29 October 2020

The Australian Competition and Consumer Commission
GPO Box 3131
Canberra ACT 2601

By email lodgement: ACCC-CDR@accc.gov.au

Dear Commissioners,

Consultation on Proposed Changes to the CDR Rules

Quantium welcomes this opportunity to comment on expanding the Rules to allow for the entry of a greater number and type of businesses in the Consumer Data Right (**CDR**) regime.

We first provide background about Quantium's interest in the CDR and then provide our comments on key proposals and consultation questions.

Background as to The Quantium Group

The Quantium Group (**Quantium**) is an Australian owned group of companies. Our head office is in Australia. We also have operations in the USA, UK, South Africa, New Zealand and India. Quantium is 18 years old. We currently employ around 800 people, making us the largest specialised data science and AI business in Australia. We work with iconic brands in over 20 countries across government, insurance, retail, banking, FMCG, health, property and consumer services.

As a custodian of valuable, commercially sensitive customer data sets for leading Australian businesses, Quantium's business depends upon demonstrable and consistently reliable compliance with law and regulations, including as to bank - customer confidentiality and data privacy. Our data analytics environment is built upon data privacy, confidentiality and information security by design and by default. Confidentiality of each of our customer's data sets is critical to Quantium maintaining digital trust of our data partners, our clients and their customers. Quantium delivers on this requirement by deploying best practice frameworks, processes and technical, operational and legal controls and safeguards.

We respond to your requests for comments as below. We have only responded to certain of your questions. Numbering below follows numbering in your request for comment.

Quantium's response to consultation questions: Restricted level - limited data restriction

4. *What are your views on the low to medium classification of risk for the data set out in Table 1?*

   Quantium's view is that individual customer identifiable information (including but not only personal information about natural persons) should always be considered highly confidential and treated with the highest level of security. As such, the "Basic Customer Data" risk level should not be considered low risk as outlined in Table 1. While noting that date of birth is not included for natural persons, it is not clear whether other information such as telephone number, street address and email address are in scope.

   Similarly, Bank Payee data (specifically payees to other retail customers, friends, family) contains individual payee identifiable information, including (but not only) personal information about natural persons. These data sets might reasonably contain personally identifiable information that should be considered a higher level of risk than Basic Customer Data, because consent of the affected party (the payee) will generally not have been obtained from these third party payees.

However, and as the paper notes, practical ability to combine elements of the individual data types with other data sources creates a higher level of risk. The regulatory focus therefore should be on specification of good data handling practices that ensure consistently reliable data governance. Good data handling practices require technical, operational and legal controls and safeguards implemented within organisations, and clear allocation of responsibilities, accountabilities and liabilities across diverse and interworked data analytics environments, including environments operated by third-party (outsourced) providers of specialised services to ADRs and other multi-party data ecosystems where CDR data will be stored and analysed. Static risk classification of data types without consideration of the context and controls governing each data ecosystem is of limited utility.

5. *Are the accreditation criteria that apply to a person accredited to the restricted accreditation level (limited data restriction) appropriate for that level?*

   Quantium believe the accreditation criteria to be adequate for the proposed restricted accreditation level.

   There is a risk that regulation fuels a consultancy industry of conduct of third party information assurance assessments and audits. This relatively static (point-of-time) review process may simply add a deadweight cost of doing business for ADRs, may not sustainably lift standards across CDR data ecosystems, and may impede innovation in services. However, self-assessment against security controls requires careful articulation of requirements and regulatory expectations as to appropriate and reasonable security controls, so that self-assessment processes are appropriately reliable, objective, informed, professional and verifiable.

   Self-assessment criteria should include information security maturity assessments which specify required minimum levels of maturity against a well-developed criteria such as a Cyber Assurance Risk Rating (CARR) score.

   The scheme should be designed to facilitate continuous improvement over time through iterative maturity assessment applying well accepted criteria. Accordingly, the scheme should permit self-accreditation on the basis that the minimum level is assessed as already achieved, with a commitment to more and higher levels of maturity within a specified period.

   Entities might be required to self-report any incidents which are relevant to the currency and correctness of their self-assessment. Accredited persons will be highly motivated to ensure compliance with their self-assessment, given that data trust and reputation (of persons with who they deal) will be critical to their businesses.

6. *Do you consider the restricted level (limited data restriction) would encourage participation in the CDR? What are the potential use cases that this level of accreditation would support, including use cases that would rely on the scope of data available under this level increasing as the CDR expands to cover new sectors beyond banking?*

   Independent assurance reports are point-in-time and often a significant business expense that constitutes a barrier to entry for smaller ADRs. Independent assurance reports do not readily facilitate commitments to continuous improvement or create meaningful measures of continuous improvement.

   Substitution of properly objective self-assessment for a requirement for an independent assurance report should lead to more participation in the CDR and reduce further enrichment of assurance consultancy practices.

   Encouragement of broader participation in the CDR at this lower risk level may also bring forward tangible customer benefits: having an understanding of product information, account balance, and

regular payments enables a high level but meaningful assessment of the likely needs of a customer, to provide a range of additional products and services.

Quantium's response to consultation questions: Restricted level - data enclave restriction

7. *Do you consider the data enclave restriction would increase participation in the CDR? Where possible, please have regard to potential use cases in the banking sector and CDR rules expansion amendments future CDR sectors.*

   The core of Quantium's offering requires the use of client data sets to undertake analysis and provide actionable insights. The data enclave model would enable Quantium to work with CDR Data on behalf of Accredited Data Recipient clients in a transparent and regulated way, implementing a combined accredited person (CAP) arrangement. The data enclave model would enable clients to benefit from Quantium's experience and expertise in dealing with complex de-identified datasets including bank transaction data.

   The data enclave model has the benefit that the enclaved entity providing services to or through the 'data enclave provider' (a confusing term as it is used in the paper, but meaning the head ADR entity setting up the enclave) may undertake prior accreditation as required to operate as a provider of services within multiple data enclaves, so reducing friction for specialist third party services providers (such as Quantium) being engaged by multiple ADRs that each operate unique data enclaves.

   Regulation of each enclaved entity could then focus upon ensuring that the enclaved entity applies good data governance practices (including as to separation of client ADR data sets) and that it is a fit and proper persons to provide relevant data enclave services. These criteria should be sufficient for prior accreditation of entities as prospective providers of services within multiple data enclaves, given that the information security for a particular data ecosystem of a particular data enclave will be governed by the accreditation of the data enclave provider.

   Regulation should be moderate, because reputational, legal and client exposure of the enclave provider creates appropriate incentive for that regulated entity to self-regulate as to prospective enclave providers with whom the enclave provider deals: for example, incentive for the enclave provider to exercise due diligence about, to require contractual terms that include appropriate assurances (supported by indemnities) given by, and ensure oversight and reliable reporting by, the person accredited at the restricted level as an enclaved entity.

8. *Should the combined accredited person (CAP) arrangement between an enclave provider and a restricted level person include additional requirements, for example, in relation to incident management between the parties?*

   A person accredited at the restricted level might be required to self-report any relevant incident to the enclave provider.

   However, if regulation of combined accredited person (CAP) arrangements is appropriate to create legal incentive for the enclave provider to hold the person accredited at the restricted level to appropriately rigorous standards of data governance (including verifiably reliable processes, controls and safeguards), the negotiation of contractual provisions to reliably and verifiably effect that standard of data governance can be left to the enclave provider and the person accredited at the restricted level.

   As to how to ensure this appropriate incentive, see our response to 7. above.

9. *Should there be additional requirements under Part 1 of Schedule 2 for enclave providers in relation to the management of data enclaves?*

   See our response to 7. and 8. above.

Quantium's response to consultation questions: Restricted level - affiliate restriction

10. *Do you consider the affiliate restriction level would increase participation in the CDR? Where possible, please have regard to potential use cases in the banking sector and future CDR sectors.*

    Quantium believes the sponsor/affiliate model, as properly designed and implemented, should promote increased participation in the CDR.

    The sponsor/affiliate model and the data enclave model are of course closely related.

    As the models are explained in the paper, the difference might be said to be that the data enclave model imposes regulation directly and separately upon each of the enclave provider and the person accredited at the restricted level, and by so doing so allowing prior or standing limited accreditation for enclaved entities, while the sponsor/affiliate model imposes regulation predominantly upon the sponsor, and therefore needs to rely upon regulatory incentives imposed upon the sponsor being sufficient to ensure appropriate behaviour by the affiliate.

    The sponsor-affiliate enclave model has an existing data regulatory analogy which demonstrate the ability of such a model to work in practice. Under Australian Privacy Principle 8.1 and section 16C of the Privacy Act 1988, an APP entity disclosing personal information to an overseas recipient must take reasonable steps to ensure that acts and practices of the overseas recipient comply with the APPs. The disclosing entity is liable if the recipient engages in an act or practice that would have been a breach of the APPs if that had been an act or practice of the discloser. This so-called 'accountability principle' creates an accountability risk and direct legal exposure of the discloser which ensures that the (otherwise not regulated) recipient is held by the discloser to the same legal standard as the discloser.

    The sponsor-affiliate model is not the same as section 16C accountability liability: instead, it is proposed that the sponsor might be exposed to civil penalty provisions, and possible review of the sponsor's licence, in the event of relevant failures by the affiliate.

    Both the APP8.1/section 16C and proposed sponsor affiliate model properly allow for regulation to be low. There is no need for direct regulatory burdens upon the affiliate (a person accredited at the restricted level) as regulation may leverage from the direct exposure of the sponsor. Reputational, legal and client exposure of the sponsor creates appropriate incentive for that regulated entity to 'regulate by contract' with prospective affiliates with whom it deals. We query therefore whether direct regulation of an affiliate is necessary or desirable, beyond 'fit and proper person' accreditation.

    Of course, the sponsor should have a legal obligation to take active and reasonable steps (in addition to extracting contractual commitments) to ensure affiliates comply with accreditation requirements, coupled with sufficient liability exposure in respect of failures by affiliates that could have been avoided if the sponsor had taken appropriate steps, to in order to ensure the integrity of the sponsor/affiliate model.

11. *Should there be additional requirements under Part 1 of Schedule 2 for sponsors?*

    For reasons noted in our response to 10. above, the sponsor should have a legal obligation to take active and reasonable steps (beyond extracting contractual commitments) to ensure affiliates comply with accreditation requirements, coupled with sufficient liability exposure in respect of failures by affiliates that could have been avoided if the sponsor had taken appropriate steps, to in order to ensure the integrity of the sponsor/affiliate model.

12. *Where a sponsor and affiliate rely on a CAP arrangement, should the CAP arrangement include additional requirements, for example, in relation to incident management between the parties?*

As 8. above.

If regulation of combined accredited person (CAP) arrangements is appropriate to create legal incentive for the sponsor to hold the affiliate to appropriately rigorous standards of data governance, the negotiation of contractual provisions to reliably and verifiably effect that standard of data governance can be left to the sponsor and affiliate.

13. *The draft rules envisage that all of Schedule 2 will apply to an affiliate of a sponsor. However, depending on the relationship between the sponsor and the affiliate, there may be options to reduce the risk associated with this model which in turn could result in less controls being relevant for some affiliates. We are interested in views on whether a distinction could, or should, be made for different levels of access to data between sponsors and affiliates (some examples below), and, if so, what approach to assurance of the information security criterion may be appropriate.*

    Example level 1: affiliate is able to obtain access to any CDR data collected by the accredited sponsor and all data is held and managed on the affiliate member's systems.

    Example level 2: affiliate is able to access all data sets, but uses some of the sponsor's systems and applications to access or manage the data.

    Example level 3: affiliate obtains access to a limited amount of CDR data held by the sponsor, or entirely uses the accredited sponsor's systems and applications to access or manage the data.

    As we noted earlier in this submission, regulatory focus should be upon specification of good data handling practices that ensure consistently reliable data governance, including clear allocation of responsibilities, accountabilities and liabilities, across diverse data analytics environments, including third-party (outsourced) provision of specialised services to ADRs and other multi-party data ecosystems where CDR data will be stored and analysed.

    Static risk classification of data types without specific ecosystem context is of limited utility. There is a risk that overly prescriptive and detailed regulation will create unnecessary classification risks and associated regulatory burdens.

    If regulation of combined accredited person (CAP) arrangements is appropriate to create legal incentive for the sponsor to hold the affiliate to appropriately rigorous standards of data governance, the different levels of access to data as between sponsors and affiliates can be left to be determined as appropriate in each case by the sponsor and affiliate.

Quantium's response to consultation questions: expanding how accredited persons can work together

14. *We consider that in the case of a CAP arrangement, it is appropriate for the principal (having the relationship with the consumer) to be responsible for ensuring that customer-facing aspects of the CDR regime are delivered (for example, dashboards and any customer-facing communications, including in relation to dispute resolution). We welcome views on this position.*

    Quantium agree that the principal in the CAP arrangement is likely to be consumer-facing and should be responsible for customer-facing aspects of the CDR regime.

    Of course, "responsibility" in this regard is a reference to legal responsibility and presentation of an identified 'face' for consumer interactions, not a reference to which entity within a data enclave or sponsor-affiliate model provisions or operates customer-facing interactions. Retaining flexibility as to CAP arrangements allows different elements to be provided by different persons, accredited to the appropriate level.

Quantium's response to consultation questions: transfer of CDR data between accredited persons

15. *Should consumers be able to consent to the disclosure of their CDR data at the same time they give a consent to collect and a consent to use their CDR data?*

    Quantium believe that simple but clear single consent is likely to be better understood by consumers, and is therefore preferable to multiple (and potentially confusingly similar) consent steps.

    a. Is the proposed threshold for being able to offer an alternative good or service in rule 7.5(3)(a)(iv) appropriate?

    The requirement that the accredited person reasonably believes the consumer might benefit from goods and services is appropriate.

    b. The transfer of CDR data between accredited persons will be commonly facilitated through commercial arrangements. Should those commercial arrangements be made transparent to the consumer and, if so, to what extent?

    The over-arching legal prohibition of misleading or deceptive conduct should be effective to ensure adequate transparency to consumers. Commercial arrangements aren't typically transparent to the consumer, for example the commission a comparison service might receive for referring the consumer to a service. However, as the facts in *ACCC v iSelect* well demonstrate (https://www.accc.gov.au/media-release/iselect-to-pay-85-million-for-misleading-consumers-comparing-energy-plans), failure to disclose the practical effect of commission arrangements can be actionably misleading or deceptive. There do not appear to be particular or unusual characteristics of the CDR scheme that require a higher level of transparency to be mandated.

Quantium's response to consultation questions: greater flexibility for consumers to share their CDR data

16. *To which professional classes do you consider consumers should be able to consent to ADRs disclosing their CDR Data? How should these classes be described in the rules? Please have regard to the likely benefits to consumers and the profession's regulatory regime in your response.*

    The relevant question is one of assessment as a class of trustworthiness of classes of trusted advisors, which practically becomes a question as to the extent to which the regulator wishes to make its own assessment as to the trustworthiness of those classes, or to leaves that assessment to consumers.

    The classes proposed in the paper to be included as trusted advisors are accountants, lawyers, tax agents, BAS agents, financial advisors, financial counsellors, and mortgage brokers. The paper notes that some of these classes will hold either an Australian financial services licence or an Australian credit licence.

    We suggest that the relevant criteria should be whether:

    - the class is appropriately regulated by application of appropriate licensing criteria that regulate intake to qualified and fit and proper persons,
    - there is readily available verification mechanism so a consumer can easily ascertain whether a particular person is a member of the class,
    - there is independent oversight and enforcement of class rules,
    - there is a history of enforcement by the entity charged with oversight and enforcement of the class rules,

    such that consumers should have reasonable confidence that wrongdoing by members of the class will be detected, investigated and appropriately addressed and disciplined.

17. *Should disclosures of CDR data to trusted advisors by ADRs be limited to situations where the ADR is providing a good or service directly to the consumer? If not, should measures be in place to prevent ADRs from operating as mere conduits for CDR data to other (non-accredited) data service providers?*

    Disclosures of CDR data to trusted advisors by ADRs should be limited to situations where the ADR is providing a good or service directly to the consumer and that product or service is significantly different to a service of providing CDR data to that consumer.

18. *Should disclosures of CDR data insights be limited to derived CDR data (i.e. excluding 'raw' CDR data as disclosed by the data holder)?*

    Quantium supports the introduction of CDR data insights, and the ability to disclose them to any party once separated from identifying information. This enables a wide variety of use cases to be developed that do not require access to or disclosure of the raw CDR data, but that do require individual-level insight to be created for the benefit of the consumer.

    There is always a difficult question as to the acceptable magnitude of risk and possible harm associated with release of information that is pseudonymised by removal of direct identifiers, but not pervasively deidentified by removal or obfuscation of all direct or indirect identifiers such that reidentification risk can be reliably assessed as remote. The aim of the CDR scheme is to facilitate customer access to and use of data that relates to them, only with their consent, and only through intermediaries, trusted advisors or other recipients that they nominate and trust. There is a risk that a definition of CDR data insights that significantly raises the bar will impede customer access to and use of data that relates to them, with reduction in real and demonstrable risks to consumers.

19. *What transparency requirements should apply to disclosures of CDR data insights? For example, should ADRs be required to provide the option for consumers to view insights via their dashboard, or should consumers be able to elect to view an insight before they consent for it to be disclosed to a non-accredited person?*

    Quantium does not believe that there is inherently consumer benefit in regulating to require transparency of ADR data insights to consumers. Indeed, transparency may itself create questions for consumers, and possible confusion. For example, if the insight is a "financial wellbeing score" operating on a scale from 1 to 50, the interpretability of this score isn't meaningful to the consumer, without additional information such as the normal range of such scores, whether their score is increasing/decreasing and whether the information that lead to that score is complete and correct.

Quantium's response to consultation questions: permitting use of CDR data for research

Section 7.7 "Permitting use of CDR data for research" details the use of de-identified data for research. This amendment would allow, with consent, the use of data for research not directly related to the original reason for collection. Quantium supports the use of CDR data in this manner, providing it is not reasonably able to be re-identified in line with the CDR data de-identification process outlined in 1.17 of the CDR Rules.

We appreciate this opportunity to present this submission to the ACCC and are keen to constructively contribute to further determinations of the framework and rules for the CDR system.

We would welcome the opportunity to participate in industry consultations and to provide any detailed input or further clarifications as may assist the ACCC.

Please do not hesitate to contact me at [redacted] should you wish to discuss this further.

Yours sincerely,

[redacted]

Ben Ashton
General Counsel