FinTech Australia

Consumer Data Right Rules: consent and operational enhancements amendments consultation

Submission

September 2024

fintechaustralia.org.au

About this Submission

This document was created by FinTech Australia in consultation with its members. In developing this Submission, interested members participated in roundtables to discuss key issues and provided feedback to inform our response to the consultation paper.

About FinTech Australia

FinTech Australia is the peak industry body for the Australian fintech sector, representing over 450 fintech companies and startups across Australia. As part of this, we work with a range of businesses in Australia's fintech ecosystem, including fintechs engaging in payments, consumer and SME lending, wealthtech and neobanking, the consumer data right (CDR) and the crypto, blockchain and Web3 space.

Our vision is to make Australia one of the world's leading markets for fintech innovation and investment. This submission has been compiled by FinTech Australia and its members in an effort to advance public debate and drive cultural, policy and regulatory change toward realising this vision, for the benefit of the Australian public.

FinTech Australia would like to recognise the support of our Policy Partners, who assist in the development of our submissions:

- Allens
- Cornwalls;
- DLA Piper;
- Gadens;
- Hamilton Locke;
- King & Wood Mallesons; and
- K&L Gates.

Executive Summary

FinTech Australia recognises the great opportunities that the CDR presents for Australian consumers and businesses. We are excited by the potential for the CDR to support the rapidly developing data-driven economy in Australia. We welcome the opportunity to provide a submission on the exposure draft rules which simplify the consumer consent process and contain a number of operational enhancements (**Draft Rules**).

In preparing this submission, we consulted extensively with our members. In general, FinTech Australia is supportive of the Draft Rules, and considers that they are an important step forward for the CDR ecosystem. Some FinTech Australia members consider that certain aspects of the Draft Rules require further consideration before implementation. These relate to:

- the application of the data minimisation principle (**DMP**) and the term "reasonably needed", particularly within the context of bundled consents and disclosure consents (proposal 1.1) requires further clarification;
- the proposed requirement to provide information about supporting parties within the consent flow (proposal 1.6), which risks adding to consumer cognitive fatigue when considering that this information is already required to be disclosed within the Accredited Data Recipient's (**ADR**'s) CDR Policy;
- the proposed 'deletion by default' treatment of redundant data (proposal 1.7), which risks preventing ADRs from being able to safely use de-identified for critical use cases (such as fraud prevention) and product development;
- the proposed 12-month deferral for the introduction of changes to the nominated representatives process (proposal 2.1), which is too long and should be confined to 3 months, and the absence of a mechanism to deem those with administrative authority as nominated representatives which would reduce data holders' operational burden;
- further expanding the proposal to allow accredited ADI data holders to hold CDR data as data holders, to allow all data holders that have been designated under the CDR (Data Holders) who are also ADRs to hold CDR data they ingest as Data Holders (and not ADRs) (proposal 2.2). This would create a level playing field, including across all designated industries;
- the liability and the civil penalties imposed on CDR representative principals (principals) for their representatives' actions, which are too onerous (proposal 2.3); and
- specific use case guidance and further guidance being required for adequate participant understanding.

Further detail on these matters is set out below. FinTech Australia is supportive of these initiatives but members consider that the current proposed drafting requires further refinement as it may lead to unintended consequences contrary to the aims of the CDR.

Separately, FinTech Australia members agree that there remains further substantial work to be done to improve participation in and the effective operation of the CDR ecosystem. With this goal

in mind, this submission outlines other recommendations on how the CDR can be further bolstered, including:

- removing derived data from the definition of CDR data, or introducing use cases where derived data is not to be treated as CDR data. Without such a change, the Rules risk limiting the true potential of the CDR by hampering the ability of any ADR, affiliates, representatives, or accredited data holders to develop new offerings built with CDR data; and
- improvements to the consent authorisation process to help prevent consumer drop-off in the consent journey due to its complexity or technical issues.

We look forward to consulting with Treasury and the Data Standards Body on the future of the CDR.

1 Proposed changes to the consumer consent process

1.1 Allowing a data recipient to bundle CDR consents, so that consumers can give multiple consents with a single action

FinTech Australia supports the bundling of CDR consents to enable consumers to give multiple consents with a single action. This is a welcome step to streamline the consent process. Importantly, consumers should be provided with sufficient information in a simple and accessible manner to provide informed consent.

The consultation paper and exposure draft provide that the collection, use, and/or disclosure consents can only be bundled if "*reasonably needed*" to provide a good or service. Though the "reasonably needed" standard is a feature of the DMP, CDR Rule 1.8 has a circular definition and the DMP itself requires consideration of whether something is "*reasonably needed*."

FinTech Australia members had differing views regarding whether consent bundling should be subject to a "reasonableness" test. Some noted that without further guidance, the term "*reasonably needed*" could be underinclusive and result in consent bundling requests involving multiple separate consents, defeating the purpose of bundling in the first place. Others could be overinclusive in their consent bundling, which could result in unnecessary consents being granted. In such circumstances, the participant may have inadvertently breached the Draft Rules. This, in turn, may have a chilling effect on participation in the CDR ecosystem as participants may not supply CDR services if they are not fully confident in their regulatory obligations. Other members were of the view that a reasonableness test is appropriate in a principles-based legal framework.

Clearly defining, with examples and scenarios, the standard of when disclosure bundling is and is not "*reasonably needed*" would help ensure that fintechs are clear on their obligations as 'gatekeepers' between data holders and CDR consumers. For example, where a consumer uses a personal finance management tool that offers integrated savings insights, bundling the collection, use and/or disclosure consents for transaction data and savings information may be reasonably needed to ensure the service can be provided effectively and efficiently.

1.2 Allowing a data recipient to pre-select the elements of an individual consent that would be reasonably necessary for the data recipient to provide the good or service

FinTech Australia supports this proposal, as it enhances consumer experience and reduces the risk of consumers failing to complete consents due to 'consent fatigue'.

1.3 Simplifying the information a data recipient is required to provide to the consumer at the time of consent

FinTech Australia supports this proposal.

1.4 Allowing a data recipient to consolidate the delivery of 90-day notifications to reduce consumer notification fatigue

FinTech Australia supports this proposal.

1.5 Simplifying the obligations in relation to CDR receipts

FinTech Australia supports this proposal.

1.6 Requiring a data recipient to provide consumers information about all supporting parties who may access the consumer's data at the time a consumer gives consent

FinTech Australia members agreed with the intention to provide clear information to consumers about supporting parties in an easily accessible form. However, some members believed this proposal did not meaningfully improve transparency for consumers, and came at the expense of a clear, simple consent flow. This is on the basis that information about outsourced service providers (**OSPs**) is already required to be included in the ADR's CDR Policy, and including it within the consent flow, particularly where multiple OSPs are in use, can increase consumers' cognitive fatigue and inhibit their ability to digest more critical information in the consent flow that is not disclosed elsewhere.

1.7 Requiring data recipients to delete redundant CDR data unless a consumer has given a de-identification request

While we agree a clear, privacy-protective approach to redundant data is essential, a number of FinTech Australia members consider that the proposed 'deletion by default' approach would effectively prevent de-identified data being used for legitimate and vital use cases like fraud detection and product development, to the ultimate detriment of consumers and CDR's long-term viability. Requiring an explicit de-identification consent from consumers in these circumstances is likely to result in the vast majority of CDR data (including derived data) being subject to deletion as consumers:

- are likely not accustomed to regularly providing such consent in other circumstances (given that the use of de-identified data is commonly permitted under privacy and data protection laws in other regimes and carries less privacy risk than data capable of re-identification); and
- are unlikely to take the time to proactively opt-into a de-identification request in a consent environment where we understand consumers are already experiencing cognitive fatigue, and may be unwilling to invest the time to understand the value of the consent or the choice they're required to make.

This would largely prevent ADRs from safely using de-identified data for essential tasks, including fraud and scam monitoring and prevention, training AI/ML models and product maintenance and innovation. For example, ADRs would largely be unable to use such de-identified CDR data to perform essential audit, review and product improvement tasks such as long run credit portfolio analysis, and building and reviewing credit risk and responsible lending models. This is despite some members noting that data holders are not required to obtain a specific consent to de-identify consumer data such as transaction data for similar purposes and that the proposed deletion by default treatment would therefore provide data holders with an unfair advantage over ADRs, many of whom are fintechs.

While FinTech Australia members have acknowledged that 'deletion by default' is likely to engender consumer trust and align with the expectations of some consumers, others

remain concerned that these potential benefits are overshadowed by broader impacts on competition and consumer access to innovative and fairly-priced products and services. Given this, some FinTech Australia members believe the current treatment that allows ADRs to define whether the data is deleted or de-identified at the end of the expiry period is appropriate, especially given that de-identified data does not carry the same privacy or security risk as data that is reasonably capable of re-identification.

We recommend further industry consultation on this issue so that the proposed 'deletion by default' approach to redundant data can be reviewed in light of contemplated broader changes to the Privacy Act, helping ensure consistency with the de-identification requirements for other types of personal information.

1.8 Requiring a data recipient to advise consumers of the marketing activities they will undertake because of a direct marketing consent

FinTech Australia members had differing views on this issue. Some supported this proposal as a welcome transparency measure for consumers or did not have specific views, while others noted that it was not necessary to prescribe in detail how a data recipient must ask for a direct marketing consent from a consumer, particularly where there is broad stakeholder feedback that the consent process needs to be simplified.

2 Proposed operational enhancements

2.1 Nominated representatives

FinTech Australia supports the CDR Rule changes to require data holders to provide a simple process for non-individuals to appoint nominated representatives and to offer an online process for account administrators with online access to an account to be appointed as nominated representatives. This is a positive step towards enhancing business consumer participation in the CDR ecosystem, and better reflects the realities of business practice.

To facilitate this, FinTech Australia members also suggest that the Draft Rules deem any person who has administrative authority over an account to be able to exercise rights over CDR Data. This should allow CDR participants to rely on existing processes to provide authority to deal with CDR Data on behalf of a party who is not an individual. 'Deeming' those with administrative authority as nominated representatives would reduce operational and technical costs for data holders, and enable them to more quickly implement system changes. This would also reduce the risk that those seeking to appoint online administrations turn to alternative solutions such as screen scraping, which can be completed in a more timely manner.

In addition, the suggested 12-month lead-in period for data holders to implement relevant system changes is unduly conservative. This will delay the benefits this change attempts to realise, and specifically delays the CDR uptake by small businesses, which the Minister recognised as a top priority. We believe that shortening the deferral of the commencement of these obligations to 3 months should be sufficient and will encourage increased business consumer participation sooner.

Furthermore, even though the Draft Rules propose the appointment process be "simple and straightforward", this may result in ambiguity for data holders and mean that different processes are employed by each data holder. There is no proposal for uniformity in how nominated representatives are appointed. This could make it more time-consuming for business consumers to appoint nominated representatives to different data holders.

To provide for a more consistent consumer experience, the specific appointment process should be prescribed by either Treasury or the Data Standards Body. These should be linked to consumer experience data standards, which directly relate to Decision Proposal 350. Additionally, data holders should be required to action nominated representative appointments in an expedient manner and some members have cautioned against the use of online forms which can lead to multi-day delays. An immediate action requirement with a maximum 30-second delay would be consistent with the expectations of modern digital services and would significantly enhance business consumer user experience. We believe these two matters can be effectively addressed by imposing Service Level Agreements on data holders.

2.2 Expanding the circumstances in which accredited ADIs can hold CDR data as a data holder

We support the broadening of the existing circumstances in which an accredited ADI can hold CDR data as a data holder, rather than as an ADR in the circumstance where it is both. It is a step in the right direction and provides a workable solution to the practicalities of how ADIs operate.

FinTech Australia members believe this concession should not be limited to ADIs. Rather, it should be broadened to allow all data holders from any designated sector that are also accredited data recipients to hold CDR data as data holders. Such an extension would promote the objectives of the CDR as it would allow consumers to experience positive benefits from a multi-sectoral 'buy-in' into the CDR.

This extension would encourage innovation and promote accredited data holders to develop new products or services that are built to leverage and use the CDR ecosystem, rather than the CDR being an 'afterthought' for existing offerings. Doing so can incentivise competition within various sectors, not just amongst ADIs. Additionally, this would allow for increased participation in the CDR ecosystem, especially from fintechs, and allow them to reach scale more quickly.

If this concession is limited exclusively to ADIs, non-ADI financial service providers would be at a disadvantage, contrary to the CDR's stated aim of increasing competition. This risks creating a lopsided system, where non-ADI financial service providers are not afforded the same opportunity as ADIs to develop their offerings using this data. One means by which this could be expanded is by allowing data holders who hold other licences, such as Australian financial services licences and Australian credit licences, to be granted the same concession as ADIs, and if necessary, be subject to meeting a published cybersecurity standard in their own right to address any potential concerns that they are not subject to the same detailed cybersecurity standards as APRA-regulated entities.

2.3 CDR representative arrangements

Some FinTech Australia members have expressed concerns with the proposed CDR Rule to expand the liability imposed on a principal for their representative's actions. The Draft Rules impose liability on a principal in circumstances a representative does not comply with the:

- consumer experience data standards as if the representative was an ADR; or
- required terms of their CDR representative arrangement, even if the required term is not included in the written contract between the principal and the representative (whether by direct action or omitting to take action).

This level of liability, when coupled with the application of civil penalties for non-compliance, is onerous and could have a chilling effect on the engagement of CDR representatives. CDR participants could be more reluctant to engage representatives, given the potential liability they could be exposed to in circumstances where they may not have asked the 'right' questions to the representative. This has the potential to undo the "substantial" participation increase in the CDR assisted by the introduction of the CDR representative model.

Some members have reiterated that an appropriately balanced approach, which ensures principals are held accountable for the actions of their representatives while not discouraging the use of representatives, would best foster wide adoption of the CDR across Australia. Achieving this balance is complex but may draw on principles of agency to determine an appropriate framework which imposes obligations on the principal and recourse against the representative in certain circumstances.

2.4 Simplifying data holder requirements – secondary users

FinTech Australia does not have any specific views in relation to this issue.

2.5 Exempting energy trial products from the CDR

FinTech Australia does not have any specific views in relation to this issue.

3 Specific use case guidance

Though the explanatory materials and guiding principles contain some examples of how the Draft Rules would work in practice, FinTech Australia members do not believe these provide sufficient clarity. The explanatory notes and guiding principles should include further examples and scenarios to illustrate the practical application of the Draft Rules. This is particularly important given the infancy of the CDR, and the need for an appropriate level of legislative and regulatory guidance to ensure a successful and effective future for the CDR.

Any examples should cover a range of situations that CDR participants may encounter, which includes but is not limited to the rule changes we have commented on above. These examples would ensure the rule changes have been considered from a practical perspective and will help all participants, including participants like fintechs who help the

flow of or deal with CDR data, to better understand their role within the CDR ecosystem, including their responsibilities and obligations.

For example, further specific guidance should include:

- when and how CDR participants who are data holders and ADRs, but are not ADIs can hold CDR data as a data holder and not an ADRs, as suggested in paragraph 2.2 above;
- step-by-step examples, potentially in the CX Standards, that outline how nominated representatives may be appointed, including by differing levels of scenario 'complexity' to reflect the various business structures and authorisations that may exist;
- what constitutes "reasonably needed" data for the purposes of collection, use, and disclosure consents (including how the DMP is applied) in various data sharing and service contexts; and
- examples or tailored case studies of when a CDR principal will be liable for the actions or inactions of their representative. Additionally, providing some liability mitigation measures or guardrails a principal can implement.

4 Further recommendations to improve the effectiveness of and participation in the CDR

While FinTech Australia members think the Draft Rules will generally improve the operation of the CDR and welcome most of the changes, further and stronger action needs to be promptly taken to ensure the CDR is fit-for-purpose and can reach its full potential.

We believe addressing the following two matters will help facilitate growth within the CDR ecosystem and increase the adoption and use of CDR in Australia.

4.1 Derived data

Under the CDR Rules, derived data includes data wholly or partly created from or based on CDR data. It includes materially enhanced information, being data about the use of a product that has become significantly more useful as a result of analysis or insight. Derived data is treated as CDR data. This means that the obligations relating to CDR data infect an overly broad range of data.

The treatment of derived data as CDR data is an impediment to the overarching purpose of the CDR, as it creates complexity in classifying data, and requires careful consideration of whether data that has been transformed to various degrees still constitutes CDR data. If entities can be forced to disclose data, including to competitors, that they have made valuable by cleaning existing data or consolidating it from different business units, they will be disincentivised from generating new information designed to give them a competitive advantage using CDR data. Instead, there may be a preference to not use CDR data as data provided through other means is not subject to the same restrictions.

Instead of protecting consumers, this has had an unintended consequence of limiting CDR participants' ability and willingness to innovate and provide new offerings. By attaching the

same obligations to derived data as 'primary' data, the stringent sharing and consent requirements can act as a disincentive for data holders to develop products and services that are built with the CDR data. It also creates significant issues for non-bank lenders, particularly when seeking to share derived data with their funding investors. Specifically, derived data may be required to be shared with banks or superannuation funds as part of their credit due diligence process or period file reviews. Further, derived data (such as income or risk score) may be required to be shared with investors who fund securitised pools of loans which is the predominant means by which fintech lenders are able to fund their loan books.

Ultimately, this limits the true potential of the CDR as entities may not consider it worthwhile to invest in CDR based products or services, and fintech lenders may be inhibited from exchanging data with funding partners to improve their access to capital. We believe many of the concerns with the current treatment of derived data can be resolved in a number of ways, including by:

- removing derived data from the definition of CDR data.[1] This would provide clarity for CDR participants and allow for freer experimentation with new products and services, provide greater certainty about what data is covered by the CDR, and would also remove the (arguably onerous) obligations on CDR participants to ensure derived data complies with the CDR Rules. We note that contemplated legislation to amend the Privacy Act may provide a legislative vehicle for consequential amendments to the Competition and Consumer Act, and an opportunity to reassess the CDR derived data framework in light of broader changes to the privacy regime; or
- introducing use cases or classes of derived data that are not to be treated as CDR data (and not subject to the same stringent privacy restrictions). This would allow for targeted exemptions for certain types of derived data. Exemptions could be provided for derived data thought to be low-risk, or for priority use cases, such as products or services related to budgeting, lending, or energy comparisons and switching.

Excluding forms of derived data from CDR data would therefore encourage a more competitive, more innovative market. Without the risk of being required to disclose value-added data to their competitors, a business, for example, could create a solution to process and analyse consumer financial data derived from CDR data and generate new insights and financial solutions for consumers, while reducing compliance costs. Fintech lenders too could benefit from improved access to capital when they are able to exchange derived data with their funding partners.

4.2 Consent authorisations

FinTech Australia members have expressed concerns about significant consumer drop-off rates during the consent authorisation process. While we acknowledge the efforts made to streamline the consent process (outlined in proposals 1.2-1.5 above), further enhancements are needed to ensure consumers are not abandoning the authorisation

[1] FinTech Australia notes that it is likely necessary to amend the Competition and Consumer Act to facilitate the removal of derived data from CDR data. However, it may also be possible to amend the CDR Rules in relation to CDR data in some circumstances.

process due to its complexity or easily solvable technical issues. In particular, two solutions would allow entities to better understand, and potentially build product experiences to address, this issue:

- public reporting on rates of consumer drop-off during the consent authorisation process. This could include reporting on the stage in the process in which drop offs occur, as well as rates of successful One-Time Password (**OTP**) delivery. Some members have noted this would be best achieved by mandatory reporting requirements on data holders; and
- requiring OTPs to be delivered to consumers by data holders within certain timeframes specified in Service Level Agreements.

In addition, we recommend including further guidance and wireframe examples in the CX Guidelines of more simplified, user-friendly authentication and consent flows, including options for app-to-app authentication and minimising redirects to different platforms/user interfaces, which can increase consumer cognitive fatigue.