Consumer Data Right Rules
Version 3 amendments

The Treasury

22 July 2021
Overview

Consultation update

A. Single consent model for joint account data sharing

B. New pathways to participation (Sponsored accreditation, CDR Representatives and collecting OSPs)

C. New authorised disclosures (Trusted advisers and CDR insights)

Questions can be submitted via slido.com with code #178 412 please identify topic at the beginning of your qn: A, B, or C.
Joint accounts: single consent model for joint account data sharing

• Allows joint account holders to consent share data, unless data sharing has been disabled by another account holder
• Current rules require all account holders to ‘turn on’ data sharing before a consent can be given
• Oversight, control, and consumer protections remain in place for all account holders

Policy intent:
- Improve consumer experience and convenience for joint account data sharing
- Keep in place current oversight, control and consumer protections
Joint accounts: example

Page 20 of Explanatory Materials:

• Bob and Erin have a joint account at Peanuts Bank
• Either Bob or Erin can ask Peanuts Bank (a data holder) to share data from their joint account to an accredited data recipient
• Erin gives consent for Penny Savers (an accredited data recipient) to collect data from the joint account and authorises Peanuts Bank to disclose the data to Penny Savers
• Peanuts Bank notifies Erin and Bob of the disclosure and updates their consumer dashboards
Joint accounts: existing consumer oversight and control mechanisms maintained

- Notifications to account holders when new sharing arrangements are initiated or ceased
- Oversight and control of joint account sharing arrangement provided through ‘consumer dashboards’
- Consumers can:
  - Disable (‘turn off’) data sharing from a joint account
  - Stop individual data sharing arrangements where these are in place
- Consumers will be notified about the change to the joint account rules at least one week before they come into effect
- Exemptions apply to data holder obligations where considered necessary to prevent physical or financial harm or abuse
Joint accounts: Key obligations for data holders

• The commencement date for the draft rules is 1 April 2022
• Data Holders must:
  – apply the ‘pre-approval’ disclosure option to joint accounts
  – notify joint account holders of the default sharing setting and how they may set data sharing to ‘off’, at least 7 business days prior to the commencement of the revised rules
  – allow joint account holders to set notification preferences in accordance with any data standards
• ‘Co-approval’ disclosure option remains optional implementation
New pathways to participation

1. Sponsored level of accreditation
2. CDR representatives
3. Collecting outsourced service providers (OSPs)

Policy intent:
- Increase uptake of CDR (consumers and participants)
- Leverage partnerships to lower barriers to entry
- Maintain consumer protection and trust
- Provide flexibility
Sponsored accreditation

- New level of accreditation
- Must be sponsored (an ‘affiliate’ of a sponsor) to receive CDR data
- Information security capability evidence - self-assessment and attestation
- Sponsors: have obligations in respect of their affiliates, including due diligence and support
<table>
<thead>
<tr>
<th>Sponsorship</th>
<th>CDR representatives</th>
<th>Collecting OSPs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parties:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unrestricted ADR</td>
<td>Sponsored ADR</td>
<td>Unrestricted ADR</td>
</tr>
<tr>
<td>(sponsor)</td>
<td>(affiliate)</td>
<td>(principal)</td>
</tr>
<tr>
<td><strong>Can collect from DHs:</strong></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Can collect from ADRs (AP disclosure consent):</strong></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Must comply with the CDR framework</strong></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Liable for breaches of CDR framework?</strong></td>
<td>✓ - liable for own actions as an ADR, sponsorship liability extends to: liable for meeting obligations that apply to sponsors and liable for collection on behalf of an affiliate</td>
<td>✓ - liable for own actions as an ADR, but not for collection when sponsor collects</td>
</tr>
</tbody>
</table>
CDR representatives

- An unrestricted accredited person can engage an unaccredited person as their CDR representative under a CDR representative arrangement
- A CDR representative can provide goods/services to consumers using CDR data
- An unrestricted accredited person is liable for its CDR representatives
<table>
<thead>
<tr>
<th>Parties:</th>
<th>Sponsorship</th>
<th>CDR representatives</th>
<th>Collecting OSPs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Unrestricted ADR (sponsor)</td>
<td>Sponsored ADR (affiliate)</td>
<td>Unrestricted ADR (principal)</td>
</tr>
<tr>
<td>Can collect from DHs:</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
</tr>
<tr>
<td>Can collect from ADRs (AP disclosure consent):</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Must comply with the CDR framework</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Liable for breaches of CDR framework?</td>
<td>✓ - liable for own actions as an ADR, sponsorship liability extends to: liable for meeting obligations that apply to sponsors and liable for collection on behalf of an affiliate</td>
<td>✓ - liable for own actions as an ADR, but not for collection when sponsor collects</td>
<td>✓</td>
</tr>
</tbody>
</table>
Collecting Outsourced Service Providers (OSPs)

- Expands OSP rules to enable accredited persons to use unaccredited OSPs to collect data on their behalf
- Accredited persons are liable for their OSPs
<table>
<thead>
<tr>
<th>Sponsorship</th>
<th>CDR representatives</th>
<th>Collecting OSPs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parties:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unrestricted ADR (sponsor)</td>
<td>Unrestricted ADR (principal)</td>
<td>Unaccredited person (CDR rep)</td>
</tr>
<tr>
<td>Sponsored ADR (affiliate)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unrestricted ADR (principal)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unaccredited person (CDR rep)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Can collect from DHs:</strong></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>×</td>
<td></td>
</tr>
<tr>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>Can collect from ADRs (AP disclosure consent):</strong></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>Must comply with the CDR framework</strong></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Liable for breaches of CDR framework?:</strong></td>
<td>✓ - liable for own actions as an ADR, sponsorship liability extends to: liable for meeting obligations that apply to sponsors and liable for collection on behalf of an affiliate</td>
<td>✓ - liable for own actions as an ADR, but not for collection when sponsor collects</td>
</tr>
</tbody>
</table>
New Authorised Disclosures

- Trusted advisers
- CDR Insights

Policy intent:
- Expand the range of services enabled by the CDR and drive participation
- Allow CDR data to be disclosed to unaccredited persons in certain circumstances
- Empower consumers, while maintaining protection and trust
Disclosures: Trusted Advisers

Categories of trusted advisers:
• accountants; lawyers; tax agents, BAS agents and tax advisers; financial advisers and financial planners; mortgage brokers; and financial counselling agencies (financial counsellors)

Consumer protections:
• The ADR must take reasonable steps to confirm data recipient is in a TA category
• Transfer of the CDR data by an ADR to a trusted adviser to be covered by the information security controls in Schedule 2, including the requirement for encryption in transit
• The ADR must update the consumer dashboard to indicate what and to whom data was disclosed
Disclosures: CDR Insights

Consumers will be able to consent to accredited persons disclosing CDR data to unaccredited persons for the following limited purposes:
- identifying the consumer
- verifying the consumer’s account balance
- verifying the consumer’s income
- verifying the consumer’s expenses

The CDR insights policy is intended to allow consumers to share simple information that has been verified using CDR data with a wider range of recipients.
Disclosures: CDR Insights

Consumer protections

• Data minimisation principle
• Need for the ADR to explain the CDR insight when seeking consent
• The CDR insight cannot include sensitive information within the meaning of *Privacy Act 1988*
• Transfer of CDR insights to recipients are to be covered by the information security controls in Schedule 2, including the requirement for encryption in transit
• The ADR is to update the consumer dashboard with a description of the CDR insight and to whom it was disclosed
• The ADR is required to keep records of any CDR insights disclosed
Disclosures: CDR Insights

Examples of CDR insights:
• Identifying the consumer when signing up to a new utility provider.
• Verifying the consumer’s account balance and notifying a service provider to remind the consumer to ‘top-up’ their account for a forthcoming payment.
• Verifying the consumer’s income and current rental expenses for a rental application.

Verification = Confirming, denying or providing other simple information about the consumer in relation to one of listed topics
Questions

Questions can be submitted via slido.com with code #178 412

Please identify topic at the beginning of your qn:

A - Joint accounts
B - Pathways to participation
   (Sponsored accreditation, CDR representatives, Collecting OSPs)
C - Trusted Advisers and Joint accounts