] to which data will be initially required under the proposal. We are concerned that the release regime makes APRA's legislative framework of limited application in practice to quarterly data.

Rather than neutralising the effect of the legislated framework by broad determinations we would argue that legislative change is the more appropriate route. This would have the advantage of making the consulting party neutral with regard to the conflict of reduced risks for the data collecting authority.

We encourage the Government to bring more structure to these processes which are currently *ad hoc*. Releasing the data of private citizens and companies under a banner of 'transparency', is not in itself a pure public good as it comes at a cost to the privacy of companies and individuals. 'Transparency' in this sense and privacy are a twin pair and cannot be considered in isolation from each other without distorting any assessment of impacts.

Section 51(xxxi) compliance and alignment

In the Bill there is currently no structured recognition of the proper ownership of the data.

Concepts in relation to data ownership, custodianship and stewardship are emerging but should be properly considered and structured into any Government data regime. In a world where data is increasingly the most valuable commodity, underpinning the valuations of some of the world's most valuable companies, a *faux-naïf* approach of treating the collected data of firms and individuals as 'there for the sharing' without the consent and compensation of those whose actions created the data is increasingly untenable. It is also unaligned with the Government's own approach to data in other contexts.

Data is progressively more recognised as being the property in certain ways of those who created the data or those who the data is about. This is the approach taken by the Government in the recent Consumer Data Right (CDR) scheme. In the CDR scheme data

[1] https://www.apra.gov.au/sites/default/files/2020-02/ADI%20Industry%20Letter%20-%20Non-confidentiality%20for%20ADI%20quarterly%20publications.pdf

[2] https://www.apra.gov.au/sites/default/files/2020-09/Letter%20to%20authorised%20deposit-taking%20institutions%20-%20Consultation%20on%20confidentiality%20of%20key%20ADI%20metrics%20%28002%29_0.pdf

that might once have been considered the property of firms that held it, is now recognised as belonging in important ways to those who the data is about, the data subject. Firms are required to follow the instructions, within limits, of data subjects with respect to the data. This is one example of the beginning of a property approach to data.

Considered as property, the most relevant limitation on the powers of the Commonwealth in this regard is section 51 (xxxi) of the Constitution that, while phrased a grant of power, limits acquisition of property to 'just terms'. Even if personal data is not yet fully formed as property for the purposes of Section 51, it is appropriate for the Government to seek alignment of the scheme with the intent of this section both to ensure the spirit of the prohibition is adhered to and to position the scheme well for the future evolution of data rights.

Determining what should constitute 'just terms' requires some work, but there are few issues with existing arrangements. The provision of regulatory data to government agencies for the purposes of ensuring the stability of the banking system and integrity of markets to the benefit of those same firms and others provides a quid pro quo even if there is not a payment of market value 'compensation'.

This does not, however, then justify further distribution of that data. Each additional 'sharing' or release is effectively another acquisition of the data for s51 purposes, just as another use of intellectual property requires just terms for each instance of use.

This would suggest that a scheme that aligns well with s51 requires just terms for the firms and individuals for each 'sharing' of data. The scheme should be altered to ensure this outcome. In part this should be achieved by introducing a division within what is now called 'public sector data'.

'Public sector data'

AFMA notes that the definition of 'public sector data' sidesteps any consideration that data that has been provided by firms and individuals oftentimes under compulsion should not be treated as the property of the government. Defining all data lawfully held by the government as 'public sector data' avoids any construction that data held by the public sector, particularly compulsorily acquired, unaggregated, source-identifiable or regulatory data, might in fact be better considered and treated as private data held in trust by the government.

We suggest that 'public sector data' be limited and a concept of 'private data held in trust' be introduced into the scheme. 'Public sector data' could include data generated by the actions of government or aggregated data. Private data held in trust would be excluded from the scheme without consent of the data subject and firms from whom the data was sourced, or subject to additional protections.

Social contract

The Privacy Impact Assessment suggests that the privacy risks for individuals under the scheme include:

- Mishandling of personal information, including risk of re-identification or data breaches;

- Loss of control – individuals don't know what is happening with information about them, might not have a choice and might not in any event support the use; and
- Personal information is used in new ways that are unexpected, unwelcome, disadvantageous, or harmful.[3]

It suggests these create risks to the community's support for data sharing. AFMA is concerned that the risks for individuals and firms alike risk undermining not just the support for the 'sharing' of data but also the legitimacy of the social contract used in the original collection of the data.

In many existing data collection regimes, there are carefully constructed exceptions to the right to privacy and other rights that are appropriate for the function and purpose of the entities that collect the information, and their relationship to the entities providing the data. Merely because this data has already been collected should not make it potentially available for other purposes. Taking as the starting point that all legally collected data held by Government entities should potentially be in scope (with very few exceptions) effectively risks ignoring the fabric of legitimacy around the original data collection and the associated structures and relationships.

If data use and the reason for compulsory collection are disconnected there is a risk that Government will be seen as finding ways to collect data unrelated to their intended usage purpose, and this could lower the perceived integrity of these processes.

Regulatory data

The scheme is a particularly poor fit for the regulatory data collection infrastructure, and risks compromising regulatory function. The scheme offers no defined protection against the release by Government of data that has been gained under regulatory schemes.

Large volumes of data are compulsorily collected from firms under these regimes. This data is typically commercially sensitive, often contains intellectual property and data that is highly confidential and sensitive for individuals and firms to whom services have been provided.

These schemes are carefully constructed, and the use of their data is limited for appropriate purposes. The potential inclusion of this data in the data 'sharing' scheme risks the integrity of these systems. Even where information has been voluntarily provided for to regulators we strongly believe this data should also be excluded to avoid damage to the level of openness regulated firms can have with regulators.

Data is shared with regulators on the basis that they understand the data and firms can have confidence that their use of the data will be within a known range of activities. The inclusion of regulatory data in the scheme will remove this assurance. In order to address the risks to their clients and operations firms will be motivated to take a more legalistic and minimal approach to the data they provide to regulators. There can be no openness with a regulator whose data even in theory could end up anywhere.

We also note the large amount of investigations and enforcement data regulators collect as a matter of course that is not appropriate for public release. This data should never be

[3] Privacy Impact Assessment – Draft Data Availability and Transparency Bill 2020, *op. cit.*

available for release under any circumstances as to do so could unfairly tarnish reputations.

AFMA's work on the Consumer Data Right also highlighted the large amount of sensitive information that is contained in financial data. There should be no suggestion that this data might find its way into research projects unknown. There is also need for provisions for excluding data from being shared regarding vulnerable customers.

More generally AFMA supports much more work being done to consider what types of data should be excluded from the scheme. The approach of having almost all data held by government entities as potentially in scope for release creates far too much risk and uncertainty for business and individuals.

Security Scheme

AFMA is concerned that the Bill proposes to introduce through the accreditation criteria yet another bespoke security scheme that is unaligned with the proliferation of other Government-mandated information security schemes.

The Department of Home Affairs (DHA) is currently undertaking a consultation that proposes to introduce a scheme to 'top-up' the range of existing information security schemes for critical infrastructure. Existing Government information security schemes in financial services include the APRA standard CPS 234 and its associated guidance, ASIC's requirements for AFS licensees, and the ACCC's CDR scheme requirements. The DHA scheme will effectively form a fourth scheme for firms in the sector with top ups to the existing three schemes. We advised DHA against this approach and suggested a single national graded scheme was appropriate. We similarly advise ONDC against introducing a fifth information security scheme for the sector (potentially requiring another top-up mini-scheme by DHA). Note that all these different schemes will often apply to the same data, for example bank account data.

We note also the different schemes will be implemented in different ways by the different regulators, with some taking a constructive accommodative approach and others a punitive approach. A common single graded standard is far more likely to meet the Government's national security, privacy and other objectives than a tapestry of mis-matched schemes.

Need for robust requirements for Data Custodians

The Bill proposes providing an alternative pathway to share data where it is currently prevented by secrecy provisions or where it simplifies existing pathways. AFMA notes that this is a significant departure from, and a simplification of existing privacy jurisprudence afforded under the Privacy Act. The Bill states that accredited entities must comply with the Privacy Act when receiving data from a data custodian but does not appear to address the data custodian's obligations under the Privacy Act.

The Bill maintains that data sharing by custodians would be based on multiple safeguards such as accreditation, data sharing purposes, principles, agreements, transparency measures, independent regulator and merit and judicial reviews. However, given the community expectations around privacy, AFMA supports that data sharing by custodians be governed by stronger circumstantial specifications as made in APP 6. AFMA recognises

that access to data can lead to efficiencies, and when applied to the right purposes, with the appropriate controls, can result in public benefits. However, greater data use and data sharing should not compromise the complexities of data privacy and the accountability of government agencies. APP 6 offers a balance between protecting the privacy and allowing for other activities in the public interest and should be included as an important safeguard for sharing data, particularly to assist ensuring that commercially sensitive data is protected and not disclosed inadvertently.

AFMA supports express provisions in the Bill to ensure that government agencies (data custodians) comply with the Privacy Act in handling information.

Data privacy controls

AFMA shares the concerns of the PIA that the privacy controls allow excessive subjective interpretation by data custodians and accredited users and therefore offer data subjects limited protection or reason for confidence. The allowable data sharing purposes are so broad as to allow almost anything to be characterised to fit within their parameters.

The precluded purpose of enforcement we note does not extend to laws not punishable by a pecuniary penalty. We also note that the exception to the exclusion is broad and potentially subject to abuse. Research that relates 'generally to compliance with laws' could reasonably be expected to turn up information about specific actions that could then be used to seed specific investigations under other powers, rendering the exclusion ineffective in practice.

We suggest the exclusion provisions be extended to exclude data that could reasonable be expected to be able to be used to identify an individual or an organisation.

AFMA supports making provisions that disallow the sharing of commercially sensitive information that is shared with government agencies under compulsory legal and compliance obligations. The possession of commercially sensitive information by accredited users may lead to the risk of unintentional disclosure of confidential or intellectual property with third parties, which may increase reputational and commercial risks for organisations. AFMA holds that regarding such data, the risks to the entity, the market or to the efficacy of the regulatory regime under which the data is collected outweigh the benefits of sharing that data.

AFMA notes that it is not common practice to code or flag data shared with the Commonwealth as confidential or subject to intellectual property rights and we note the Bill does not expect this from data custodians either. This document classification activity may be done on an exception basis, such as where required due to legal proceedings requesting document discovery to be made available to the Court. However, this is not an efficient business practice due to the significant time and resource investment that would be required on an administrative task. We therefore submit that further consideration should be given to the storage and handling of confidential information and intellectual property to ensure it can be appropriately held and protected from undue disclosure to third parties.

Interaction with the CDR regime

As noted above, there are inconsistencies between the proposed regime by the Bill and the CDR regime. The accreditation framework proposed by the Bill imposes an additional, duplicative and resource-intensive accreditation application process and system over the one proposed by the CDR regime. For example, the CDR regime holds that once accreditation is granted, the accredited user then is governed by reciprocal data holder obligations separate to the obligations of an accredited data recipient. We note the CDR itself is not compatible with the Privacy Act imposing an inconsistent and complex overlay of its own rules.

It is incumbent on the government to ensure that the proposed regime and the CDR regime converge to a consistent framework for the use, disclosure and protection of data, including a consistent approach to consent and an approach opt out of either regime. In suggesting this approach, AFMA supports the pursuit of administrative efficiency, consistency of underlying principles and avoiding duplicative poorly structured frameworks.