EXPLANATORY STATEMENT

Issued by authority of the Minister for Superannuation, Financial Services and the Digital Economy

Competition and Consumer Act 2010

Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021

Section 56BA of the *Competition and Consumer Act 2010* (the Act) provides that the Minister may, by legislative instrument, make consumer data rules for designated sectors in accordance with Division 2 of Part IVD of the Act.

The Consumer Data Right (CDR) is an economy-wide regime which gives consumers access to and control over their data, and the ability to obtain products and services from accredited persons using CDR data.

The purpose of the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021* (the Amending Rules) is to amend the *Competition and Consumer (Consumer Data Right) Rules 2020* (the CDR Rules) to:

- facilitate greater participation in the CDR regime by participants and consumers;
- provide greater control and choice to consumers in sharing their data;
- promote innovation of CDR offerings including intermediary services; and
- enable services to be more effectively and efficiently provided to customers.

Schedule 1 to the Amending Rules implements the sponsored accreditation model. This reduces the cost of accreditation by altering certain obligations to establish information security capability as part of the accreditation process and ongoing accreditation obligations.

Schedule 2 to the Amending Rules establishes the CDR representative model. This allows eligible participants to access the CDR and use data without the need for accreditation in circumstances where they offer CDR-related services to consumers as a representative of an accredited data recipient.

Schedule 3 to the Amending Rules allows consumers to nominate persons as ***trusted advisers*** to whom an accredited person may disclose the consumer's data outside the CDR regime. The classes of trusted advisers are professions that are considered to be appropriately regulated to ensure a strong level of consumer protection is maintained.

Schedule 3 to the Amending Rules also introduces the concept of a CDR insight. This allows CDR consumers to consent to their data being shared outside the CDR regime for prescribed purposes that are considered low risk and that are designed to limit the data shared to only what is necessary for the consumer to receive a service.

Schedule 4 to the Amending Rules provides for joint accounts to be in scope for data sharing under the CDR by default (a 'pre-approval' setting), with mechanisms by which a joint account holder may adjust or change the pre-approval option also

provided. Any joint account holder may withdraw a consent for data sharing on an account at any time.

Schedule 5 to the Amending Rules provides for staged implementation of rules relating to joint accounts and 'direct to consumer' obligations in the banking sector.

Schedule 6 to the Amending Rules enables an accredited person to rely on unaccredited outsourced service providers to collect CDR data and thereby reduce the cost of building and operating application programming interfaces that connect to data holders.

Schedule 6 to the Amending Rules also makes consequential and minor amendments, with Schedule 7 to Amending Rules setting out transitional matters relating to the joint account amendments.

Details of the Amending Rules are set out in Attachment A.

A Statement of Compatibility with Human Rights is at Attachment B.

Before making consumer data rules, section 56BP of the Act requires the Minister to have regard to certain matters outlined in section 56AD. These include the effect of the rules on the interests of consumers, the efficiency of relevant markets, the privacy and confidentiality of consumers' information, and the regulatory impact of the rules. The Minister has considered each of the factors required by the legislation when making the Amending Rules.

Section 56BP requires the Minister to be satisfied that the Secretary of the Department has arranged for consultation as required by the Act and a report before the rules are made. This requirement has been met.

Section 56BP also requires the Minister to wait at least 60 days after the day public consultation begins before making consumer data rules. With public consultation having commenced on 1 July 2021 with publication of draft exposure rules on the Treasury website, this requirement has been met.

An exposure draft of the Amending Rules was released for consultation from 1 July 2021 to 30 July 2021. Submissions were received from 56 respondents. Stakeholders were largely supportive of the proposed reforms. Feedback from stakeholders has been taken into account in drafting minor changes to the Amending Rules post consultation.

Schedules 1 to 4 to the Amending Rules implement recommendations of the 2017 Review into Open Banking, which was previously certified by Treasury as having undertaken a process and analysis equivalent to a Regulation Impact Statement. These amendments are not considered to significantly impact on the estimate of annual regulatory costs assessed for the implementation of the CDR Rules. Schedules 5 and 6 are minor in nature. On this basis, the Office of Best Practice Regulation (OBPR) advised that a Regulation Impact Statement was not required (OBPR reference ID 24996).

The Amending Rules are a legislative instrument for the purposes of the *Legislation Act 2003*.

The Amending Rules commenced on the day after they were registered on the Federal Register of Legislation. Schedule 1 commenced on 1 February 2022. Schedule 2 and certain items in Schedule 6 relating to outsourced service providers commenced on

the day 14 days after registration of the Amending Rules. Schedules 3, 4, 5 and 7, and the balance of Schedule 6, commenced on the day after registration.

ATTACHMENT A

Details of the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021*

Section 1 – Name of the instrument

This section provides that the name of the instrument is the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021* (the Amending Rules).

Section 2 – Commencement

This section provides that sections 1 to 4 of the Amending Rules commence on the day after the Amending Rules are registered. It also provides that the Schedules to the Amending Rules commence as follows:

- Schedule 1 on 1 February 2022;
- Schedule 2 and certain items in Schedule 6 relating to outsourced service providers (items 1, 2, 3, 15, 18 and 19) – on the day 14 days after registration of the Amending Rules; and
- Schedules 3, 4, 5 and 7, and the balance of Schedule 6, on the day after the Amending Rules are registered.

Section 3 – Authority

The Amending Rules are made under the *Competition and Consumer Act 2010* (the Act).

Section 4 – Schedules

This section provides that each instrument specified in a Schedule to this instrument will be amended or repealed as set out in the applicable items in the Schedule concerned. Any other item in a Schedule to this instrument has effect according to its terms.

In citations of provisions in this explanatory statement, unless otherwise specified:

- references to Schedules in citations of provisions in this explanatory statement are to Schedules to the Amending Rules, unless otherwise specified; and
- references to rules are to CDR Rules.

Schedule 1 - Amendments relating to sponsored accreditation

Background

Schedule 1 to the Amending Rules introduces a new level of accreditation designed to reduce barriers to entry for parties who wish to participate in the CDR regime as accredited persons. The new level of accreditation is known as sponsored accreditation.

The sponsored level of accreditation is for persons with or who intend to have an arrangement with an unrestricted accredited person who is willing to act as their sponsor in the CDR regime. Persons with sponsored accreditation are restricted from accessing CDR data directly from data holders.

A person accredited to the sponsored level and in a sponsorship arrangement is known as an affiliate of its sponsor.

Persons who wish to participate in the CDR regime as affiliates must have sponsored accreditation, an arrangement with a registered sponsor, and have this arrangement published on the Register of Accredited Persons before they can access CDR data.

An affiliate is an accredited person and is required to fulfil the obligations of an accredited person in the CDR regime. This includes (but is not limited to) compliance with dispute resolution obligations, the privacy safeguards and consent rules.

The accreditation criteria for sponsored accreditation are the same as for unrestricted accreditation. However, an affiliate is not required to provide an assurance report to establish that it meets the information security criterion once accredited, and this approach is intended to reflect the evidence that is required at the accreditation application stage as well. Instead, an affiliate provides a self-assessment and attestation to the Data Recipient Accreditor (DRA).

The following table sets out key differences between sponsored accreditation and unrestricted accreditation, with more detail provided below.

Issue	Unrestricted	Sponsored
What is the evidence needed to establish information security on an ongoing basis?	Independent third-party assurance report (for further information, including on partial acceptance of industry standards, see the 'Supplementary Accreditation Guidelines' published by the DRA).	Self-assessment and attestation against accredited person's ability to comply with Schedule 2 to the CDR Rules.
When can the accredited person be an active participant in the CDR system?	Upon accreditation and successful completion of any testing or other requirements determined by the Registrar in order to be included in the Register.	Must be accredited and in a sponsorship arrangement with an unrestricted accredited person. May not access CDR data or provide goods or services unless it has an arrangement with a registered sponsor which has been entered on the Register of Accredited Persons.
Who can the accredited person collect CDR data from?	Data holders and other accredited data recipients.	Cannot collect data directly from data holders. May request its sponsor to collect data from a data holder and disclose that data to the affiliate. May also collect data from another accredited person who is not their sponsor, relying on the g disclosure rules (see rule 1.10A).
Can the accredited person use outsourced service providers (OSPs)?	May use OSPs to collect data under a CDR outsourcing arrangement. May disclose data to OSPs under a CDR outsourcing arrangement.	May not enter into a CDR outsourcing arrangement to collect CDR data. May disclose data to OSPs under a CDR outsourcing arrangement.
Can the accredited person have CDR representatives?	Yes.	No.

Becoming accredited at the sponsored level

The Amending Rules introduce a new sponsored level of accreditation, with certain restrictions on participation in the CDR regime applicable for those with sponsored accreditation. ***[Schedule 1, item 8, Subdivision 5.2.1A]***

There are now two levels of accreditation within the CDR regime: unrestricted accreditation, and sponsored accreditation. ***[Schedule 1, items 2 and 8, rule 1.7(1) and rule 5.1A]***

Consequential amendments are made throughout Part 5 of the CDR Rules to reflect that there are now two levels of accreditation within the CDR system. ***[Schedule 1, items 1 and 9 to 16, rules 1.6(11), 5.2, 5.5 and 5.12]***

Applicants for sponsored accreditation must make their application to the DRA in a form approved by the DRA and specify that the person seeks sponsored accreditation. ***[Schedule 1, items 9 and 10, rule 5.2(2)(aa)]***

Applicants for sponsored accreditation must meet the same accreditation criteria as persons with unrestricted accreditation. This includes complying with the obligations of an accredited person specified in rule 5.12 of the CDR Rules. ***[Schedule 1, items 11 to 16, rules 5.5 and 5.12]***

An affiliate's accreditation is taken to have been surrendered if it is not in a sponsorship arrangement for 120 consecutive days. ***[Schedule 1, item 8, rule 5.1B(7)]***

The DRA may suspend or revoke an affiliate's accreditation if a sponsorship arrangement expires or terminates, if the sponsor's accreditation is suspended or revoked, or if the affiliate no longer has a sponsor. Consistent with rules 5.18 and 5.20 of the Rules, the DRA must notify the accredited person of their intention to suspend or revoke their accreditation and give the accredited person a reasonable opportunity to respond. ***[Schedule 1, item 18, item 11 of the table in rule 5.17(1)]***

Before revoking a sponsor's accreditation, the DRA must inform any affiliate and give them a reasonable opportunity to be heard in relation to the proposed revocation, and vice versa before revoking an affiliate's accreditation. If the DRA proceeds to revoke a sponsor's accreditation, it must notify any associate, and vice versa. ***[Schedule 1, items 19 to 22, rule 5.18]***

For a sponsor, the Accreditation Registrar must enter each affiliate of the sponsor on the Register of Accredited Persons, and vice versa for an affiliate. ***[Schedule 1, items 23 and 24, rules 5.24(ba)-(bb)]***

The sponsor and affiliate relationship

A sponsorship arrangement must be a written contract between a person with unrestricted accreditation (defined as the ***sponsor***) and another person (defined as the ***affiliate***). The other person may have sponsored accreditation at the time they enter into a sponsorship arrangement, or may apply for and be granted sponsored accreditation before having a sponsorship arrangement in place. ***[Schedule 1, items 2 and 3, rules 1.7(1) and 1.10D]***

The sponsorship arrangement must provide for the sponsor to disclose CDR data to its affiliate, in response to a consumer data request. ***[Schedule 1, item 3, rule 1.10D(1)(a)]***

The arrangement must also require the affiliate to provide the sponsor with the appropriate information and access to its operations as needed for the sponsor to fulfil its obligations as a sponsor. ***[Schedule 1, item 3, rule 1.10D(1)(b)]***

The parties may agree for the sponsor to make consumer data requests, or to use or disclose CDR data, at the request of the affiliate. In this case, the sponsor would be liable for its conduct when it makes consumer data requests, or uses or discloses the data. This can be compared to outsourcing arrangements, where an accredited data recipient that uses outsourced service providers (OSPs) for collection is ultimately liable for them. ***[Schedule 1, item 3, rule 1.10D(2)]***

Similarly, the affiliate would be liable for its conduct when it uses or discloses CDR data to provide goods and services.

Collecting and using data

Persons with sponsored accreditation are prohibited from making consumer data requests unless they are a party to a sponsorship arrangement. ***[Schedule 1, item 8, rule 5.1B(2)]***

Similarly, an affiliate cannot make a consumer data request otherwise than through its sponsor or to another accredited data recipient under the AP rules. This means an affiliate cannot make a consumer data request directly to a data holder. ***[Schedule 1, item 8, rule 5.1B(3)]***

An affiliate must not have a CDR representative (explained in connection with Schedule 2 to the Amending Rules in this explanatory statement) or engage an outsourced service provider to collect data from a CDR participant on its behalf. ***[Schedule 1, item 8, rules 5.1B(4)-(5)]***

The standard maximum civil penalty for CDR Rule breaches applies for a contravention of these restrictions. A robust penalty setting is important to deter sponsors or affiliates from entering arrangements or engaging in conduct that would jeopardise the security of consumers' data and undermine the integrity of the CDR regime, and is consistent with similar civil penalty obligations applying to accredited persons that already exist in the CDR rules. ***[Schedule 6, item 21, rule 9.8(nn)-(qq)]***

When seeking to access data, an affiliate must comply with the consumer data request requirements in Part 4 of the CDR Rules as amended by Schedule 1 to the Amending Rules.

In particular, when an affiliate seeks a collection consent from a consumer, and the consumer's CDR data will be collected by the sponsor at the affiliate's request, this fact must be disclosed to the CDR consumer. In this case, if the consumer gives the collection consent, they are deemed to have consented to the sponsor collecting the CDR data, even though the consent is given to the affiliate. ***[Schedule 1, item 5, rule 4.3(2B)]***

If the consumer's CDR data will be collected by a sponsor at the affiliate's request, the affiliate must give the sponsor's name, accreditation number, an explanation that the consumer can seek further information about the collection and disclosures of CDR data from the sponsor's CDR policy, and a link to that CDR policy. ***[Schedule 1, item 6, rule 4.11(3)(i)]***

The affiliate must also state in the CDR consumer's dashboard that their data will be collected by a sponsor at the affiliate's request along with the sponsor's name and accreditation number. ***[Schedule 1, item 4, rule 1.14(3)(ha)]***

The sponsor and affiliate may choose which of the two of them will give the notifications required by Subdivision 4.3.5 of the CDR Rules (CDR receipts, etc.) in circumstances where those requirements would otherwise involve both of them giving a notice to a CDR consumer. ***[Schedule 1, item 7, rule 4.20A]***

The AP disclosure consent rule (rule 4.7B) applies to both sponsors and affiliates. Where an affiliate seeks to rely on AP disclosure to access CDR data, it must comply with rule 4.7B in obtaining an AP disclosure consent.

> **Example 1: Customer-facing affiliate accesses CDR data through non-customer-facing sponsor**
>
> iAggregate, a small-to-medium enterprise, wants to provide an account aggregation service to customers using CDR data and applies for accreditation at the sponsored level. Dachshund Data is accredited to the unrestricted level

and enters into a sponsorship arrangement to sponsor iAggregate as its affiliate in the CDR, enabling iAggregate to use CDR data for the service. Consumers give consent to iAggregate for it to use their CDR data to provide the account aggregation service. Dachshund Data collects CDR data from data holders at the request of iAggregate. Although iAggregate's customers do not have a direct relationship with Dachshund Data, they are informed that Dachshund Data collects their data during the consent process. As a sponsor, Dachshund Data has a third-party management framework and takes steps to ensure iAggregate's information security is adequate by assisting iAggregate with tailored technical advice and assistance, both before entering into the sponsorship arrangement and on an ongoing basis.

Example 2: Affiliate relies on AP disclosures of CDR data

Pulpit is a platform service provider that offers SaaS services to SME consumers directly, as well as the ability to download apps from its marketplace and for consumers to share their data with them. Pulpit is a person accredited to the unrestricted level that acts as a sponsor in the CDR, collects CDR data from data holders on behalf of consumers, and retains that data as an accredited data recipient. Pulpit relies on the AP disclosure rules to share data it holds with its affiliates, at a consumer's request, in situations where a consumer downloads an affiliate's app from its marketplace. Before deciding whether to sponsor affiliates, Pulpit undertakes an assessment of whether they are appropriate partners for its platform. Pulpit evaluates their general security posture by reference to Schedule 2 to the CDR Rules.

Responsibility and liability for affiliates' use and disclosure of data

Affiliates are responsible for their use and disclosure of CDR data they receive, and management of CDR data in accordance with the obligations under the Act and rules. Like all accredited data recipients, affiliates must not use or disclose data collected under a consumer data request made under Part 4 of the CDR Rules otherwise than for a permitted use or disclosure (rule 7.6(1)). This applies whether the affiliate accesses CDR data through its sponsor or through AP disclosure rules.

To ensure that affiliates are appropriately liable for their use and disclosure of data, any data collected by a sponsor at the request of an affiliate is deemed to have also been collected by the affiliate. This amendment ensures the limitation to permitted uses and disclosures applies to affiliates when they have used their sponsor to collect data from data holders. ***[Schedule 1, item 28, rule 7.6(3)]***

If an affiliate ceases to have a sponsor registered with the DRA, any collection consents relevant to that sponsor for the affiliate expire, but the corresponding use consents and disclosure consents continue in effect. ***[Schedule 1, item 8, rules 5.1B(6) and (8)]***

The affiliate's obligations

As accredited persons, affiliates must comply with obligations on accredited persons in the CDR Rules. However, Schedule 1 to the Amending Rules adjusts some of these obligations specifically for persons with sponsored accreditation. Relevant instances are set out below.

The ongoing reporting requirements in Schedule 1 to the CDR Rules, which are default conditions on accreditation, are adjusted for persons with sponsored accreditation. A person with sponsored accreditation must provide a self-assessment against the requirements in Schedule 2 to the CDR Rules (with respect to information

security) and an attestation statement every two years. The self-assessment and the attestation statement must be made in the form of any approved requirements by the DRA. ***[Schedule 1, items 33 and 35, definitions of 'assurance report' and 'attestation statement' in clause 2.1(1) of Schedule 1 to the CDR Rules, and clause 1.5(1)(a) of Schedule 2 to the CDR Rules]***

Rules relating to privacy safeguards in Part 7 of the CDR Rules are also amended to reflect specific obligations for affiliates. In particular:

- Rule 7.2 relating to privacy safeguard 1 is amended to require the affiliate's CDR policy to include a list of the persons with whom it has a sponsorship arrangement, and to provide information about the nature of the services one party provides to the other for each such sponsorship arrangement; and
- Rule 7.4 relating to privacy safeguard 5 is amended to require information about whether CDR data was collected by a sponsor at their affiliate's request to be included in the consumer's dashboard when notifying of the collection of CDR data (with the sponsor and affiliate able to choose which of them will be responsible for updating the consumer's dashboard).

[Schedule 1, items 25 and 26, rules 7.2(4)(aa)-(ab) and 7.4]

Schedule 1 to the Amending Rules also inserts new obligations that only apply to affiliates.

Specifically, affiliates are prohibited from accessing data directly from data holders. ***[Schedule 1, item 8, rule 5.1B(3)]***

Affiliates must also provide their sponsor with the information and access to their operations it needs to fulfil its obligations as a sponsor, under the terms of the sponsorship arrangement. ***[Schedule 1, item 3, rule 1.10D(1)(b)]***

The sponsor's obligations

Additional obligations apply to sponsors with respect to their sponsorship arrangements and their affiliates.

Under new default conditions on accreditation in Schedule 1 to the CDR Rules, sponsors and potential sponsors must:

- before entering into a sponsorship arrangement, have in place a third-party management framework that will ensure the person maintains appropriate information security capabilities as an affiliate, including: due diligence requirements for new relationships or contracts, annual review and assurance activities, and reporting requirements;
- before entering into a sponsorship arrangement, provide any appropriate assistance or training to the proposed affiliate on technical and compliance matters relating to Schedule 2 to the CDR Rules;
- once the sponsorship arrangement has commenced, continue to provide any appropriate assistance and training in technical and compliance matters to affiliates, maintain its third-party management framework, and manage its relationship with the affiliate in accordance with it; and
- take reasonable steps to ensure affiliates comply with their obligations under Schedule 2 to the CDR Rules.

[Schedule 1, item 34, clause 2.2 of Schedule 1 to the CDR Rules]

These obligations are intended to be principles-based and scalable, with what constitutes reasonable steps and appropriate due diligence or assistance with respect of information security depending on the nature and context of the services being provided by affiliates using the CDR and under the sponsorship arrangement.

Sponsors must also comply with the rules relating to privacy safeguards in Part 7 as amended. Rules 7.2 and 7.4 as described above apply to sponsors in the same way as they do to affiliates. ***[Schedule 1, items 25 and 26, rules 7.2(4)(aa)-(ab) and 7.4]***

Sponsors must notify the DRA of becoming a sponsor of an affiliate, or the suspension, expiration or termination of a sponsorship agreement. They must do so as soon as practicable, and in any event, within 5 business days ***[Schedule 1, item 17, rule 5.14(2)]***

Record-keeping and reporting

Sponsors and affiliates must keep and maintain records of any sponsorship arrangement to which they are a party, as well as records of the other party's use and management of CDR data collected by it or provided to it under the arrangement. ***[Schedule 1, item 29, rule 9.3(2)(i)]***

Like other accredited data recipients, sponsors and affiliates must prepare a report of certain matters for the Australian Competition and Consumer Commission (ACCC) and the Office of the Australian Information Commissioner (OAIC) each six-month reporting period.

Among other matters, a sponsor's report must set out:

- the number of consumer data requests made during the reporting period, distinguishing between requests made on its own behalf and those made on behalf of affiliates;
- the number of consumer data requests it received from an accredited person on behalf of a CDR consumer, distinguishing between requests from affiliates and other accredited persons; and
- the number of sponsorship arrangements to which it was a party during the period.

[Schedule 1, items 30 to 32, rules 9.4(2)(f)(i)(A), (iii) and (ix)]

Among other matters, an affiliate's report must set out:

- the number of consumer data requests made during the reporting period, distinguishing those made to its sponsors and those made to other accredited persons;
- the number of consumer data requests it received from an accredited person on behalf of a CDR consumer; and
- the number of sponsorship arrangements to which it was a party during the period.

[Schedule 1, items 30 to 32, rules 9.4(2)(f)(i)(B), (iii) and (ix)]

A maximum civil penalty of $50,000 for an individual and $250,000 for a body corporate applies for a contravention of these record-keeping and reporting obligations. This is consistent with the existing penalty provisions that apply to accredited data recipients under the CDR Rules.

Schedule 2 - Amendments relating to CDR representatives

The CDR representative model enables unaccredited persons to provide goods and services to consumers using CDR data in circumstances where they are in a CDR representative arrangement with an unrestricted accredited person who is liable for them.

An unaccredited person who is in a CDR representative arrangement is known as the CDR representative of the principal accredited person.

CDR representative and principal relationship

The Amending Rules introduce the new concepts of a ***CDR representative*** and ***principal.*** The new rule also establishes the minimum required terms in a ***CDR representative arrangement***. ***[Schedule 2, items 1 and 4, rules 1.7(1) and 1.10AA]***

A CDR representative arrangement must be a written contract between the principal (a person with unrestricted accreditation) and a CDR representative (a person without accreditation). The arrangement establishes a mechanism for CDR representatives to access and use CDR data and the obligations of both the principal and the CDR representative in respect of that CDR data.

Where a representative has obtained the consent of a CDR consumer to collect and use CDR data, the principal's obligations under the arrangement are to make a consumer data request and disclose the CDR data (***service data***) it obtains under the request to the representative. ***[Schedule 2, item 4, rule 1.10AA(2)(a)]***

The CDR representative will then be able to use that CDR data to provide goods and services to the consumer. ***[Schedule 2, item 4, rule 1.10AA(2)(a)(ii)]***

The CDR representative will also be able to disclose that CDR data (in accordance with a valid disclosure consent from the consumer). ***[Schedule 2, item 4, rule 1.10AA(2)(a)(iii)]***

The CDR representative's obligations under the arrangement are to:

- not enter into a CDR representative arrangement with another principal;
- not engage an outsourced service provider in its own right;
- comply with privacy safeguard 2 (giving the CDR consumer the option of using a pseudonym, or not identifying themselves), privacy safeguard 4 (destroying unsolicited CDR data), privacy safeguard 8 (overseas disclosure of CDR data), privacy safeguard 9 (adoption or disclosure of government-related identifiers), privacy safeguard 11 (ensuring the quality of CDR data), privacy safeguard 12 (security of CDR data) and privacy safeguard 13 (correction of CDR data), as if it were the principal;
- take the steps in Schedule 2 to the CDR Rules to protect the service data for the purposes of privacy safeguard 12;
- not disclose the service data other than in accordance with the contract with the principal;
- delete service data when directed to by the principal and provide records of the deletion; and
- adopt and comply with the principal's CDR policy in relation to the service data.

[Schedule 2, item 4, rule 1.10AA(2)(a)-(f)]

However, the arrangement cannot allow the CDR representative to access or use CDR data unless the CDR representative's details have been entered on the Register of Accredited Persons. This means that a CDR representative must not make any consumer data requests until it is registered. ***[Schedule 2, item 4, rule 1.10AA(2)(g)]***

The Amending Rules impose several obligations on the CDR principal in relation to its CDR representative arrangements. These obligations are in addition to other deeming rules holding the CDR principal liable for the actions or omissions of its CDR representatives. Those deeming rules are explained under *Collecting, using and disclosing data*.

Firstly, the principal must ensure its CDR representatives comply with their requirements under the arrangement.

There is a new rule to hold a CDR principal accountable if its CDR representative breaches any of the requirements that form part of the definition of CDR representative arrangement. The standard maximum civil penalty for CDR Rule breaches applies for a contravention of this rule. A robust penalty setting is important to deter principals from entering arrangements or facilitating conduct that would jeopardise the security of consumers' data and undermine the integrity of the CDR regime. ***[Schedule 2, item 7, rule 1.16A(2), and Schedule 6, item 21, rule 9.8(h)]***

In particular, and in relation to the collection of CDR data, a CDR principal may be liable for a civil penalty if their CDR representative makes a consumer data request before their details are entered on the Register of Accredited Persons. ***[Schedule 2, items 4 and 7, rules 1.10AA(2)(a) and 1.16A]***

Secondly, the principal must notify the Data Recipient Accreditor as soon as practicable, and within 5 business days, of entering into a new CDR representative arrangement for the purposes of having those details entered onto the Register of Accredited Persons. The 5-day timeframe is the maximum time allowed before the principal must notify the Data Recipient Accreditor of the arrangement – the core obligation is to notify the Data Recipient Accreditor as soon as practicable after the event. This is intended to protect the integrity of the information contained in the Register. This shortened notification window complements other amendments to restrict CDR representatives from accessing CDR data unless they have been entered on the Register (see rule 1.10AA). ***[Schedule 2, item 14, rules 5.14(3) and (4)]***

Likewise, the principal must notify the DRA if their arrangement with a CDR representative terminates or otherwise ends as soon as practicable after that happens, but in any case, within 5 business days. ***[Schedule 2, item 14, rule 5.14(5)].***

Once a CDR representative arrangement has ended or been terminated, the CDR representative is unable to continue collecting data from its principal, using or otherwise managing CDR data.

The Accreditation Registrar is required to enter the name, ABN (if applicable) and business address (whether in Australia or overseas) of any CDR representative of an accredited person. ***[Schedule 2, item 15, rule 5.24(bc)]***

Thirdly, the CDR principal is responsible for dispute resolution in relation to its CDR representatives (consistently with its obligations as an accredited person under rule 5.12). The definition of *CDR consumer complaint* in rule 1.7(1) is amended to allow CDR consumers to complain directly to CDR representatives about the provision of

goods or services by that CDR representative, and therefore trigger the internal dispute resolution obligations of the CDR principal. ***[Schedule 2, item 2, definition of 'CDR consumer complaint' in rule 1.7(1)]***

Fourthly, the CDR principal must keep and maintain records in relation to each of its CDR representatives. Broadly, those records must cover and explain the CDR representative's use and management of CDR data. Among other things, the records must cover and explain:

- the CDR representative arrangement itself;
- the steps the principal has taken to ensure the CDR representative complies with its obligations under the CDR representative arrangement;
- records of all consents given to CDR representatives, amendments to and withdrawals of those consents by CDR consumers, the process by which the CDR representative asks for those consents, and notifications of withdrawals of authorisations by data holders;
- complaint data;
- de-identification of CDR data and deletion of CDR data by the CDR representative and how the CDR representative used de-identified data if applicable; and
- the terms and conditions on which the CDR representative offers goods and services to consumers, including the collection, use and disclosure of CDR data in order to provide those goods or services.

[Schedule 2, item 30, rule 9.3(2A)]

Fifthly, the CDR principal must prepare reports in relation to each of its CDR representatives. Among other things, the report must contain the following information:

- a summary of the CDR complaint data for the reporting period;
- a description of the goods or services provided by the CDR representative (if not provided in the previous reporting period) and the CDR data required to provide those goods and services, and any material changes made to those offerings since the previous reporting period; and
- the total number of consumer data requests made by the CDR principal on behalf of its CDR representative, and the total number of consumer data requests the CDR representative made to the CDR principal.

[Schedule 2, item 31, rule 9.4(2A)]

A maximum civil penalty of $50,000 for an individual and $250,000 for a body corporate applies for a contravention of these record-keeping and reporting obligations. This is consistent with the existing penalty provisions that apply to accredited data recipients under the CDR Rules.

Collection, use and disclosure of data and privacy safeguards

When necessary to provide requested goods or services to a consumer, rule 4.3A provides that a CDR representative may ask the consumer for a collection consent for the principal to collect on the representative's behalf, a use consent for the principal to provide the CDR data to the representative, and a use consent for the representative to

use the CDR data to provide the requested goods and services. If the CDR consumer has given such a collection consent, the CDR representative may also ask the consumer to give a disclosure consent for that CDR data. ***[Schedule 2, items 8 to 13, rules 4.1, 4.3(2), 4.3A, 4.4(1)(a), 4.7A(1)(a) and 4.11]***

New rule 4.3B applies the existing AP disclosure rules (rules 4.7A and 4.7B) to CDR representatives. The effect of this is to allow a CDR representative that receives an AP disclosure request from an accredited person to seek a disclosure consent from the CDR consumer. ***[Schedule 2, item 10, rule 4.3B]***

New rule 4.3C requires the CDR principal to ensure that, when its CDR representative asks for the required consents from a consumer in order to provide goods and services, the CDR representative does so in accordance with Division 4.3. Rule 4.3C also modifies specific provisions of Division 4.3 to ensure it can apply to CDR representatives and operate consistently with the principal-CDR representative relationship and liability framework. ***[Schedule 2, item 10, rule 4.3C]***

The standard maximum civil penalty for CDR Rule breaches applies for a contravention of this rule. A robust penalty setting is important to ensure principals are responsible for preventing conduct that would jeopardise the security of consumers data and undermine the integrity of the CDR regime. ***[Schedule 6, item 21, rule 9.8(n)]***

Where a consumer gives a consent to a CDR representative for their principal to collect CDR data and disclose it to the CDR representative, this is also taken to be a collection consent. ***[Schedule 2, item 5, rules 1.10A(4)-(5)]***

A CDR representative will be able to seek ***TA disclosure consents***, ***AP disclosure consents*** and ***insight disclosure consents*** as well as collection and use consents in order to provide goods and services. In this way, a CDR representative is able to disclose CDR data as if it is an accredited person. The only exception to this is that a CDR representative cannot disclose CDR data to an outsourced service provider. ***[Schedule 2, items 5 and 10, rules 1.10A and 4.3C]***

A CDR principal is permitted to disclose data to a CDR representative in order for the CDR representative to do one or more of the following:

- use the CDR data to provide goods or services;
- in accordance with a valid use consent, de-identify data to use for general research or to disclose (including by sale);
- disclose that de-identified data to any person (including by sale);
- transform, analyse or otherwise derive CDR data to provide goods or services, or to de-identify for general research or on-disclosure;
- disclose to the CDR consumer any of their own CDR data to provide the consumer with goods or services; and
- otherwise disclose the consumer's CDR data in accordance with a current disclosure consent.

[Schedule 2, item 19, rule 7.5(1)(h)]

A CDR principal is also permitted to disclose data to a CDR representative for one of the following direct marketing uses or disclosures:

- sending the CDR consumer information about upgraded or alternative goods or services, offers to renew existing goods or services, information about the benefits of existing goods or services, or information about other goods or services provided by another accredited person; or
- using the CDR data (including by analysing it) in order to send the consumer such information.

[Schedule 2, item 20, rule 7.5(3)(d)]

Importantly, any use or disclosure of service data by a CDR representative is taken to have been by the unrestricted accredited data recipient principal, including any use or disclosure that occurs outside the scope of the CDR representative agreement. This means that if a CDR representative uses or discloses CDR data other than for a permitted purpose, it is the principal that is liable for the contravention of the existing civil penalty provision in rule 7.6(1). ***[Schedule 2, items 21 and 22, note to rule 7.6(2) and rule 7.6(4)]***

The principal must update and maintain the consumer dashboard for requests, although the principal may delegate this responsibility to the representative in the CDR representative arrangement. For the purposes of complying with its obligations under privacy safeguard 10, a disclosure of service data by a CDR representative is taken to have been a disclosure by the CDR principal. Accordingly, the obligation to update the consumer dashboard falls on the CDR principal, although it may delegate the performance of that obligation to the CDR representative. ***[Schedule 2, items 6 and 24, rules 1.14(5) and 7.9(5)]***

For the purposes of complying with its obligations under privacy safeguard 1 (the open and transparent management of CDR data), the CDR principal must include a list of its CDR representatives in its policy about the management of CDR data and a description of the goods and services they provide to consumers. ***[Schedule 2, items 16 and 17, rules 7.2(4)(ac)-(ad) and 7.2(8)]***

Where a CDR representative fails to comply with:

- privacy safeguard 2 (section 56EE of the Act);
- privacy safeguard 4 (section 56EG) of the Act);
- privacy safeguard 8 (section 56EK of the Act);
- privacy safeguard 9 (section 56EL of the Act);
- privacy safeguard 11(section 56EN(2) of the Act);
- privacy safeguard 12 (section 56EO(2) of the Act); or
- privacy safeguard 13 (section 56EP(2) of the Act)

as if it were an accredited person, this is also deemed to be a breach of each relevant rule by the CDR principal. It is irrelevant whether the breach occurred within the scope of the CDR representative arrangement. ***[Schedule 2, items 18, 23, and 25 to 29, rules 7.3, 7.3A, 7.8A, 7.10A, 7.11(2), 7.12(2)(b), 7.12(3) and 7.16]***

If a CDR representative fails to comply with one of the above privacy safeguards, its CDR principal is liable for the maximum civil penalty for CDR Rule breaches. This reflects the critical importance of the privacy safeguards to the CDR regime. These

penalties are intended to put accredited persons who propose to become CDR principals on notice to ensure that their CDR representatives properly protect any CDR data they handle, use or disclose. ***[Schedule 6, item 21, rules 9.8(fff)-(ggg), (iii)-(kkk) and (nnn)]***

Example 3: White-labelled banking services with CDR functionality

Bank A is an unrestricted accredited person. It provides goods and services directly to consumers under its Bank A brand. However, to grow its deposit base, Bank A is willing to take on liability for third parties that use its underlying banking infrastructure to provide consumers with banking products that also have added features that use CDR data.

Bank A partners with Fintech B. Fintech B markets a service to consumers where they can open a Fintech B branded bank account which is white-labelled by Bank A, and see all their existing bank account balances in their Fintech B app (including from other banks). Bank A collects CDR data in order for Fintech B to display the aggregated accounts and balances.

Sponsorship does not suit Bank A and Fintech B because Fintech B does not seek to become accredited. However, Bank A is prepared to assume full liability for Fintech B's use of CDR data as part of its commercial arrangement with Fintech B and therefore agrees to register Fintech B as its CDR representative.

Example 4: 'CDR as a service'

Fastroad is a fintech with unrestricted accreditation that provides a packaged suite of CDR services to which its customers may add branding . In this instance, that includes providing the infrastructure for collection, consent screens, CDR data storage, and dashboards. Jamborine is an unaccredited business that offers a budgeting service. Jamborine enters a representative arrangement with Fastroad, who agrees to provide the necessary CDR infrastructure and management services to Jamborine so it can use CDR data to provide its service. To manage the risks with being responsible for Jamborine as its representative, Fastroad and Jamborine agree that Jamborine will not make disclosures to other accredited data recipients, and Jamborine will use CDR data within Fastroad's secure CDR data environment.

Example 5: Subsidiary acting as a representative

Bank X is an Authorised Deposit-taking Institution (ADI) with unrestricted accreditation. Y Financial is a subsidiary of Bank X that provides retail financial advice services. Y Financial wants to streamline its processes for reporting financial information to its customers' accountants. It believes using the CDR to provide this service as an add-on to its retail offering would be the simplest approach and wants to use its parent company's accreditation to participate in the CDR. As a subsidiary, Bank X is comfortable with taking on liability for Y Financial. Bank X and Y Financial enter a CDR representative arrangement and notify the Data Recipient Accreditor of their arrangement. This allows Y Financial to collect its customers' CDR data through Bank X and disclose the information to the customers' nominated trusted advisers.

Schedule 3: Amendments relating to trusted advisers and insights

The Amending Rules establish two new data sharing models which are intended to provide consumers with greater choice in who they can direct that their data be shared with, while maintaining adequate protections:

- The trusted adviser model allows consumers to consent to an accredited data recipient disclosing their CDR data outside the CDR system with certain professionals. These are professions that are considered to be appropriately regulated to receive CDR data, particularly due to consumer protection mechanisms that form part of their regulatory framework. This model facilitates access to relevant data for those working within these professions, while ensuring that disclosure of data can only occur with a consumer's consent.
- The CDR insights model allows consumers to consent to insights informed by CDR data being shared outside the system for a range of prescribed purposes that are considered low risk. This increases consumers' ability to engage with unaccredited parties in a way that limits the data they share to only what is necessary for the prescribed purpose.

Trusted advisers

Background

Schedule 3 to the Amending Rules amends the CDR Rules to allow a consumer to consent to an accredited person disclosing their CDR data to a person within a specified class (referred to as ***trusted advisers***). The intention is to:

- facilitate current consumer practices of sharing their data with certain classes of trusted third parties in order to receive advice or a service; and
- increase convenience and control for consumers by enabling them to use the CDR to share their data with their chosen trusted advisers.

In turn, this is designed to encourage greater participation in the CDR by accommodating existing and new use cases which rely on the ability to disclose data to third parties.

Trusted adviser disclosure consent

A new ***TA disclosure consent*** enables a consumer to consent to an accredited data recipient disclosing their CDR data to a nominated trusted adviser. ***[Schedule 3, items 1 to 3, rules 1.7(1), 1.10A(1)(c)(iii) and 1.10A(2)(f)]***

As with other CDR consumer consents, the accredited person's processes for asking a consumer to give a TA disclosure consent must accord with any consumer experience data standards, and, consistent with the object set out in rule 4.9, the consent given must be voluntary, express, informed, specific as to purpose, time limited and easily withdrawn.

An accredited person can invite a CDR consumer to nominate one or more trusted advisers. The trusted adviser must be a member of one of the following classes:

- qualified accountants within the meaning of the *Corporations Act 2001*;

- persons who are admitted to the legal profession (however described) and hold a current practising certificate under a law of a State or Territory that regulates the legal profession;
- registered tax agents, Business Activity Statement agents and tax (financial) advisers within the meaning of the *Tax Agent Services Act 2009*;
- financial counselling agencies;
- financial advisers;
- mortgage brokers within the meaning of the *National Consumer Credit Protection Act 2009*.

[Schedule 3, item 5, rules 1.10C(1)-(2)]

For defining the scope of financial counselling agencies, the *ASIC Corporations (Financial Counselling Agencies) Instrument 2017/792* is incorporated by reference. Section 56BG of the Act provides that the rules may make provision by applying, adopting, or incorporating any matter contained in any other instrument or writing as in force or existing at a particular time or as in force or existing from time to time. *ASIC Corporations (Financial Counselling Agencies) Instrument 2017/792* is incorporated as existing from time to time. The instrument can be found on the Australian Securities and Investments Commission (ASIC) website.

The scope of the 'financial advisers' class of trusted advisers relies on the broad definition of 'relevant provider' in the *Corporations Act 2001*. While they are 'relevant providers', limited-service time-sharing advisers and provisional relevant providers have been excluded on the basis that the *Corporations Act 2001* does not allow them to refer to themselves as 'financial advisers'. Additionally, limited-service time-sharing advisers have lower education and training standards and are exempt from the ban on conflicted remuneration, and provisional relevant providers are required to be supervised.

Where an accredited data recipient discloses to someone who is not a member of a trusted adviser class, this would not be a permitted use or disclosure and a contravention of the civil penalty obligation in existing rule 7.6. However, where an accredited person takes reasonable steps to confirm that a nominated trusted adviser was, and remains a member of a trusted adviser class, the person is taken to be a member of that class. ***[Schedule 3, item 5, rule 1.10C(3)]***

The reasonable steps that an accredited data recipient may take to confirm that a nominated trusted adviser is a member of a trusted adviser class is a scalable standard that will depend on the circumstances. For example, the intention is that seeking confirmation from the trusted adviser that they are a member of a class of trusted advisers (which may take the form of a contractual warranty, or an attestation or representation by the adviser), or searching publicly available information, would generally satisfy this test. Circumstances that may be relevant to whether steps taken are 'reasonable' include whether it is the consumer, or accredited data recipient, that has a closer relationship with the proposed trusted adviser when they are nominated by the consumer, or whether the accredited data recipient knew, or ought to have known, that the relevant person was not a trusted adviser. Where the consumer has an existing relationship with the trusted adviser, the intention is that what is required to meet the reasonable steps test will be less onerous than where is the accredited

data recipient that has an existing relationship. Further, where the accredited data recipient knew, or ought to have known that a person is not a trusted adviser, the intention is that they would not be able to satisfy the reasonable steps test.

An accredited person cannot make the nomination of a trusted adviser or the giving of a TA disclosure consent a condition for the supply of goods and services requested by the CDR consumer. ***[Schedule 3, item 5, rule 1.10C(4)]***

Consumer protections

Trusted advisers, being unaccredited, do not attract the regulatory obligations that apply to accredited data recipients under the CDR regime. However, the Amending Rules recognise that as members of a professional class, they are subject to existing professional or regulatory oversight, including obligations to act in accordance with the consumer's interests (e.g. fiduciary or other duties to act in the best interests of their clients).

The following requirements strengthen the protections for CDR consumers who wish to disclose their CDR data to their nominated trusted advisers:

- The disclosure of the CDR data from an accredited data recipient to a trusted adviser is covered by the information security controls in Schedule 2 to the CDR Rules. Therefore, the minimum information security control of encrypting data in transit applies to the disclosure.
- TA disclosures are subject to consumer experience data standards made by the Data Standards Chair. A disclosure to a trusted adviser is not a permitted use or disclosure until 1 February 2022 or the day the Data Standards Chair makes the relevant data standards ***[Schedule 3, item 10, rule 7.5A(2)]***. This ensures the CDR consumer is provided with adequate information to give informed consent – for example, this may include information that the use of the data by the recipient will not be covered by the CDR regime and the recipient may not have obligations under the *Privacy Act 1988.*
- When the accredited data recipient discloses the CDR data to a trusted adviser, the accredited data recipient must update each consumer dashboard that relates to the request to indicate what CDR data was disclosed, when it was disclosed and the name of the trusted adviser it was disclosed to. This enables the CDR consumer to monitor who has received their data, and if they decide to, withdraw any active consents to disclose further CDR data. ***[Schedule 3, item 11, rule 7.9(3)]***

Record keeping and reporting

Accredited data recipients are subject to record keeping requirements for TA disclosures. They must maintain records of what CDR data was disclosed to trusted advisers, the trusted advisers to whom it was disclosed, and any steps taken to confirm that the trusted adviser was a member of a class of trusted advisers. ***[Schedule 3, item 14, rules 9.3(2)(eb)-(ec)]***.

Accredited data recipients must include, in their regular reports to the Australian Competition and Consumer Commission, the number of consents they receive from CDR consumers and, for each class of trusted adviser, the number of trusted advisers to whom the CDR data was disclosed. ***[Schedule 3, item 15, rules 9.4(2)(f)(vi)-(vii)]***

CDR insights

Background

Schedule 3 to the Amending Rules amends the CDR Rules to allow a consumer to consent to an accredited data recipient sharing CDR insights containing the consumer's CDR data with any person, provided the disclosure is for one of the purposes specified in the CDR Rules.

Allowing the disclosure of CDR insights is intended to provide a safer and more efficient way for consumers to share certain insights obtained from their CDR data to receive goods and services, reducing the need to share detailed records or passwords to facilitate access to their information.

The Amending rules allow consumers to request that CDR insights be shared outside the CDR system, meaning this data would no longer be subject to the protections of the CDR privacy safeguards. However, the CDR Rules limit the data that can be disclosed in a CDR insight by reference to specified purposes, and specifically disallow the sharing of the amounts and dates of multiple transactions. Certain protections are also provided to ensure consumers properly understand the nature of the information they are agreeing to disclose.

Insight disclosure consents

A new ***insight disclosure consent*** enables a consumer to consent to an accredited data recipient disclosing particular CDR data to a specified person for a specified purpose. ***[Schedule 3, items 1 to 3, rules 1.7(1), 1.10A(1)(c)(iv) and 1.10A(2)(g)]***

As with other CDR consumer consents, the accredited person's processes for asking a consumer to give an insight disclosure consent must accord with consumer experience data standards, and, in accordance with rule 4.9, the consent given must be voluntary, express, informed, specific as to purpose, time limited and easily withdrawn.

The CDR data that is disclosed under an insight disclosure consent is a ***CDR insight***. ***[Schedule 3, item 1, rule 1.7(1)]***

The specified purposes for which an insight disclosure consent could be given are:

- to verify the consumer's identity (CDR insights could be used as supporting information about a consumer's identity, but they would not necessarily substitute for formal proof of identity requirements such as proving someone is of age to buy alcohol, identification elements needed to set up a bank account, or instances where a particular identity proofing standard is required);
- to verify the consumer's account balance; or
- to verify the details of credits to or debits from the consumer's accounts.

[Schedule 3, item 4, rule 1.10A(3)(a)]

For these purposes, 'verify' refers to confirming, denying or providing some simple information about the consumer's identity, account balance, credits or debits based on their CDR data.

CDR insights allow consumers to securely provide and confirm relevant factual information about themselves, while giving the recipient comfort in its authenticity

and accuracy. These purposes are intended to support the sharing of information that the consumer could themselves confirm and understand.

For example, CDR insights could be used to:

- confirm whether a consumer's account balance is over a certain amount;
- disclose a consumer's account balance at a specific point in time;
- disclose the amount, date, counterparty and a description of a single transaction;
- disclose the consumer's average income over a specific period of time;
- provide a summary of the total amount a consumer spent at a store over a month;
- provide a summary of the total amount a consumer spent on different categories of goods over a month;
- confirm whether a consumer has received a transfer of funds from a specific counterparty;
- notify a merchant whether a direct debit payment will fail;
- notify when transactions with a particular store exceed a specific amount;
- confirm whether a consumer made a transaction at a specific store on a specific day;
- disclose a profit and loss statement (that does not include itemised transactions); or
- confirm the number of times over the last 6 months that a consumer paid their rent after the due date.

Example 6: CDR insights to verify a consumer's identity

A consumer is signing up to a new service provider and manually gives the provider their name and address. Though the service provider does not have a legal obligation to identify their customer, they want to know that the person they are dealing with is who they claim to be. Instead of asking for copies of identity documents to confirm the consumer's identity, the service provider asks the consumer to verify their identity using an accredited data recipient.

Through this service, the consumer agrees to the new service provider sharing the details they provided with the accredited data recipient. The consumer then also consents to the accredited data recipient securely collecting relevant details from their data holder through the CDR, and to the accredited data recipient passing a 'yes' or 'no' CDR insight to their new service provider to confirm that the details they received through the CDR match those provided manually. This gives the provider greater confidence regarding the consumer's identity and allows the consumer to easily set up a new service.

Example 7: CDR insights to verify a consumer's account balance

An accredited data recipient partners with a gym to allow a consumer to consent to disclosing CDR insights that inform the gym if a consumer has insufficient funds in their account to meet their subscription payment obligations. Where the insight reveals the consumer has insufficient funds, the gym can send the consumer a prompt to transfer money into their account in time for their next payment and avoid a late payment fee.

The following would not be permitted to be disclosed as a CDR insight because they are not consistent with the listed verification purposes:

- disclose a recommendation to a provider about whether the consumer should be eligible for a product or service;
- disclose a recommendation to a provider about the price a consumer should pay for a product or service; or
- disclose a consumer 'score' or 'ranking'.

Accredited data recipients are responsible for ensuring that any CDR insights they disclose are within the purposes consented to by the consumer and that these purposes align with the list of permitted purposes and any other obligations that they have under the CDR Rules. Disclosure of CDR insights is subject to the existing civil penalty provision under rule 7.6 requiring that accredited data recipients' use or disclosure of CDR data be a permitted use or disclosure.

Once disclosed by the accredited data recipient, the recipient of a CDR insight is responsible for ensuring that their use of this data is in line with any obligations they may have that arise outside the CDR regime. For example, CDR insight recipients may be subject to obligations under the *Privacy Act 1988*, including complying with the Australian Privacy Principles.

Consumer protections

An accredited person must give an explanation of the CDR insight to the CDR consumer when seeking the insight disclosure consent that makes it clear what the CDR insight would reveal or describe. A CDR insight is not required to be shown to a consumer prior to it being disclosed. However, where practical, this could be done in order to assist the consumer's understanding of what the CDR insight would reveal or describe and help meet the accredited person's obligation under rule 4.11. ***[Schedule 3, item 9, rule 4.11(3)(ca)]***

Data standards are required to be made about the processes by which insight disclosure consents are obtained, including ensuring the consumer understands their data will leave the CDR system and explaining the CDR insight in accordance with rule 4.11. ***[Schedule 3, items 12 and 13, rules 8.11(1)(c)(v) and 8.11(1A)]***

The Data Minimisation Principle set out in rule 1.8 prohibits an accredited person from collecting or using a CDR consumer's data beyond what is reasonably needed to provide the goods and services the consumer requested. This requirement applies when an insight disclosure consent is sought and when the CDR insight is disclosed. As a result, accredited data recipients are required to limit CDR insights to the minimum information necessary to meet the consumer's request.

In addition, disclosure of CDR data in a CDR insight is covered by the existing information security controls in Schedule 2 to the CDR Rules, which means that the minimum information security control of encrypting data in transit applies to the disclosure of the CDR insight.

An accredited data recipient is not permitted to disclose the CDR insight if it includes or reveals sensitive information within the meaning of the *Privacy Act 1988*. ***[Schedule 3, item 10, rule 7.5A(4)]***

An insight disclosure consent that relates to more than one transaction cannot authorise the accredited data recipient to disclose the date or amount of any individual

transaction. This is in order that large amounts of detailed transaction data, such as a full transaction list or detailed business ledger will not be able to be disclosed using a CDR insight. However, a summary of transactions disclosed as a verification of credits or debits could be consented to as a CDR insight provided it does not attribute a date or amount to any specific transaction. The amount and date of a single credit or debit could be provided where the CDR insight disclosure consent relates only to that transaction. ***[Schedule 3, item 4, rule 1.10A(3)(b)]***

> **Example 8: CDR insights to verify a consumer's income and rental payments**
>
> An accredited data recipient offers a service to help real estate agents verify a consumer's income and rental payment history using CDR insights. With the consumer's consent, the accredited data recipient discloses the consumer's average monthly income based on all of the consumer's income sources over the past 6 months. The CDR insight does not contain the specific dates or amounts of any of the incoming payments. With the consumer's consent, the accredited data recipient also discloses the number of times over the last 6 months that a rental payment was made from the consumer's account after the rental due date. The CDR insight does not contain the specific dates or amounts of any of the outgoing transactions.

Accredited data recipients must include on consumers' dashboards for each insight disclosure consent, a description of the CDR insight and to whom it was disclosed. ***[Schedule 3, items 6 and 7, rules 1.14(1)(b) and (3)(ea)]***

As soon as practicable after disclosing a CDR insight in response to a consumer data request, accredited data recipients must update each consumer dashboard that relates to the request to indicate what CDR data was disclosed and when and to whom it was disclosed. ***[Schedule 3, item 11, rule 7.9(4)]***

A disclosure of CDR data under an insight disclosure consent is not a permitted use or disclosure until the earlier of 1 February 2022 or when the Data Standards Chair makes consumer experience data standards for disclosure of CDR insights. ***[Schedule 3, item 10, rule 7.5A(3)]***

Record-keeping and reporting

Accredited data recipients must keep records of CDR insights, including a copy of each insight disclosed and when and to whom it was disclosed. ***[Schedule 3, item 14, rule 9.3(2)(ed)]***

Accredited data recipients must include on consumers' dashboards a statement that the consumer is entitled to request copies of these records and how they may make such requests. ***[Schedule 3, item 8, rule 1.14(3A)]***

Accredited data recipients must also report to the Australian Competition and Consumer Commission and the Office of the Australian Information Commissioner on the number of insight disclosure consents they received during a reporting period. ***[Schedule 3, item 15, rule 9.4(2)(f)(viii)]***

Schedule 4 – Amendments relating to joint accounts

Background

Schedule 4 to the Amending Rules establishes new economy-wide rules that set out the approach for sharing CDR data held in joint accounts. Where the concept of a

joint account is not relevant to a sector, the joint account rules would accordingly not be relevant. For example, in a sector where accounts are set up with a primary account holder, the existing secondary user rules could be used to enable an account holder to provide data sharing access to additional persons.

The new rules apply to consumer data requests under Part 4 that involve a request for disclosure of CDR data that relates to one or more joint accounts. CDR data that relates to a joint account must be disclosed in accordance with the disclosure option that applies to the account, and the process for dealing with such requests and disclosures is set out in the new Part 4A of the CDR Rules. ***[Schedule 4, item 14, Part 4A]***

The new rules aim to provide simple, intuitive data sharing on joint accounts, while providing joint account holders with increased oversight and control of data sharing, compared to current data sharing practices outside the CDR.

Disclosure options

One of three disclosure options - pre-approval, co-approval, or non-disclosure – will apply to a joint account. These disclosure options are relevant when an accredited person makes a consumer data request under Part 4 that relates to one or more joint accounts on behalf of a joint account holder or a secondary user on the account. ***[Schedule 4, item 14, rule 4A.5]***

Unless otherwise provided in a sector Schedule, the pre-approval option applies by default. This automatically allows an individual joint account holder to independently share data on the joint account by consenting to an accredited person collecting and using the data from the joint account, and authorising the data holder to disclose that data. If the pre-approval option applies to a joint account, when a data holder receives a consumer data request from a joint account holder or a secondary user (the ***requester***) that includes CDR data relating to the joint account, the data holder must process the request (under existing rules 4.5 to 4.7) as it would any other request on a non-joint account unless an account holder other than the requester (a ***relevant account holder***) has withdrawn their approval to disclosure, in which case, the data holder cannot disclose the requested joint account data. ***[Schedule 4, item 14, rules 4A.3, 4A.5(1)(a) and (5), and 4A.10(2) and (3)]***

Under the co-approval option, joint account data may be disclosed in response to a valid consumer data request that relates to a joint account with the agreement of all account holders. If co-approval applies, and the requester has authorised disclosure, the data holder must seek the relevant account holders' approval to disclose. If such approval is given, the data holder must disclose the requested data (under rules 4.6 to 4.7), as it would any other request on a non-joint account, unless a relevant account holder has withdrawn their approval, in which case the requested joint account data cannot be disclosed. ***[Schedule 4, item 14, rules 4A.5(1)(b) and 4A.10(4) and (5)]***

Under the non-disclosure option, a data holder must refuse a consumer data request to disclose CDR data relating to the joint account. ***[Schedule 4, item 14, rules 4A.5(1)(c) and 4A.10(6)]***

Data holders must offer the pre-approval option and non-disclosure option on joint accounts, and may choose to also offer the co-approval option. ***[Schedule 4, item 14, rules 4A.5(2) and (3)]***

Where the joint account rules apply, the data holder must provide the requester with an online consumer dashboard under existing rule 1.15. The requester can use the dashboard to manage authorisations to disclose CDR data.

The data holder must also provide an online consumer dashboard for each of the other relevant account holders that will enable them to see and manage their approvals related to requests to disclose CDR data that relates to a joint account. The rules require a level of dashboard functionality that allows an account holder to at any time, withdraw an approval for CDR data that relates to the joint account to be disclosed. The dashboard must be prominently displayed and simple and straightforward for the joint account holder to use. The standard maximum civil penalty for CDR Rule breaches applies for a contravention of new rule 4A.13. A robust penalty setting is important to ensure consumers are aware of, and have control over access to, their joint account data. However, a data holder will not contravene the rule provided it takes reasonable steps to ensure the consumer dashboard has the required functionality. ***[Schedule 4, item 14, rules 4A.11, 4A.12 and 4A.13(1) and (4), and Schedule 6, item 21, rule 9.8(kk)]***

Where the data holder already provides the relevant account holder with a consumer dashboard under existing rule 1.15, the ability to see and manage their approvals must be included in that dashboard. ***[Schedule 4, item 14, rule 4A.13(2)]***

To ensure that relevant information is shared across the dashboards of all joint account holders, if a relevant account holder's dashboard contains details of approvals related to the joint account then the dashboards of all the other joint account holders must contain those details. ***[Schedule 4, item 14, rule 4A.13(5)]***

Notification requirements

When a requesting account holder has given, amended or withdrawn an authorisation to disclose requested joint account data, the data holder must notify the other account holders of this. Data holders must also notify the requester when another account holder has not approved, or has withdrawn their approval for, disclosure of the requested data. Data holders must provide for joint account holders to select alternative frequencies of receiving communications from the data holder, including notifications about authorisations and approvals. This may include not receiving any notifications. The standard maximum civil penalty for CDR Rule breaches applies for a contravention. A robust penalty setting is important to ensure consumers are aware of, and have control over access to, their joint account data. ***[Schedule 4, item 14, rule 4A.14, and Schedule 6, item 21, rule 9.8(ll)-(mm)]***

Example 9: Joint account holder initiates data sharing on a joint account under the single consent model for data sharing

Bob and Erin have a joint account with Peanuts Bank. The default pre-approval disclosure option applies to the joint account which means that the joint account is available for sharing.

Erin wishes to share data from the joint account with Green Savers, an accredited person. She gives her consent to Green Savers to collect data on the joint account and provides her authorisation to Peanuts Bank to disclose the data. Peanuts Bank discloses the data to Green Savers. Peanuts Bank sends a notification to Bob that Erin has authorised the disclosure of data on the joint account to Green Savers. Peanuts Bank also updates Bob and Erin's consumer dashboard to reflect details of the sharing arrangement.

Changing disclosure options

Data holders must provide joint account holders with an online service called the disclosure option management service that joint account holders can use to change, propose a change to and respond to a proposal to change the disclosure option that applies to the account. If the data holder already provides a consumer dashboard to an account holder, that account holder's disclosure option management service may be included in their dashboard. The requirement for data holders to ensure joint account holders have this service is a civil penalty provision, reflecting the critical importance such a service has to a consumer's ability to be aware of, and control access to, their joint account data. ***[Schedule 4, item 14, rule 4A.6]***

Any joint account holder may at any time, using the disclosure option management service, set the non-disclosure option as applying to the account. If pre-approval applies to a joint account, any account holder may at any time, change the disclosure option on the account to have the co-approval option apply (if this option is offered by the data holder). Data holders must notify the other joint account holders if the disclosure option has been changed to non-disclosure or co-approval under this rule. ***[Schedule 4, item 14, rule 4A.7]***

A joint account holder may propose to change the disclosure option from the non-disclosure option to the co-approval or pre-approval option, or from the co-approval option to the pre-approval option, using the disclosure option management service. If such a change is proposed, the data holder must contact the other account holders to explain the proposal and invite them to agree or not agree to the change within a specified period. The specified period is not defined in the rules but should be consistent with a data holder's non-CDR services and requests. ***[Schedule 4, item 14, rule 4A.8]***

The standard maximum civil penalty for CDR Rule breaches applies for a contravention of new rules 4A.6, 4A.7 and 4A.8. A robust penalty setting is important to ensure consumers are aware of, and have control over access to, their joint account data. ***[Schedule 6, item 21, rule 9.8(gg)-(jj)]***

> **Example 10: Joint account holder turns sharing setting 'off' on a joint account**
>
> Bob decides to set his data sharing preference to 'off' to stop data sharing on the joint account and uses the disclosure option management service to have the non-disclosure option apply to the account.
>
> Peanuts Bank stops sharing data from the joint account with Green Savers. Peanuts Bank contacts Erin using its ordinary means for contacting her to notify her that Bob selected the non-disclosure option, and consequently that disclosure option now applies to their joint account. Peanuts Bank also updates both Bob and Erin's consumer dashboard and disclosure option management service to show that the non-disclosure option applies to their joint account.

Secondary users of joint accounts

The CDR Rules include principles-based provisions relating to 'secondary users' of joint accounts. The Amending Rules maintain these settings. That is, in order for a secondary user to be able to share data on a joint account, a secondary user instruction must be provided by an account holder.

The secondary user rules generally operate such that:

- if a pre-approval disclosure option applies to the joint account, secondary users can independently authorise data sharing on the account (if there is a secondary user instruction in place on the account);
- if a co-approval option applies to the joint account, secondary users can authorise data sharing on the joint account, but the data holder must obtain the approval of all joint account holders before data on the joint account can be shared; and
- if a non-disclosure option applies to the joint account, secondary users cannot authorise data sharing on the joint account.

Vulnerable consumers

A broad exemption is provided for data holders to not comply with the requirements under Part 4A where the data holder considers this necessary to prevent physical, psychological or financial harm or abuse to any person. For example, a data holder may - where the data holder considers this necessary to prevent physical, psychological or financial harm or abuse to any person - decide to:

- if the non-disclosure option is in place, to not invite the relevant account holder(s) to agree to a disclosure option applying before disclosing data relating to the joint account,
- if the co-approval disclosure option is in place, to not seek the approval of the relevant account holder(s) before disclosing data on the joint account,
- to not provide relevant account holder(s) with a consumer dashboard or to update an existing dashboard with details regarding a joint account.

[Schedule 4, item 14, rule 4A.15]

Implementation and transitional rules

On 30 April 2021, Treasury announced that requirements for banks to implement the joint account requirements that would have applied from November 2021 would be deferred, with new compliance dates to be set following consultation.

The Amending Rules set 1 July 2022 as the compliance date for new joint account data sharing provisions in the banking sector. This date seeks to balance the benefits of having joint accounts data sharing in the CDR and the need for sufficient time for data holders to meet technical requirements. ***[Schedule 5, items 1 and 2, clauses 6.4(3) and 6.6 of Schedule 3 to the CDR Rules]***

Transitional provisions allow major banks (as 'initial data holders') to elect to continue complying with the joint account provisions established when the CDR Rules were first made, until 1 July 2022 or the data holder revokes its election. ***[Schedule 7, items 1 and 2]***

This means major banks continue to share joint account data under the previous rules or under the new joint account data sharing provisions.

Other relevant Authorised Deposit-taking Institutions (ADIs) and initial data holders for non-primary brands, or accredited ADI and accredited non-ADIs (reciprocal data holders) for Schedule 3 (collectively, 'non-major banks') are subject to the new joint account requirements in Part 4A of the CDR Rules from 1 July 2022, but have the

option of voluntarily adhering to the new rules prior to 1 July 2022.
[Schedule 7, items 1 and 3]

Transitional provisions – treatment of disclosure options for existing joint accounts

If a major bank elects to continue complying with the original joint account provisions, the following settings apply to joint accounts with that data holder in existence immediately before 1 July 2022 (or, if the data holder revokes its election, in existence immediately before that revocation):

- for a joint account where a disclosure option has never previously applied, the pre-approval disclosure option applies from 1 July 2022 (or, if the data holder revokes its election, from the day of the revocation); ***[Schedule 7, items 4(1), (2)(c) and (3)(a)]***
- for a joint account that already has a set disclosure option applying to it immediately before 1 July 2022 (or, if the data holder revokes its election, immediately before the revocation date), the equivalent disclosure option under the new joint account requirements applies after that time; ***[Schedule 7, items 4(1), (2)(a) and (3)(a)]***
- for a joint account that, immediately before 1 July 2022 (or the revocation date), had no disclosure option applying to the account, the non-disclosure option applies after that time, rather than switching to the default pre-approval option. ***[Schedule 7, items 4(1), (2)(b) and (3)(a)]***

For the non-major banks, the pre-approval option applies to joint accounts already in existence. In detail:

- if not electing to adhere to the new provisions early, the pre-approval option applies from 1 July 2022 to any joint accounts in existence immediately before 1 July 2022; ***[Schedule 7, items 5(1), (2) and (3)(b)]***
- if electing to adhere to the new provisions early, the pre-approval option applies from the day of that election to any joint accounts in existence immediately before the day of that election. ***[Schedule 7, items 5(1), (2) and (3)(a)]***

Any joint account that comes into existence after the defined 'Part 4A day' will have the pre-approval option provided by default.
[Schedule 4, item 14, rule 4A.5(5), and Schedule 7, the definition of 'Part 4A day' in items 4(3) and 5(3)]

Schedule 5 – Amendments relating to staged implementation

Direct to consumer request service

Part 3 of the CDR Rules sets out future requirements for data holders to implement an online service that allows consumers to directly request their CDR data in a human-readable form and in accordance with the data standards. The deadline for data holders in the banking sector to comply with these requirements had previously been set at 1 November 2021.

The Amending Rules remove the compliance date for the Part 3 obligations in the banking sector. ***[Schedule 5, items 1 and 2, clauses 6.4(3) and 6.6 of Schedule 3 to the CDR Rules]***

This deferral was announced by Treasury on 30 April 2021 and will allow a future consultation process to be undertaken about the way in which direct to consumer

obligations should be specified, including how the data standards should provide for data in machine-readable form via application programming interfaces.

Schedule 6 - Unaccredited collecting outsourced service providers

The definition of *CDR outsourcing arrangement* in rule 1.10 of the CDR Rules is amended to allow any OSP, whether accredited or not, to collect CDR data on behalf of an accredited data recipient and to use that data, or data the accredited data recipient has disclosed to the OSP, to provide goods and services to the accredited data recipient. This allows accredited data recipients to use the services of an unaccredited OSP to collect data directly from a data holder on their behalf. ***[Schedule 6, item 1, rule 1.10(2)(a)]***

Outsourced service providers may now subcontract collecting activities. This prohibition was originally required to ensure only accredited OSPs could collect CDR data on behalf of the principal under the existing rules, and is no longer necessary given the expansion to unaccredited OSPs. ***[Schedule 6, items 2 and 3, rule 1.10(2)]***

The Amending Rules make two consequential amendments in the privacy safeguard provisions to reflect that unaccredited outsourced service providers can collect CDR data on behalf of their principal.

An accredited person's CDR policy must contain details of each outsourced service provider, and include a description of the classes of CDR data collected by it. ***[Schedule 6, item 15, rule 7.2(4)(c)(ii)]***

For the purposes of rule 7.6, any collection of service data by the provider in a CDR outsourcing arrangement is taken to have been by the principal under the arrangement. It is irrelevant whether the collection was in accordance with the CDR outsourcing arrangement. This rule makes the principal liable for the existing civil penalty obligation in rule 7.6, which has the default maximum available under section 76 of the Act. The size of the maximum penalty reflects the critical importance of the privacy safeguards to the CDR regime, in particular, the fundamental need to ensure CDR data is only used or disclosed for a permitted purpose. ***[Schedule 6, item 19, rule 7.6(5)]***

Schedule 6 – Consequential and minor amendments

On consumer dashboards, minor amendments are made to:

- clarify aspects of the consumer dashboard requirements; and ***[Schedule 6, items 4, 5 and 8, rules 1.15(1) and (3)]***
- reflect that dashboard requirements relating to joint accounts have been relocated from the (banking-specific) Schedule 3 to the CDR Rules to the new (sector-neutral) Part 4A. ***[Schedule 6, items 6 and 7, rule 1.15(1)]***

Typographical corrections are made to a note about a civil penalty provision and a reference to the Office of the Australian Information Commissioner. ***[Schedule 6, items 9 and 10, rules 1.16(1) and 1.17(5)]***

Certain elements of rule 4.10, concerning requirements relating to an accredited person's processes for seeking consent, are repealed. These elements are redundant as they have been replaced with new rules that deal with the application of data in transit standards. ***[Schedule 6, items 11 and 12, rules 4.10(1)(a)(ia) and (2)]***

A consequential amendment ensures the Data Recipient Accreditor is required to notify the Accreditation Registrar of certain notifications made by sponsors of affiliates or principals in a CDR representative arrangement. ***[Schedule 6, item 14, item 5.15(a)(vi)]***

Minor amendments are made to clarify:

- the exception to rule 4.16 about electing to delete redundant data; ***[Schedule 6, item 13, rule 4.16(3)]***
- what must be included in an accredited data recipient's CDR policy; and ***[Schedule 6, item 15, rule 7.2(4)(c)(ii)]***
- that a disclosure is not a permitted use or disclosure unless it is done in accordance with the data standards; ***[Schedule 6, item 16, rule 7.5(2)]***
- that rule 7.5(3) about direct marketing uses and disclosures applies in relation to a use or disclosure by an accredited data recipient; and ***[Schedule 6, item 17, rule 7.5(3)]***
- how rule 7.6 describes the provider in a CDR outsourcing arrangement. ***[Schedule 6, items 18, rule 7.6(2)(a)]***

On record-keeping, consequential amendments are made to ensure a CDR consumer may request an accredited data recipient for copies of records that relate to the consumer, in connection with trusted advisers, CDR insights and CDR representative arrangements. ***[Schedule 6, item 20, rule 9.5(2)]***

Amendments are made to improve the presentation of the information security controls table in Schedule 2 to the CDR Rules (which relates to privacy safeguard 12 – security of CDR data held by accredited data recipients). ***[Schedule 6, item 22, table in clause 2.2 of Schedule 2 to the CDR Rules]***

Under section 56BL of the Act, the rules may specify that certain provisions of the rules are civil penalty provisions (within the meaning of the *Regulatory Powers (Standard Provisions) Act 2014*). Amendments are made to Rule 9.8 to include the new civil penalty provisions set out above in this explanatory statement. ***[Schedule 6, item 21, rule 9.8]***

Civil penalty provisions

The default maximum civil penalty for a breach of CDR Rules is $500,000 for an individual. For a body corporate, the maximum is the greatest of:

- $10 million;
- if the court can determine the value of the benefit obtained and that is reasonably attributable to the act or omission – three times the value of that benefit; and
- if the court cannot determine the value of that benefit – 10% of annual turnover during the period of 12 months ending at the end of the month in which the act or omission occurred.

The Act provides that where a civil penalty does apply to a breach of the CDR Rules, the CDR Rules may specify a lower penalty amount than the default maximum. If the CDR Rules do not specify an amount, then the maximum civil penalty is as per the amount worked out under paragraph 76(1A)(b) of the Act.

This explanatory statement indicates where the Amending Rules introduce a civil penalty provision and the rationale for each penalty. It also indicates whether the default maximum civil penalty applies or a lower maximum is set to reflect the particular nature of the obligation.

The Amending Rules introduce civil penalties for record keeping and reporting obligations in relation to the new rules for sponsored accreditation and CDR representatives, as well as the new disclosure options for trusted advisers and CDR insights. The Amending Rules specify that these maximum civil penalties ($50,000 for an individual and $250,000 for a body corporate) are set below the default maximum civil penalty.

Rules 9.3 and 9.4 set out obligations on data holders and accredited data recipients to keep and maintain records of a range of specified matters relating to disclosure of CDR consumers' data. As CDR regulators, the OAIC and ACCC may require data holders and accredited data recipients to provide copies of these records, as needed in the performance of their statutory functions. CDR consumers may also require data holders and accredited data recipients to provide them with copies of certain kinds of records required to be kept by rule 9.3. Compliance with these record keeping requirements is critical to support effective enforcement of the CDR obligations by the ACCC and OAIC, and to enable consumers to obtain records to assist them in using the dispute resolution processes available under the CDR regime to resolve disputes with CDR participants. These obligations reflect the importance of the availability and accuracy of records to enable the effective operation of the CDR regulatory framework and the maximum penalties in relation to these obligations reflect the importance of compliance and are therefore appropriate and proportionate.

ATTACHMENT B

Statement of Compatibility with Human Rights

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021

This Legislative Instrument is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Overview of the Legislative Instrument

The purpose of the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021* (the Amending Rules) is to amend the *Competition and Consumer (Consumer Data Right) Rules 2020* (the CDR Rules) to:

- facilitate greater participation in the CDR regime by participants and consumers;
- provide greater control and choice to consumers in sharing their data;
- promote innovation of CDR offerings including intermediary services; and
- enable services to be more effectively and efficiently provided to customers.

Schedule 1 to the Amending Rules implements the sponsored accreditation model. This reduces the cost of accreditation by altering certain obligations to establish information security capability as part of the accreditation process and ongoing accreditation obligations.

Schedule 2 to the Amending Rules establishes the CDR representative model. This allows eligible participants to access the CDR and use data without the need for accreditation in circumstances where they offer CDR-related services to consumers as a representative of an accredited data recipient.

Schedule 3 to the Amending Rules allows consumers to nominate persons as trusted advisers to whom an accredited person may disclose the consumer's data outside the CDR regime. The classes of trusted advisers are professions that are considered to be sufficiently regulated to ensure a strong level of consumer protection is maintained.

Schedule 3 to the Amending Rules also introduces the concept of a CDR insight. This allows CDR consumers to consent to their data being shared outside the CDR regime for prescribed purposes that are considered low risk and that are designed to limit the data shared to only what is necessary for the consumer to receive a service.

Schedule 4 to the Amending Rules provides for joint accounts to be in scope for data sharing under the CDR by default (a 'pre-approval' setting), with mechanisms by which a joint account holder may adjust or change the pre-approval option also provided. Any joint account holder may withdraw a consent for data sharing on an account at any time.

Schedule 5 to the Amending Rules provides for staged implementation of rules relating to joint accounts and 'direct to consumer' obligations in the banking sector.

Schedule 6 to the Amending Rules enables an accredited person to rely on unaccredited outsourced service providers to collect CDR data and thereby reduce the cost of building and operating application programming interfaces that connect to data holders.

Schedule 6 to the Amending Rules also makes consequential and minor amendments, with Schedule 7 to Amending Rules setting out transitional matters relating to the joint account amendments.

Human rights implications

CDR Representatives, Trusted Advisers and CDR Insights

The Amending Rules engage the right to protection from unlawful or arbitrary interference with privacy under Article 17 of the International Covenant on Civil and Politics Rights (ICCPR) because they provide for new avenues for third parties to engage with consumer data, including instances where consumer data may leave the CDR regime.

The right in Article 17 may be subject to permissible limitations, where these limitations are authorised by law and are not arbitrary. In order for an interference with the right to privacy to be permissible, the interference must be authorised by law, be for a reason consistent with the ICCPR and be reasonable in the particular circumstances. The UN Human Rights Committee has interpreted the requirement of 'reasonableness' to imply that any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case.

Under the existing CDR rules, data holders can disclose consumer data to accredited data recipients, where the consumer to whom the data pertains has provided consent for their data to be transferred. The privacy of the consumer is protected by several Privacy Safeguards that require data holders and accredited data recipients to ensure the protection of the consumers for whom they hold data.

The Amending Rules provide for new recipients of data including CDR representatives and trusted advisers, as well as recipients of CDR insights derived from consumer data. In each of these circumstances, consumers must still consent for the transfer of these data. As such, the interference with a consumer's privacy is proportional to the objectives of increasing access to and meeting demand for goods or services under the CDR regime, and consistent with their consent to exchange a measure of privacy in exchange for the provision of these goods and services.

Joint accounts: pre-approval

The Amending Rules set a new default approval setting for joint account holders when an accredited person makes a consumer data request on behalf of one joint account holder or a secondary user. By default, the pre-approval option applies, which allows an individual joint account holder to independently share data on the joint account by consenting to an accredited person collecting and using the data from a joint account. A data holder must process the request unless an account holder has withdrawn their approval, in which case, the data holder cannot disclose the requested data.

These amendments engage Article 17 as, by default, some joint account holders will not be actively providing consent for the disclosure of data that pertains to them as a consumer and this may have an impact on their privacy. However, the basis for these amendments is aligning joint account disclosure with the existing ability of joint account holders to view and share their joint account data. Additionally, any given account holder can unilaterally change the approval option to a more restricted privacy setting (either non-non-disclosure or co-approval, where that is offered by a data holder) whilst changing the option to a more open setting requires approval of all joint account holders. Additionally, under the Amending Rules, joint account holders receive notification when their data is shared, providing a greater level of transparency about their privacy than exists outside of the CDR regime.

As such, these amending provisions are consistent with Article 17 of the ICCPR, as they are proportional to the end sought and necessary in the circumstances.

Avoidance of harm

The Amending Rules also engage the ICCPR right to privacy by expanding the existing harm prevention measures available to data holders.

The existing CDR rules allowing for a data holder to refuse to disclose consumer data where the data holder considers it necessary to prevent physical or financial harm or abuse. The Amending Rules also engage the ICCPR right to privacy as it expands the harm prevention measures available to data holders such that in certain circumstances they may make disclosures without all account holders' consent.

For joint accounts, where a data holder considers that it is necessary to prevent physical, psychological or financial harm or abuse to any person, they are not held liable if they fail to comply with the requirement of Part 4A. As a consequence of this, where a data holder considers it necessary to prevent harm, they may permit a disclosure request that otherwise would not have been allowed due to a joint account requiring all account holders to approve the disclosure.

The right to protection from exploitation, violence and abuse is contained in article 20(2) of the International Covenant on Civil and Political Rights, article 19(1) of the Convention on the Rights of the Child and article 16(1) of the Convention on the Rights of Persons with Disabilities.

The avoidance of harm provisions in the Amending Rules provides a balancing point against these competing rights, by ensuring that the CDR regime is not an impediment to the operation of existing harm prevention measures utilised by CDR participants.

Civil penalties

Like the existing CDR rules, the Amending Rules introduce several civil penalty obligations. These civil penalty provisions potentially invoke Articles 14 and 15 of the ICCPR. Although the Articles cover criminal process rights, in international human rights law, where a civil penalty is imposed, it must be determined whether it nevertheless amounts to a 'criminal' penalty. As with the existing civil penalties, the new civil penalty provisions should not be considered 'criminal' for this purpose. While they are intended to deter non-compliance with CDR obligations, none of the provisions carry a penalty of imprisonment for non-payment of a penalty.

Conclusion

The Amending Rules are consistent with human rights and freedoms.