Australian Government
The Treasury

TSY/AU

CONSUMER DATA RIGHT

PRIVACY IMPACT ASSESSMENT AGENCY RESPONSE

Treasury, ACCC, OAIC, Data61

Date created: December 2019

Manager
Media Unit
The Treasury
Langton Crescent
Parkes ACT 2600
Email: medialiaison@treasury.gov.au

CONTEXT

This document has been prepared by the agencies responsible for the design and implementation of the Consumer Data Right. It is intended to respond to the recommendations provided by Maddocks in their 29 November Privacy Impact Assessment (PIA).

Further discussion of potential privacy risks can be found in the Treasury's internal PIA published on 1 March 2019.

Maddocks Recommendation 1: Further updates to this PIA

Our analysis in this PIA report has been undertaken on the basis of the "point in time" development of the CDR Act, Draft Rules, Draft Data Standards and the Open Banking Designation (i.e. the legislative framework).

We **recommend** that this PIA report be treated as a "living document", which is further updated and/or supplemented as the various components of the legislative framework are revised and/or extended.

We also **recommend** that the criteria for triggering a further PIA should be clearly identified, and either included in the Draft Rules, or be otherwise publicly committed. For example, such criteria could include reconsideration of this PIA being triggered by any of the following being proposed:

- a change which would apply the CDR regime to another Sector;
- a change to the scope of the data for which the CDR regime will apply in a particular Sector;
- a change to the scope of Data Holders for which the CDR regime will apply in a particular Sector;
- the introduction of designated gateways or other intermediaries in a particular Sector, where this was not part of the initial implementation of the CDR regime for that Sector;
- changes to other legislation that affects, or intersects with, the privacy obligations under the CDR regime (such as future changes to the Privacy Act);
- changes that would alter the information flows identified in this PIA report, or would remove or reduce any privacy mitigation strategies identified in this PIA report;
- changes to the legislative framework (including the Draft Rules or Draft Data Standards) that would impact on the application of the Privacy Safeguards and/or APPs, or remove or reduce any privacy mitigation strategies in the legislative framework identified in this PIA report, or which would introduce new privacy risks; or
- a 'significant' Eligible Data Breach occurs (where 'significant' is defined as affecting a certain number of CDR Consumers, or having a defined likelihood or impact of harm).

In addition to the above, the Department could consider adopting regular reviews to assess whether any criteria have been triggered requiring this PIA report to be updated, and such reviews should be scheduled into the Department's work schedule.

This PIA report could also be updated or supplemented once further information about the Accreditation Register (e.g. information about its design and operation), and how it will operate within the ACCC's broader ICT system for the CDR regime, is available. For example, a future post implementation review could be conducted once all elements of the CDR regime are settled and finalised, including the Accreditation Register and the ACCC's broader ICT system for the CDR regime.

Agency response: Support

Assessments of privacy impacts are mandated for all changes to sectoral designation instruments (s56AD of the *Competition and Consumer Act 2010*) or Rules (s56BP). This is irrespective of the significance of the changes.

While not legislatively mandated, changes in data practices, adverse events or changes to non-CDR regulatory frameworks may also trigger privacy assessments.

The extent to which this will occur through the creation or revision of a Privacy Impact Assessment (PIA) will depend upon the potential significance of the impact. Agencies will rely upon the principles and criteria in the OAIC *Guide to Undertaking Privacy Impact Assessments*, May 2014 in determining when this threshold is met. While the *Privacy (Australian Government Agencies – Governance) Code 2017* legally compels agencies to conduct PIAs in certain circumstances, CDR agencies will adhere to the lower thresholds for conducting PIAs set out in the OAIC guidelines.

Further information on our commitments to conducting PIAs and our treatment of all PIAs as living documents can be found in the *Privacy Impact Assessment – Consumer Data Right*, 1 March 2019 (in particular pages 10 and 45).

Regular reviews are proposed for the regime as a whole, including in relation to its privacy impacts. The first holistic review, scheduled by July 2022, is required by s56GH of the Act. Other ways in which limited privacy health checks may occur (other than through formal PIA processes) include behavioural research into consumer consent processes and independent information security reviews.

Maddocks Recommendation 2: Further guidance on operation of the CDR regime

The CDR legislative framework, operating across different documents, is very complex. We suggest that guidelines which may be issued, and other activities which may be undertaken, by the Information Commissioner under section 56EQ in the CDR Act will be critical to ensuring that Data Holders, Accredited Data Recipients, outsourced service providers and CDR Consumers are able to understand their rights and obligations under the CDR regime.

We **recommend** that the Information Commissioner be asked to particularly focus on providing guidance about:

2.1 when the protections in the CDR legislative framework will apply to particular data (including explaining if data may be subject to both the APPs and Privacy Safeguards, and at what point the information is captured by the CDR regime and no longer falls within the protections of the APPs);

2.2 when entities will be a Data Holder under the CDR regime (and particularly when an Accredited Data Recipient may become a Data Holder in respect of CDR Data it has collected in accordance with the Draft Rules); and

2.3 when data will be defined as CDR Data (including explaining the complexities around "materially enhanced data" and data which is "wholly or partly" derived from other data).

Further guidance could also be provided:

2.4 about measures that Data Holders and Accredited Data Recipients can take to ensure that their APP Privacy Policy and CDR Policy can be easily accessed and compared by CDR Consumers;

2.5 to assist CDR Consumers to understand the implications if they agree to an Accredited Data Recipient de-identifying their CDR Data for the purposes of further disclosure;

2.6 to assist CDR Consumers, who wish to complain about privacy issues in connection with the CDR regime, to understand how their complaint will be managed, and by which regulator;

2.7. about the required treatment of redundant data, including the technical requirements for de-identification in accordance with the Draft Rules and Draft Data Standards; and

2.8. to assist Accredited Data Recipients and Data Holders in understanding the potential impact of any disclosure to a CDR Consumer of actual or suspected family violence as the reason for a refusal to provide CDR Data.

We note that since completion of the analysis in this PIA report, the OAIC has released further draft guidance about the CDR regime,1 and the OAIC may wish to consider whether that draft guidance appropriately covers the above issues.

We have noted the clear view expressed by some stakeholders that consumer education is not, by itself, likely to be sufficient to mitigate against identified privacy risks, and that this is particularly so for vulnerable CDR Consumers (where vulnerability is likely to be broader than just that related to lack of education or disability, but may include vulnerability related to financial or other stress). Accordingly, we do not consider that **Recommendation 2** in isolation is likely to be sufficient protection for these individuals or businesses.

Agency Response: Support
It is agreed that clarity is important to ensure that the Consumer Data Right can be properly and safely engaged with by those who wish to participate. The OAIC therefore bears an important role in providing guidance to help navigate the framework in place to allow for protection of consumers' privacy.

OAIC's Privacy Safeguard Guidelines (prepared under s 56EQ and currently being finalised having been open for public consultation from 16 October 2019 to 20 November 2019) go to the matters outlined in points 2.1 – 2.4. Guidance touching on the matters raised in 2.5 and 2.6 is planned, but as separate consumer guidance.

CDR rule 1.17 will require ADRs to have regard to *The De-Identification Decision-Making Framework* published by the OAIC and Data61. The OAIC is also currently considering creating further guidance on de-identification and the matters in point 2.7.

The Guidelines that have been consulted on and are in the process of being finalised are industry-focused. OAIC intends to release further guidance for consumers ahead of the launch of the CDR for consumer data.

Maddocks Recommendation 3: Further consideration of the Draft Rules

The Draft Rules have not yet been finalised. We **recommend** that the ACCC should be asked to consider whether the Draft Rules should be further amended before finalisation to:

3.1 include a process for testing a Data Holder's compliance with the Draft Data Standards (including when, how, and how often, testing will occur), possibly also including assessment of a Data Holder's security in relation to the transmission of CDR Data;

3.2 include an obligation on Data Holders to "warn" CDR Consumers when providing them with their CDR Data pursuant to their request (for example to state that the protections of the CDR regime (and possibly the APPs) will not apply if they provide that data to a third party). Similarly, if an Accredited Data Recipient discloses CDR Data to the CDR Consumer (which is a 'permitted use' of that CDR Data), indicate whether a similar protection is required in these circumstances;

3.3 require CDR receipts to be given in respect of both consents and authorisations, and also provide advice about what the CDR Consumer should do if the consent(s) and authorisation(s) recorded do not match their understanding of the consent(s) and authorisation(s) that have been given. The Draft Rules could also be clarified to determine the consequences if the CDR Consumer acts on this advice (e.g. whether the consent(s) and/or authorisation(s) are rendered void and need to be reobtained); or

3.4 expressly ensure that contractual arrangements between an Accredited Data Recipient and a CDR Consumer cannot override rights and protections provided to CDR Consumers by the legislative framework (e.g. by providing that any such clause will have no effect). If it is decided that it is not legally and/or technically necessary to implement this recommendation, we consider that the ACCC should take steps to ensure that Accredited Data Recipients have clear guidance in relation to the effect of attempting to override the rights and protections for CDR Consumers in the CDR regime.

Agency Response: Support in part

Recommendation 3.1: Support

Only four Data Holders are included in the initial launch of access to consumer data under the CDR. These initial Data Holders are being subject to specific testing tailored to their requirements; and are in fact actively engaged in those testing processes. These testing arrangements must be viewed in the context of existing banking regulatory systems governing information security and duties of confidentiality.

A business as usual approach to testing additional Data Holders beyond the initial four Authorised Deposit-Taking Institutions (ADIs) will be settled, informed by the testing that is currently taking place.

The proposal that Data Holders be required to be subject to specific testing relating to their capacity to engage with the CDR is being considered for future versions of the Rules.

Recommendation 3.2: Note

Requiring additional warnings to consumers of potential dangers of their directly distributing their data to third parties outside of the CDR system is not currently included in the Rules.

The privacy risks associated with providing human readable data directly to the consumer is lower than the risks of providing machine readable data, being similar to the risks associated with consumers currently having an ability to view their own bank statements. The suggested "warning" may unduly discourage consumers from accessing their data through the CDR

regime in a situation where privacy implications are lower than for other methods of data sharing, such as screen scraping, for which no warnings would be required.

That said, consideration will be given to having the option of providing additional requirements to "warn" consumers of potential dangers of distributing their data to third parties, subject to the outcomes of further CX testing.

Recommendation 3.3: Support in principle
The current requirement on Accredited Data Recipients (ADRs) to provide consent receipts was provided for following earlier consumer research into consent processes.

Consent receipt requirements apply in addition to obligations on ADRs to provide consumers with access to consumer dashboards. There are similar dashboard obligations upon Data Holders in relation to authorisations to share data. The balance of these disclosure obligations are expected to adequately inform customers of the status of all consents and authorisations. These dashboards are also required to provide user-friendly mechanisms for consumers to withdraw those consents and equivalent authorisations (for example, if they do not align with what the consumer intended).

OAIC and ACCC education and information material will be available to consumers regarding their rights if consents are inaccurately recorded – including processes for making complaints and for obtaining redress.

A balance must be achieved when determining when and where information is provided to consumers. Excessive information in consent screens may be counterproductive, in that too much detail may result in consumers 'clicking' through screens without reading any of the information they contain.

There will be ongoing research into how consumers actually engage with consent processes. This will provide an opportunity to refine the consent process to better promote consumer engagement and understanding in the future.

Recommendation 3.4: Do not support
The purpose for having a rule that explicitly states that a contract cannot override a rule would be to provide clarity on the face of the law for a reader. This clarity can be adequately provided for through information and guidance material, rather than providing additional detail in the law that does no more than state the natural hierarchy between legislation and contracts.

If a Data Holder or ADR seeks to enter into an arrangement that contravenes the law (including a rule), then following receipt of a complaint or report from an aggrieved party, the OAIC (or ACCC) may exercise their compliance and enforcement powers. Alternatively, if they are an individual or small business, they may seek redress through alternative dispute resolution arrangements. All Data Holders and ADRs must be members of approved dispute resolution schemes.

Earlier versions of the Rules had more detailed rules regarding this issue, but were amended following stakeholder feedback, including feedback that such additional provisions were unnecessary and created complexity.

Maddocks Recommendation 4: CDR Consumer right to access CDR Data held by the Accredited Data Recipient We **recommend** that the Department consider whether a right for CDR Consumers to access their CDR Data whilst it is held by the Accredited Data Recipient (similar to the rights afforded under APP 12) should be included in the CDR regime.
Agency response: Support In relation to ADRs, the CDR regime authorises an ADR to disclose to the CDR consumer any of their CDR data for the purpose of providing the requested goods or services (rules 7.5(1)(c) and 7.6). Clause 7.2 of Schedule 3 enables an ADR that is an ADI, with the consumer's consent to hold CDR data as a data holder. If the consumer agrees to this, then APP 12 would apply to that data. APP 12 continues to apply to Data Holders. It also continues to apply to ADRs in relation to non-CDR data. The rulemaking powers support the potential to extend the rights of consumers to access information held by ADRs. An APP12 equivalent rule for CDR data will be considered for a future version of the CDR Rules. It will be important to consult on the development of this rule given the likely costs for ADRs and the need to consider the form in which consumers should be able to access this information having regard to the risks referred to in recommendation 3.2.

Maddocks Recommendation 5: Draft Data Standards

We **recommend** that the Draft Data Standards should be recast into language that will allow CDR Participants to easily distinguish which parts of Draft Data Standards are binding legal requirements. Further, we **recommend** that as the Draft Data Standards change and are updated, there needs to be adequately detailed version control to allow for easy identification of any changes to the Draft Data Standards (to ensure the consistent implementation of the Draft Data Standards by all CDR Participants).

Agency Response: Support

The Data Standards Body (DSB) recognises that consumer adoption is critical to the success of the CDR regime. Consumer adoption will be influenced by the consistency with which industry adopts the Standards, especially in terms of the Consumer Experience (CX).

Since the release of version 1 of the Standards (30/09/2019), binding CX requirements (including for authentication) are now clearly included, along with version controlled change logs. In addition to these binding Standards, non-binding CX Guidelines continue to be provided in order to promote consistency. ADRs are required to have regard to these CX Guidelines when designing their consent processes to make them as easy to understand as practicable.

Standards and Guidelines are drafted having regard to relevant international standards, including RFC2119, which is considered best current practice. The purpose of using RFC2119 is to clearly indicate expectations of compliance levels to industry. The granularity provided by RFC2119 is appropriate because it allows industry flexibility in their approach, such as is required when trade-offs are imposed by various technologies. In certain situations, industry participants may be forced to not adopt certain optional suggestions in order to implement mandatory requirements. Maximum consistency would be achieved if all propositions in the Standards and Guidelines were universally adopted, but this is not pragmatic or realistic.

The DSB has undertaken an innovative and highly transparent approach to a public sector Standards development process. This stakeholder engagement has included the use of different channels designed to engage various communities, such as a public Github portal, a well-represented Advisory Committee for the Data Standards Body Chair (the Chair), and various working groups and public fora.

Consensus is impractical to achieve when dealing with the CDR's extensive and diverse eco-system of stakeholders from various backgrounds and interests. Issues such as authentication and consent have been extensively discussed, and will continue to be reviewed and reconsidered as the CDR evolves, matures and expands.

The DSB's advice to the Chair is informed by this stakeholder engagement, and is guided and framed by the principles outlined in both the Farrell Report, and on the Consumer Data Standards website. For example, the proposed decision to implement a One Time Password (OTP) was taken on principle in order to reduce security risks. Designing the CDR to specifically not ask for bank account passwords provides protection against phishing attacks. Trust in the safety and security of the CDR is critical for consumer adoption.
The methods and channels for the Standards and Guidelines are also being reviewed and reconsidered as the CDR evolves, matures and expands. As new Standards are released, the clarity of these new requirements is fundamental to the consistency of their adoption. The DSB has, and continues to take steps to educate relevant stakeholders and communicate these requirements, under the supervision of the Chair. Further details and examples of this are available through the DSB's various online channels.

Maddocks Recommendation 6: Joint account holders in the banking Sector

We **recommend** that the Department consider whether the CDR legislative framework implements an appropriate policy balance between the protection of the privacy of joint account holders, against the need to facilitate access to information by victims of family violence. The Department may wish to issue a public statement in this regard, explaining how the competing privacy and policy issues were considered.

Further guidance should also be provided about the operation of the CDR regime to joint accounts, including the level of evidence that a Data Holder requires in order to come to a view about whether it should refuse to update a joint account holder's Consumer Dashboard in order to prevent physical or financial harm or abuse.

Agency Response: Support – An information note on why Treasury considers the rules on joint accounts to strike an appropriate balance will be published shortly.
In developing the CDR Rules the ACCC sought to strike a balance between the protection of the privacy of joint account holders, and the need to facilitate access to information by victims of domestic and family violence. The existing provisions, which provide certain limitations in relation to joint account holders, were developed having regard to submissions from privacy advocates and groups that represent victims of domestic violence.

For example, the Rules currently provide certain limitations in relation to joint account holders. Clause 4.6 in Schedule 3 provides that if no election has been made by the two joint account holders to authorise the sharing of CDR data, then requests for data cannot be made to that account. Customer information about the non-requesting joint account holder is also excluded from the data that may be disclosed by a Data Holder (rule 3.2(3)(b) of Schedule 3). Similarly, the obligation to update each consumer dashboard does not apply if the Data Holder considers it necessary in order to prevent physical or financial harm or abuse not to update the consumer dashboard of the other joint account holder. This is to accommodate existing procedures a Data Holder may have to protect consumers, for example particular account arrangements relating to consumers that may be experiencing family violence.

The ACCC understands that many banks have policies and procedures in place to deal with customers experiencing domestic violence but that these procedures differ between banks and are not universally applied. Nevertheless, this is an area in which the ACCC and other agencies intend to have continued engagement with stakeholders representing domestic and family violence victims, as well as the banks to understand existing procedures and how they may be applied in the context of digital data sharing authorisations.

Treasury will issue a public rationale outlining in greater detail the considerations involved in arriving at the current determined position on joint accounts.

Maddocks Recommendation 7: CDR Data which includes personal information about third parties

We understand that, for the initial implementation, CDR Data which is disclosed by a Data Holder may include information about third party individuals (for example, transaction data about payment made to the CDR Consumer's account).

The third party individual will not have provided any consents (and is unlikely to be aware) that their information has been disclosed by the Data Holder to the Accredited Data Recipient, and will be used by the Accredited Data Recipient.

We understand that this issue has been carefully considered by the ACCC and the Department, including how this issue is treated in other jurisdictions (e.g. under the GDPR). We understand that the position that has been reached represents a balancing of interests, between the privacy rights of the third party individual against the utility for CDR Consumers to access and use their information, and the benefits of encouraging competition and innovation.

Although this disclosure will be permitted by law, we expect that the Australian community may have privacy concerns about this aspect of the CDR regime. We therefore **recommend** that the Department consider publishing information to support this aspect, including a clear description of the benefits for CDR Consumers, how privacy concerns have been balanced against the potential concerns third party individuals may have (including the reasons why personal information in relation to third party individuals is not required to be redacted by the Data Holder before release).

Agency Response: Support, see below.

Information that described a person's interactions with other people in society will not only be information relating to them but also information relating to those other people with whom they have engaged.

For example: Records that Jane has always paid rent to her landlord on time discloses personal information about them both.

A person's rights to share and use (or not share and use) information about their lives will therefore overlap and potentially conflict with other persons' rights to share and use (or not share and use) that information.

These rights may be relevant to protecting privacy or to protecting some other interests (such as economic security and wellbeing).

Agencies have extensively examined how these rights may be appropriately balanced; and has, in respect of banking information, adopted a similar outcome to that in the European Union General Data Protection Regulation (GDPR).

Other future data sets may be treated differently. Any future decisions will be informed by future PIAs.

Additionally, the Rules currently impose restrictions on the extent to which an ADR can develop profiles and insights into third parties.

Preventing the sharing of certain information, such as transaction data that may include information about third party individuals, would materially reduce the benefits of the CDR regime. To facilitate the CDR to a workable extent, it is necessary that third party information is provided.

Maddocks Recommendation 8: Seeking CDR Consumer agreement for an Accredited Data Recipient to become a Data Holder of CDR Data

We **recommend** that the ACCC considers whether the Draft Rules should incorporate additional protections about *how* the Accredited Data Recipients may seek agreement from the CDR Consumer for an Accredited Data Recipient of CDR Data to become a Data Holder, similar to the protections currently afforded for how consent may be sought.

Agency Response: Support

Rule 7.2 sets out a process that is required before a relevant ADR (i.e. an ADI) can treat banking data collected through the CDR in accordance with the privacy, confidentiality and security requirements that ordinarily apply to banking data, rather than in accordance with the requirements imposed under the CDR.

This process imposes requirements to ensure that the consumer understands that the CDR requirements will cease to apply, how the data will be treated, why the bank is entitled to seek this change in the status of the data and the consequences of not agreeing to this change. Actual agreement by the consumer to the change is required.

Notwithstanding these existing provisions, and recognising the significance of the loss of the additional protections afforded by the Privacy Safeguards, the ACCC is working with the DSB to undertake consumer experience testing on the requirements for when an ADR may become a Data Holder of CDR data as part of the next phase of CX research.

The findings of this testing is likely to inform what, if any, changes may be incorporated into the Rules.

Maddocks Recommendation 9: Adequate ACCC and OAIC resourcing

The OAIC and ACCC, as the relevant regulators, will have critical roles to play in ensuring that risks identified in this PIA report are appropriately addressed, through the provision of suitable guidance material and the implementation of effective monitoring and enforcement regimes.

We have not investigated, or been provided with, any information about current or future funding levels for these agencies, but we **recommend** that the Department consider whether the OAIC and ACCC will have the necessary funding and resources to provide appropriate guidance material and undertake other educational activities, and to implement effective monitoring and enforcement regimes.

Agency Response: Support
Funding decisions are a matter for Government. The Government has committed substantial funding to the ACCC and OAIC.

Further funding information is available in Australian Government Budgets and Mid-Year Economic and Fiscal Outlooks.

Maddocks Recommendation 10: Consistent and effective complaints and compliance processes

We **recommend** that the ACCC and the OAIC have consistent processes so that complaints by CDR Consumers about their privacy under the CDR regime are handled by the appropriate regulator. This could include, for example, similar or identical processes and information on their websites.

We **recommend** that external dispute resolution schemes for each Sector be carefully considered, with additional guidance and resources provided as appropriate, to ensure effective resolution of any issues experienced by CDR Consumers.

We also **recommend** that the OAIC and the ACCC consider the strategies that should be included in a compliance framework for the CDR regime, and whether these should be made publicly available.

Agency Response: Support
The OAIC and ACCC are implementing the Government's clear 'no wrong door' approach to complaint handling, ensuring that consumers will have their concerns addressed regardless of which regulator they approach.

Current work includes providing consumer guidance on complaints, to ensure consumers understand which entities are collecting their information and handling their complaint.