Australian Banking Association

06 November 2020

Office of the National Data Commissioner
1 National Circuit, Barton, ACT 2600

Consultation on the Data Availability and Transparency (DAT) Bill 2020

The Australian Banking Association (**ABA**) welcomes the opportunity to comment on the DAT Bill.

The ABA supports the broad policy that public sector data should be able to be shared with appropriate safeguards if doing so is in the public interest, under the proposed regime (**DAT regime**). However, the ABA considers the Bill as drafted would significantly undermine Commonwealth regimes that have enabled effective business regulation in banking and other critical economic sectors. As such, the ABA strongly urges the Government to provide an exclusion for data that is covered by existing confidentiality provisions in regulatory regimes, such as section 56 of the *APRA Act 1998*, and consider alternative means of achieving this policy objective in relation to this class of data.

Impact on business regulatory regimes

The current draft Bill provides that data can be shared if it meets the purposes of the data sharing bill (proposed section 13) unless it is excluded from the scheme (proposed section 17) and that the authorisation to share overrides other prohibitions (proposed section 22). The Bill has specific provisions about use and protection for data about individuals but not for data about businesses.

This approach significantly changes the balance of policy considerations underpinning regulatory regimes in the financial services sector, and in other sectors. Under regimes such as the *Banking Act 1959*, regulators have significant and intrusive powers to require data and other information from regulated entities; the data and information can reveal the details of the entity's business strategy, financial positions, and information about their customers, suppliers and staff. These legislative powers also override the regulated entity's confidentiality obligations including under commercial contracts, common law and equity, and include third parties' commercially sensitive data.

In return, such legislation provides strong safeguards for the confidentiality of the information received by regulators. Unauthorised disclosure of confidential information is a criminal offence under prudential legislation. These safeguards are important to the regulators because they are often the basis for information sharing arrangements between regulators and law enforcement bodies. Equally importantly, these safeguards recognise the sensitivity of the data to the regulated entities and third parties, encourages proactive and open dealings with the regulators, and helps ensure availability of suppliers and service providers to regulated entities.

Current approach to confidential data: Australian Prudential Regulation Authority (**APRA**) and Australian Securities and Investments Commission (**ASIC**)

Banks are required to regularly report financial information and respond to ad hoc regulatory notices for data. The information disclosed by banks is predominantly commercially or market sensitive.

Each regulatory agency has their own legislative requirements outlining how they can use the data they collect. For example, data collected by APRA is subject to sections 56 and 57 of the *APRA Act 1998*. Section 56 of the APRA Act prohibits the unauthorised sharing of confidential information and data, which would include information and data that APRA collects under the APRA Act, the *Financial Sector (Collection of Data) Act 2001* (**FSCODA**), the industry Acts (*Banking Act 1959*, *Insurance Act 1973*, *Life Insurance Act 1995*, *Superannuation Industry (Supervision) Act 1993*) and other financial sector

legislation. The prohibition applies not just to APRA, but also to any other person who acquires the information in the course of their employment (other than the entity the information relates to). A breach of the prohibition is an offence with criminal penalties.

Section 57 of the APRA Act provides a limited mechanism for APRA to determine that certain data collected under the FSCODA is not confidential. In practice, to make any data non-confidential APRA is required to publicly consult with regulated entities, industry associations and other representatives of the entities and provide them with an opportunity to make representations as to whether or not a reporting document contains confidential information.

The mechanism under section 57 cannot be used for data and information collected under any other legislation administered by APRA, including under the broad information gathering powers in the APRA Act and industry Acts. There are two additional elements to note:

1) Section 57 is specific to APRA, and other financial sector and competition regulators do not appear to have this limited determination-making power.

2) Section 57 does not apply to information collected under information gathering provisions under the industry Acts. These provisions are cast broadly, and are not limited to powers by a person to compel the answering of questions.

The final Productivity Commission Inquiry Report (No. 82), *Data Availability and Use*, referred to the approach taken by APRA as an example of best practice when it comes to managing decisions about data sharing. This approach includes substantial consultation with interested parties and careful assessment of the costs and benefits including commercial detriment over public interest.

Data and information collected by ASIC is subject to section 127 of the *ASIC Act 2001*. This applies to information that is collected under the ASIC Act, *Corporations Act 2001*, *National Consumer Credit Protection Act 2009*, and others. Unlike APRA, ASIC does not have an ability to make determinations that data or information is confidential in relation to data or information held by ASIC.

Consequences of proposed section 22 of the Bill

Proposed section 22 of the Bill provides that a sharing of data that is authorised by proposed section 13(1) of the Bill does not contravene any law of the Commonwealth or of a State or Territory. This provision has the effect of overriding the confidentiality provisions contained in the business regulatory regimes. This removes a key underpinning of business regulation.

The ABA understands from the Data Legislation team that they consider the following mechanisms can be used to address these concerns. However, for the reasons stated below the ABA does not believe these mechanisms would do so.

Proposed section 17 and informal policy are insufficient

The data legislation team asked the ABA to consider whether the exclusions set out under section 17, and/or the ability for each government agency to adopt its own policy about release of data, may be sufficient. The ABA does not consider they are.

Each regulatory agency creates their own policy about how data is governed and shared

The ABA does not consider this to be an adequate replacement for current data protections. Policy is not legally enforceable and can be changed by regulators. The result is a lack of legally enforceable protection for data, which is an inadequate arrangement for commercially sensitive business information shared with regulators.

Each individual bank establishes a contract with each regulatory agency that holds their data

Under this approach, contract or agreements would be used to impose confidentiality obligations that apply to data collected by each agency. The data legislation team considers these agreements may have the result of bringing data into the exclusion in proposed section 17(3)(a)(ii).

The ABA does not consider this is a practical solution. Currently, commercial entities can negotiate the terms on which they voluntarily provide data to government agencies. Regulated entities are compelled by law to provide data to their regulators, making any attempt to negotiate the terms on which they provide data artificial. Secondly, entering such contracts could be criticised as a device to circumvent this regime. Finally, it would be impractical to negotiate and update contracts for the thousands of APRA regulated entities, thousands of ASIC regulated entities, their associated entities and third party service providers or counterparts whose data would be subject to this regime.

The regulated entities and regulators determine whether sharing of specified data may found an action for breach of confidence or breach a common law duty of confidence

The ABA considers there will be uncertainty about whether a regulator may owe a common law duty of confidence or be liable for an action for a breach of confidence. These questions may need to be considered on a case by case basis and may need to be clarified by the court, which would impede data collection by regulators and impose significant demands on limited court resources.

APRA may use section 57 APRA Act to determine that certain data is confidential

APRA can make a determination under section 57 of the APRA Act that data collected under the FSCODA is not confidential. The data legislation team queried whether this would allow APRA to determine that certain data is confidential, to impose on APRA the necessary confidentiality obligations, such that the data would fall within one of the exclusions in proposed section 17(3). The ABA has three comments on this.

First, there is significant uncertainty about the intended interplay between proposed section 22 and provisions in other Commonwealth legislation that identify specific information as confidential or non-confidential *for the purposes of legislative confidentiality regimes which are overridden by section 22*. If the government's intention is that any information that is identified under existing Commonwealth legislation as confidential would retain their status as confidential information, and therefore be excluded from the DAT regime by proposed section 17, this should be made expressly clear.

Second, this provision only applies to a subset of the data and information that APRA collects under the FSCODA. This does not address concerns about other data held by APRA, or information held by other regulators. If this is the result, it is not clear why APRA would be able to disclose some data that is considered to be commercially sensitive (and where APRA does not have the ability to 'declassify' the data), and be unable to disclose other data that may be less commercially sensitive, merely because APRA has the ability to make a determination about the confidentiality status of the second set of data.

Third, if APRA shares data subject to a section 57 determination of confidentiality with ASIC in accordance with section 56 APRA Act, it appears ASIC would become the Data Custodian in relation to that data instead of APRA. The Bill does not clearly address whether ASIC should also treat that data as excluded data, and it is unclear whether the effect of a section 57 determination would also impose the requisite duty of confidence on ASIC (currently, section 56 is used to ensure that confidentiality is maintained). The result can be excluded data being brought back into the DAT regime, contrary to the intention of the regulator that the data originated from.

This last comment points to a more general question about whether the Bill also preserves the effect of conditions that regulators may impose when they share information with other regulators. This may become particularly important, since the providing regulator would not be able to rely on the receiving regulator's confidentiality regime. Even if these conditions are preserved under the Bill, this may result in an increased number of conditions being imposed, which would be complex for the receiving regulator to track and comply with.

Risks for regulators and regulated entities

The ABA considers overriding confidentiality provisions under business regulatory regimes will create unintended consequences and risks, both for regulators and the regulated entities. These risks can undermine the effectiveness of business regulation.

There is no clear provisions dealing with how data custodians determine what data can be shared even where it is confidential for supervisory, enforcement or commercial reasons. This lack of guidance can create uncertainty which could undermine regulators' oversight duties. Examples of data not clearly excluded as part of the Bill, includes data obtained as part of:

- **Regulatory reviews and/or investigations:** Inadvertent disclosure of the existence of investigations can unfairly destroy entities' and individuals' reputation, as well as expose a regulator to criticism. Complex regulatory reviews and investigations are initiated and conducted using a range of supervisory and information gathering powers other than the coercive powers covered by proposed section 17(6)(a). Only a very small proportion of data used in an investigation would be filed with a court or tribunal, and the remainder would fall outside of proposed section 17(6)(b).
- **Information sharing with foreign regulators:** Foreign regulators routinely require APRA and ASIC to keep information confidential as a precondition of information sharing. The exclusion in proposed section 17(5) is unlikely to apply, as regulatory information sharing is not commonly conducted under binding international agreements, and many independent regulators are not considered to be part of a foreign 'government'. Given the uncertainty, foreign regulators may cease to share data with APRA and ASIC.
- **Receiving reports from individual and corporate whistleblowers:** Whistleblowers and entities that provide data under the ACCC's immunity and cooperation policy for cartel conduct could be discouraged from coming forward, if there is greater risk of data they report being shared.

Other risks of concern to businesses providing data to regulators, and third parties whose data can be compelled by the regulators under current regulatory regimes, include:

- **Information about individuals and other third parties:** Business regulators can obtain information about individuals in entities as part of licensing applications, reporting about governance including under the BEAR. It is unclear how this could be treated under the current drafting of the Bill. Secondly, data provided by regulated entities can be a 'blend' of data about services and products and data about the customers that use those services and products. This can include vulnerable or at-risk customers (child sexual abuse victims, domestic violence victims and child support matters). The data custodian's obligations relating to 'blended' data should be expressly clarified. The Bill does not appear to address the data custodian's obligations under the Privacy Act. Also see our comments about the interplay between the DAT regime and the Consumer Data Right (**CDR**) regime below.
- **Intellectual Property:** Given the volume of data given to business regulators on a regular, recurring basis, a regulator may not be aware of the existence of intellectual property and therefore not be aware that sharing of the data may be restricted under proposed section 17(3)(a)(i). It would be extremely time consuming to seek to tag all data subject to IP, particularly for data that has already been provided to regulators prior to the commencement of the regime. The ABA holds similar concerns about commercially sensitive data that can provide insights into business performance or practices.
- **National security and law enforcement data:** The current drafting excludes data held by national securities agencies, law enforcement agencies and AUSTRAC, but the same data can often be reported to business regulators and would be able to be shared.

Regulatory burden and unintended 'chilling effect'

In light of these risks, it is likely that many regulated entities will provide data to their regulators on the basis that the data is not protected by confidentiality safeguards. This would change how regulated entities provide data to regulators and potentially how regulators collect data.

Regulators may need to revise their data collection mechanisms to ensure that they are able to identify data that fall within one of the exclusions in the bill, for example, identifying where data is subject to

intellectual property (held by the regulated entity or another entity) or where the regulator has a common law duty of confidence. Regulators may also need to review their existing data for these exclusions. Regulated entities would likely need to conduct additional legal due diligence on all data provided to regulators, because they would need to consider whether any exclusions apply to some or all of the data, and if not, ensure the entity understands the potential impact of data being shared with third parties. In context of the banking industry where banks provide significant volumes of data to APRA, on a formal and voluntary basis, conducting such due diligence would be a significant additional regulatory impost.

The additional legal and operational regulatory impost can have a 'chilling' effect, such as on the speed with which regulators can obtain information from entities.

Proposed approach to business regulatory data

The ABA provides three proposals for consideration. Our key proposal is for the Bill to provide an exclusion from the regime for certain data covered by existing confidentiality regimes.

Exclude certain confidential data collected by business regulators

For the reasons set out above, the ABA proposes that the Bill provide an exclusion for data that is covered by existing confidentiality provisions in regulatory regimes, such as section 56 of the APRA Act. We recommend the Government consider ways to require greater openness from business regulators without dismantling critical confidentiality regimes.

This approach would be most effective in removing the concerns the ABA has outlined and ensure that business regulation remains effective, from both regulators' and regulated entities' perspectives.

If this is not possible, then the ABA strongly urges that any business data which is to be shared must be subject to additional safeguards:

- The Bill expressly enable business regulators to specify, in a legislative instrument, whether certain data is confidential for the purposes of this regime. This would be modelled on section 57 of the APRA Act, and the legislation should provide that data covered by a Determination is also excluded, potentially under proposed section 17(3).
- This proposal would in effect require business regulators to publicly consult about their approach to sharing data, in a manner similar to APRA's current approach.
- The Bill prohibit business regulators from sharing data that may identify an individual or an entity including through re-identification techniques.
- The Bill specifically exclude certain types of highly sensitive data as well as specify additional grounds on which a regulator may refuse a data request. This would provide the necessary legal certainty and address risks for regulators.
- The Bill clearly state that a decision by a regulator to refuse an application is not a reviewable decision.

Prohibit on-sharing of business data and addressing other risks

The ABA proposes the legislation prohibit data recipients from on-sharing business data, and this prohibition be supplemented by requirements in ministerial rules or data codes about use of up to date data, ensuring accurate interpretation and use of data, and storage of data. This proposal would address the following risks:

- The further data is shared away from the initial point of submission, the further away the user would be from understanding data taxonomy, definitions and the scope of data collection, the purpose for which data was collected, and other factors affecting how a data set was created. Permitting on-sharing of data increases the risk that the data is not fit for purpose or is misused (including unintentionally).

- Data projects that propose to use two or more data sets need to ensure adequate alignment of definitions. On-sharing of data increases the risk of mis-alignment leading to data being not fit for purpose or misused.
- These risks also exist where data is shared by the original data collection agency with other government agencies and the receiving agencies need to consider whether to share the data under the DAT regime. The ABA proposes the DAT regime consider how to address this concern.
- A governance concern is that the longer data recipients retain data, the more risk of the data recipient failing to track use of data and ensure governance, especially if there are changes in ownership, the structure of the entity or changes in personnel and systems. The DAT regime should ensure adequate consideration is given to this risk.

Additional data sharing principle

Also in light of the concerns outlined above, the ABA proposes the Bill include an additional data sharing principle dealing with commercial data. Where data is reported or provided by commercial entities, this proposed data sharing principle would require a data custodian to consider the benefits of sharing the data may be outweighed by the detriments. Detriments can include the inappropriate disclosure of commercially sensitive information and risks to the operations of a business regulator.

We propose the Bill include this additional data sharing principle, whether or not the Government accepts our proposed approach to business regulatory data. This is because data is collected from commercial entities under a broad range of Commonwealth legislation, and this proposed principle would explicitly acknowledge that there are competing considerations at play when a government department or agency proposes to share commercial data.

Alignment with other data and privacy regimes

The Government is implementing further stages of the Consumer Data Right (**CDR**) regime. It is critical that the DAT regime and the CDR regime provide a consistent framework for the use, disclosure and protection of data about customers, including a consistent approach to whether a customer's consent must be sought before his or her data is shared and whether an individual customer can opt out of either regime. Otherwise the protections provided under one regime can be unintentionally lost when data is shared under a different regime.

For example, an individual or corporate customer may consent for their data to be shared with an accredited data recipient under CDR. If the data is provided by the data recipient to a regulator under a compulsory information gathering power, it will be possible for that consumer's data to be shared by the regulator (as Data Custodian) with a third party (as accredited data recipient under the DAT regime), with the result that the customer loses the ability to control the use of their data as intended under CDR.

Finally, the ABA urges the government to ensure that the approach to data about individuals under this regime remains consistent with the outcomes of the Privacy Act review.

If you have any questions, please contact me at rhonda.luo@ausbanking.org.au.

Yours faithfully

Rhonda Luo
Director, Policy
0430 724 852

Australian Banking Association

Appendix

Types of data that may be reported

Specific examples of data and information submitted to APRA include:

- Internal governance and organisation of the business, which could include data about individuals. For example, board and committee papers and minutes, papers and minutes from business divisions, CPS220 Risk Management reports (annual and triennial) and annual declaration from the board, BEAR accountability statements, framework and governance documentation.
- Financial position of the entity, including market sensitive or commercially sensitive data. For example, capital management plans, capital and liquidity positions and forecasts, large exposure reporting.
- Strategy and operations of the entity. For example, strategy and operating plans for the business as a whole or divisions of the business, product approvals and strategies for specific business or product lines, risk appetite statements and reporting, ad hoc data requests (e.g. residential mortgage exposures).
- Potential weaknesses in critical aspects of the business or the business as a whole. For example, stress testing reports, recovery and resolution plans, risk reporting including market risk and credit risk, technology and information security reports under APS 234, operational resilience reporting.
- Current or potential regulatory matters. For example, internal and external audit reporting, remediation programme details and updates.
- Related parties or third parties. For example, select related entity notifications and consultations.