RSM Australia Pty Ltd

Level 21, 55 Collins Street Melbourne VIC 3000
PO Box 248 Collins Street West VIC 8007

T +61 (0) 3 9286 8000
F +61 (0) 3 9286 8199

www.rsm.com.au

30 July 2021

Consumer Data Right Division
Treasury
Langton Cres
Parkes ACT 2600

By email: data@treasury.gov.au

Submission to Treasury on Consumer Data Right rules amendments (version 3)

RSM Australia welcomes the opportunity to comment on Treasury's proposed CDR Rules amendments.

About RSM Australia

RSM Australia is a leading provider of audit, tax, and consulting services for entrepreneurial growth-focused organisations, with over 150 Partners and Principals and over 1,200 staff operating out of 30 offices throughout Australia. We deliver highly personalised services and have repeatedly won national awards for the quality of our client service, most recently in March 2021 when we won the Australian Financial Review (AFR) Client Choice Award for Best Accounting & Consulting Services firm (Revenue > $200m).

RSM Australia is an independent member firm of RSM, the 6th largest professional service accounting and consulting organisation in the world. As a registered auditing firm (Chartered Accountants Australia & New Zealand), RSM Australia has suitably experienced and qualified individuals who can complete independent assurance reports in accordance with International / Australian Standards on Assurance Engagements (ISAE/ASAE) as lead information security assurance practitioners (including SOC 1/2 reports).

RSM Australia's experience completing CDR information security accreditation assurance reports

RSM Australia provides Consumer Data Right (CDR) information security accreditation assurance and advisory services. As well as providing CDR control assessment program, gap assessment and readiness services, we are the most experienced CDR auditor having provided CDR assurance reports (ASAE 3150) for over 50% of the FinTech unrestricted Accredited Data Recipients. This includes: Frollo, Intuit, Adatree, Finder and Basiq.

As well as the completed CDR assurance reports, RSM is working with over 20 other potential applicants to become Accredited Data Recipients. This experience has given us a clear understanding of the challenges facing an organisation seeking to become an ADR.

Overarching approach to information security assurance

Based on the experience of APRA for compliance with CPS 234 organisations do not know how to comply with information security requirements. RSM Australia has identified many issues with applicants (ADI's and non-ADIs) not understanding the Rules.

All participants in CDR need to comply with the information security requirements in Schedule 2 of the Rules. Therefore, they all need to document the boundaries of the CDR data environment and implement a Controls Assessment Program. Given this is already a requirement of the Rules, we propose that all applicants (ADI, non-ADI, unrestricted, representative agents and affiliates) should be required to submit the CDR data environment boundaries document and the outcomes from the Control Assessment Program to the DRA for accreditation. This would provide a more consistent approach to information security, without any additional costs for applicants. The only difference to this should be that the unrestricted non-ADI is required to provide an independent assurance report (consistent with current Rules) and sponsors and representatives should obtain assurance that their affiliates and agents comply with the Rules.

Sponsored level of accreditation

Further clarifications are required on the practical implementation of this model. Given a sponsor is required to implement a third party management framework, any breaches by their affiliates will mean that the third party management framework is not effective and therefore the Sponsor has a liability if an affiliate breaches the Rules.

It should be a requirement of sponsored accreditation to have a sponsorship arrangement in place, to provide the DRA with assurance that the sponsor has performed their third party obligations. Otherwise, the situation may occur where the DRA has accredited the affiliate as meeting the Rules but a sponsor subsequently identifies that the affiliate does not comply with the Rules. This may have unintended consequences of affiliates shopping around for sponsors that have weaker third party assurance controls. The Sponsor should therefore also provide attestation that they have met their obligations for the affiliate accreditation.

Similar to Schedule 2 Part 1 Control Assessment Program, any self-assessment on the implementation of controls to meet Schedule 2 should be performed by persons with suitable knowledge and understanding of the controls and their expected operations (technical expertise), but independent from the day-to-day performance and administration of the control.

For proposed Rule 2.2, it should be clarified whether the Sponsor can outsource the assistance or training in technical and compliance matters e.g. can a sponsor engage RSM Australia to provide assistance in technical matters, noting that the Sponsor will still be responsible and liable for compliance with the Rules.

Schedule 2 Requirement 7 annual review and assurance activities should explicitly state independent annual review and assurance activities on the design and operating effectiveness of information security controls to comply with Schedule 2. This still provides the sponsor with a principle based approach on how to obtain the assurance e.g. independent and appropriately skilled self-assessment or independent assurance report, based on the nature and context of the services being provided by affiliates, but makes it clear that the assurance is required to meet a minimum threshold of coverage.

Due to the reduced assurance threshold for affiliates, the sponsor should be required to provide an explicit annual attestation for each affiliate that the sponsor has performed an independent annual review and obtained assurance that the affiliate complies with its obligations as an accredited person. This could be included in the current annual attestation statement.

To better manage the risks of non-compliance, we propose that a sponsor must report to DRA no later that 10 business days after it becomes aware of a material information security control weaknesses by an affiliate, which the sponsor expects will not be able to be remediated in a timely manner.

CDR representative model

Further clarifications are required on the practical implementation of this model.

Are the representative agents in scope for the Principal's CDR Data Boundary for the unrestricted assurance report (non-ADI) (should a Principal seek to make an application as an unrestricted ADR, knowing they will have representative agents) and assurance report every 2 years (non-ADI and ADI)? Under the carve-in audit model in the Supplementary Accreditation Guidelines Information Security, it seems that they would be included, but this is not clear in the proposed Rules.

Does the Principal need to comply with Schedule 2 Requirement 7 and with proposed Rule 2.2? The proposed Rules seem to apply to only the Sponsor/Affiliate model, not the Representative model. This seems unusual, given there is no other oversight of the agent other than the oversight provided by the Principal and there is a high risk of non-compliance with the Rules.

The proposed Rules indicate that the Consumer will have the right to a pseudonym. How is a pseudonym and Privacy Principle 2 able to be applied in the Banking Sector? If it can't be applied to the Banking sector, this should be removed from the Privacy Impact Assessment, and risks appropriately noted.

Collecting outsourced service providers

We have no comments given there are no proposed changes to the threshold of de-identification, and the OSP still needs to comply with all the Rules and will be included in the 'carve-in' assurance report for non-ADIs unrestricted accreditation assurance report.

Expanded data sharing arrangements - Trusted advisers

Under the current Rules a consumer can be provided (disclosed) their CDR data and once done the consumer can do what they want with that data, for example, they could provide it to a Trusted Advisor. This is a manual and insecure way to transfer CDR data. We see the proposed Trusted Advisor model as merely automating the current rights of the consumer. From a Privacy Impact Assessment perspective, this is lower risk than the other method currently open to the consumer under CDR. We therefore support sharing with additional Trusted Advisors, such as book-keepers under a consent model.

Expanded data sharing arrangements - CDR insights

The proposed Rules do not allow an ADR to share CDR insights with unaccredited systems within their own IT environment. Any ADR system interacting with CDR insights needs to comply with the Rules. This is anti-competitive for ADRs compared to non-ADR's who can obtain the same insight data (with the same Privacy Impact Assessment) but do not have to harden the systems using the insight to comply with the Rules.

Under the proposed Rules, if an ADR shares an insight with another ADR, the insight is considered data derived from CDR data. Again, this is anti-competitive for ADRs compared to non-ADR's who can obtain the same insight data (with the same Privacy Impact Assessment) but do not have to harden the systems using the insight to comply with the Rules.

For example, if an ADR creates its own insight (or an ADR to ADR insight is used), this is deemed data derived from CDR data and any data interacting with it will be considered data derived from CDR data. So, if the insight is a validated bank account but that bank account is then used to process a payment, the processing of a payment is not within the four insight categories and it is therefore not possible to share with an unaccredited organisation (noting this could potentially fall under an OSP arrangement, but for a non-ADI the OSP is included in boundaries of the CDR data environment for the accreditation). A non-ADR could use the insight to validate a bank account then process a payment with no restrictions.

The cost to harden all systems within an organisation to use CDR data (or data derived from CDR data) is cost prohibitive for many organisations. The Rules should be amended to enable sharing of an insight with any organisation (including with unaccredited systems within an ADR), not just an unaccredited organisation.

Regards

Darren Booth

Darren Booth
Partner/Director, National Head of Cyber Security & Privacy Risk Services
RSM Australia Pty Ltd