RSM

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

20 July 2020

CDR Rules team
GPO Box 3131
Canberra ACT 2601

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

Dear Sir or Madam

Submission to the Australian Competition and Consumer Commission (ACCC) on Consumer Data Right (CDR) Rules consultation - Draft rules that allow for accredited collecting third parties ('intermediaries')

RSM welcomes the opportunity to comment on the ACCC's proposed CDR Rules that would allow accredited persons to utilise other accredited parties to collect CDR data and provide other services that facilitate the provision of goods and services to consumers. RSM is one of Australia's leading professional services firms, with a national partnership of over 100 Partners and Principals and over 1,200 staff operating out of 30 offices throughout Australia. RSM in 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 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. RSM has completed independent assurance reports for the CDR information security accreditation in accordance with ASAE 3150 – Assurance Engagements on Controls for two Accredited Data Recipient (ADR) applicants. This experience has provided us with valuable insights on the CDR Rules, including defining the boundaries of the CDR data environment, Schedule 2 Part 1 and Part 2. We would therefore like to highlight the following for consideration by the ACCC:

Proposed minimum control: Encryption in transit

The description of minimum controls does not specify whether this control applies to transit related to the internal (i.e. the trusted network of the CDR data environment) and/or external (untrusted) network. This clarification is required to ensure ADRs and ADR applicants understand the investment and security requirements.

Proposed minimum control: Data segregation

The description of minimum controls states that data needs to be segregated but does not specify whether other shared resources also need to be segregated. Examples of this could include non-transactional audit logs (noting that transactional audit logs would be classified as derived CDR Data), shared server or database

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM Australia Pty Ltd is a member of the RSM network and trades as RSM. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm which practices in its own right. The RSM network is not itself a separate legal entity in any jurisdiction.

RSM Australia Pty Ltd ACN 009 321 377 atf Birdanco Practice Trust ABN 65 319 382 479 trading as RSM

Liability limited by a scheme approved under Professional Standards Legislation

resources, shared scripts, etc. Further clarification on the segregation scope and whether it applies to these other shared resources would ensure ADRs and ADR applicants understand security requirements within a CAP arrangement.

It could also be made clear that the segregation of CDR data that is stored or hosted on behalf of an accredited data recipient from other CDR data should be explicitly included in the scope of penetration testing.
Whilst not directly requested by the ACCC, we would also like to provide the following feedback on the existing CDR Rules based on our recent experience:

Boundaries of the CDR data environment scope

The CDR Rules state that the CDR data environment means '*the information technology systems used for, and processes that relate to, the management of CDR data*'. Whereas the 'CDR - Supplementary accreditation guidelines information security' states that the boundaries of the CDR data environment '*involves identifying the people, processes, technology and infrastructure that manages, secures, stores or otherwise interacts with CDR data,…may include infrastructure owned by, and management provided by, an outsourced service provider or third party*'. The inconsistent inclusion of the words '*interacts with*' results in confusion for ADRs and ADR applicants. 'Interacts with' indicates that the CDR Rules applies to all system components included in or connected to the CDR data environment, including system components indirectly connected, impacting the configuration or security, or providing security services to the CDR data environment.

'The CDR Rules and the 'CDR - Supplementary accreditation guidelines information security' could be updated to align wording. If 'interacts with' remains, the ACCC could provide further guidance to ADRs on the scope of the boundaries the CDR data environment, similar to that provided by the PCI Security Standards Council for scoping a cardholder data environment https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1.pdf

Current minimum control: Restrict administrative privileges

The controls states that '*Privileges granted on an ongoing basis are regularly reviewed to confirm their ongoing need.*' The use of the word 'regularly' provides a point of confusion for ADRs and ADR applicants, as regularly is interpreted differently. Whilst the 'CDR - Accreditation controls guidance.xls' provides additional guidance that it should be monthly, this is not included in the Rules, unlike the 'Access security' minimum control, which states a frequency.

Current minimum control: Limit physical access

The control states that 'premises of business operation' are in scope. The modern working environment means that staff can do anything remotely that they can do whilst physically in the premises of business operation, making premises of business operation redundant as a physical control. The CDR Rules could be updated to remove this requirement (noting other controls on data loss prevention).

It is noted that the 'CDR - Accreditation controls guidance.xls' states a combination of location and office network may be considered as an authentication factor for Multi-factor authentication. Many information security professionals would disagree with physical access being a valid authentication factor. If this is still deemed appropriate by the ACCC, controls to limit physical access to premises of business operation should instead be linked to this control guidance.

Current minimum control: Firewalls

The controls states '…*review configurations on a regular basis.*' The use of the word 'regular' provides a point of confusion for ADRs and ADR applicants, as regular is interpreted differently. The CDR Rules could state that this should be aligned to industry best practice (six-monthly review) or state a frequency, like the 'Access security' minimum control, which states a frequency.

Current minimum control: Data loss prevention

Whilst the controls stated seem valid, the scope of CDR data (and derived data) results in the control ‘email filtering and blocking methods that block emails with CDR data in text and attachments’ being impractical to implement. Filtering and blocking systems are unable to identify whether text is CDR data or non-CDR data with similar attributes. The CDR Rules could be updated to instead focus controls on preventing downloading of CDR data to locations outside the CDR data environment e.g. file shares, workstations, printers.

Current minimum control: Vulnerability management

The controls states ‘…*regular vulnerability scanning and penetration testing on systems within the CDR data environment.*’ The use of the word ‘regular’ provides a point of confusion for ADRs and ADR applicants, as regular is interpreted differently. The CDR Rules could state that this should be aligned to industry best practice (at least annually or after any significant change to the CDR data environment) or state a frequency, like the ‘Access security’ minimum control, which states a frequency.

Current minimum control: Application whitelisting

The Australian Cyber Security Centre (ACSC) have recently updated terminology from application whitelisting (which is typically a specific solution used for Microsoft Windows operating systems) to the more generic term ‘implement application control’. The CDR Rules could be updated to align terminology with the ACSC.

The ACSC recognises that implementing application control within Linux environments is challenging https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-linux-environments. The CDR Rules could be updated to provide options to comply with this control depending on whether the ADR operates a Microsoft Windows environments or a non-Microsoft Windows environment. As it is currently worded an ADR applicant operating a non-Microsoft Windows environment will likely have a qualified assurance report.

Regards

[redacted]

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