



14 October 2022

Rules Unit  
Consumer Data and Digital Division  
Treasury  
Langton Cres  
Parkes ACT 2600  
By email: [data@treasury.gov.au](mailto:data@treasury.gov.au)

## Consumer Data Right rules - Operational enhancements

The Australian Banking Association (**ABA**) notes Treasury's consultation on the Consumer Data Right (**CDR**) – Operational enhancements.

The ABA supports a CDR rollout that balances the need for innovation and expansion of use cases with the need ensure the security and privacy of customer data. We note the proposed enhancements to allow businesses to share their data with more parties and extend business use and disclosure consents for 7 years present additional risks that need to be carefully considered.

The need to protect and uplift data security across the economy is key given recent data breaches.

### Safety-by-design

The ABA reiterates the need to take a safety-by-design approach to implementing changes in the CDR.<sup>1</sup> The key principles as outlined by the eSafety commissioner should guide all CDR proposals.

The first key principle is the idea that the potential risks of online interactions should be assessed upfront and there should be active steps taken to engineer out potential misuse, reducing people's exposure to harms. The second requires the need to support the dignity of users and to design features and functions that empower individuals with choice and act in the best interests of those users. The final principle provides that there should be an ability for consumers to best understand the risks they face and options to address those risks upfront.

The ABA **recommends** that all three are considered in this context ahead of making further changes.

### Allowing business consumers to share their data with more third parties

The ABA acknowledges the intent of this proposal is to provide additional flexibility for businesses to share data to more third parties and enable the CDR ecosystem to grow. A key use case appears to be for business to share data with their bookkeepers and accounting software more seamlessly and also enables many different use cases where data recipients can offer services to businesses.

While Rules 3.0 enabled customers to share data outside of the CDR environment to unaccredited parties, those recipients had existing professional obligations which were to provide sufficient protection. The proposed extension in these rules go further, placing no requirements on unaccredited third parties to secure customer data. The ABA recommended against the disclosure of CDR data to trusted advisers given the risks involved and reiterate our concerns over the further reductions in protections as reflected in this proposal.

Business data is a key target for scammers as it contains valuable information that can be used to exploit businesses in a number of ways. For example, scammers can use transaction data to impersonate another entity, build trust and ultimately scam businesses. With this proposal, recipients of that data can be prime targets by scammers.

Further, the proposal provides the data is to be shared via a specific business data consent. However, for many businesses, it is not possible to separate personal and business data, and the consent would

<sup>1</sup> See Letter on 13/7/2022 from the ABA, Financial Rights Legal Centre, Consumer Action Law Centre and the Consumer Policy Research Centre.



result in unaccredited persons accessing both personal and business data. Nothing in the proposals appear to prevent this. Even for businesses that can clearly separate business and personal data, we note that business data requires at least the same level of protection as personal data since small businesses are frequently the target of scammers and cyber-attacks.

Finally, we consider that rather than seeing imposing stricter security requirements on third parties as an impediment to CDR expansion, it should be seen as an opportunity to increase the security posture for how data is managed and handled across the economy. The framework for the CDR should continue to place the integrity, security and safety of customer data at the heart of the CDR, and we are concerned that this proposal serves to water down these key objectives.

### Extend business consumer use and disclosure consents from 12 months to 7 years

The ABA considers that the data minimisation principle should be retained in every context where CDR data used. Enabling a 7-year consent for use rather than asking a business to revisit the consent every 12 months may result in consent being sought for 7 years as the default. Many businesses may not read the fine points of a contract and may not realise their data would be held for this length of time.

The proposals seek to ensure customer data is not inadvertently deleted if they have not produced a consent. We further note that only certain categories of data can be subject to this provision, and it does not apply to disclosure or collection. There are also notification requirements so that businesses will be aware of such sharing arrangements where sharing has been dormant for 90 days, and also to notify them of their collection consents. We support these safeguards and understand the concerns.

However, proposal can result in ADRs retaining business customer data for longer periods of time than potentially required, with customers having to sign 'take it or leave it' contracts where they do not have a genuine choice. This can raise risks for business consumers. As recent events suggest, the longer the data that can be held, the more exposed those businesses are to data breaches and may become a more attractive target.

### Reciprocity exemption

We finally note the changes to exempt accredited parties from sharing data for 12 months under reciprocity rules. It is not clear why an entity should be accredited if they are not in a position to share data, and we consider there should be a case-by-case basis for exemptions rather than allowing for a blanket exemption. We do not support this change as proposed and note its detrimental impact on competitive neutrality and competition within the CDR.

Thank you for the opportunity to provide feedback. If you have any queries, please contact me at [Prashant.ramkumar@ausbanking.org.au](mailto:Prashant.ramkumar@ausbanking.org.au)

Yours sincerely,

Prashant Ramkumar  
Associate Policy Director,  
Australian Banking Association