EXPLANATORY STATEMENT

Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020

Prepared by the Australian Competition and Consumer Commission

Explanatory Statement: Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020

Background

1. This Explanatory Statement accompanies the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3)* 2020 (**Amending Instrument**) which amends the *Competition and Consumer (Consumer Data Right) Rules* 2020 (**Rules**).

2. The Rules are a critical component of the Consumer Data Right (**CDR**) regime, an economy-wide reform that gives consumers the ability to safely, efficiently and conveniently access specified data about them. This data is held by businesses (data holders) and consumers may request that data be disclosed to accredited data recipients (**ADRs**).

Purpose

3. The Australian Competition and Consumer Commission (**ACCC**) made foundational Rules in February 2020.

4. The primary purpose of the Amending Instrument is to expand and build the functionality of the CDR regime, in line with the recommendations of the Open Banking Review.[1] The Amending Instrument also makes amendments to clarify the application and operation of the Rules.

Changes to rules about consents

5. The Amending Instrument introduces additional functionality to the rules relating to consents.

6. The Rules as amended (**Amended Rules**) allow accredited data recipients (**ADRs**) to offer to their CDR consumers the ability to amend an existing consent. This includes the ability to add or remove uses, data types, accounts or data holders, or to amend the duration of the consent.

7. The Amended Rules also provide for separate consent types — including consents for collection, use, disclosure, direct marketing and research – which operate independently of each other. This means that consumers can give more than one type of consent and can independently withdraw or amend each type of consent. A consumer may stop the collection of CDR data by withdrawing the authorisation they gave to the data holder. Alternatively, if the ADR provides this functionality, they may either withdraw or amend the consent to collect.

8. The Amended Rules provide that when a consumer withdraws an authorisation to disclose CDR data given to a data holder, the consumer's associated consent to collect the CDR data with an accredited person expires. At this point, the accredited person must inform the consumer that they may also withdraw their use consent, and they may make the election to delete redundant data in respect of CDR data that has been collected under the collection consent under rule 4.16. However, the expiry of the collection consent does not automatically result in expiry of the use consent relating to any CDR data that has already been collected.

9. This addresses a potential source of confusion for CDR consumers, and the technical difficulties that may be faced by ADRs if they were required to delete or de-identify only a subset of CDR data they had already collected, as required under the former Rules. In

[1] *Open Banking: giving customers choice, convenience and confidence* (final report), December 2017.

effect, the Amended Rules mean consent to collect and consent to use do not have to align and the two consents may relate to different data types or time periods.

10. The means that following such a change, data already collected may not become redundant data (and therefore subject to deletion and de-identification obligations). The ADR may continue to use the already collected CDR data, and any CDR data that it may continue to collect, in accordance with the consent to use, until such time as the consent to use is withdrawn by the consumer or otherwise expires.
11. The Amended Rules introduce additional notification requirements to ensure the existence of use consents will be transparent to consumers.

Example of different approaches to redundant data

Redundancy when consent to collect and consent to use are aligned	**'Point in time' approach, where consent to collect and consent to use are not aligned**
Umbel offers consumers the ability to amend their consents to collect and use at the same time, including to remove data types that are 'optional' fields. After the amendment process, Umbel tells consumers: *You have successfully amended your consents to collect and use. We will no longer collect your account balance and details, and will delete this data in accordance with our CDR policy…*	Pard offers consumers the ability to amend their consents to collect, in order to remove data types that are 'optional' fields. After the amendment process, Pard tells consumers: *You have successfully amended your consent to collect CDR data. We will no longer collect your account balance and details, but we will use the data we've already collected. Don't worry – when you withdraw your use consent or when it expires on 1 October, we will delete it, along with all your other data in accordance with our CDR policy…*

Authorising transfers of CDR data between accredited persons

12. The Amended Rules permit accredited persons, with the consumer's consent, to collect CDR data from, and disclose CDR data to, other accredited persons who are also providing goods or services to the consumer.
13. Before CDR data can be disclosed to an accredited person, an ADR must have a valid consent from the consumer to disclose the CDR data to that accredited person and that accredited person must have a valid consent from the CDR consumer to collect the CDR data from the ADR.
14. Informed consumer consent is integral to transfers between accredited persons. The Rules therefore require the Data Standards Chair to make consumer experience data standards for the disclosure of CDR data to accredited persons. Disclosures to accredited persons will only be permitted from the earlier of: when the consumer experience data standards are made; or 1 July 2021, to provide time for the new standards to be made.
15. An accredited person who collects or discloses CDR data through this mechanism has obligations in relation to providing consumer dashboards, receipts and the appropriate notifications. Each accredited person is subject to the Privacy Safeguards set out in the *Competition and Consumer Act 2010* (Cth) (**Competition and Consumer Act**) sections 56ED-56EO. In particular, Privacy Safeguard 10 (notifying of the disclosure of CDR data) and Privacy Safeguard 11 (quality of CDR data) also apply to transfers of CDR data between accredited persons.

16. The Amending Instrument also expands the circumstances in which an accredited person may engage in direct marketing. In particular, the Amended Rules permit an accredited person to recommend to a consumer the goods or services of another accredited person, provided that the first accredited person:
    a. has a valid direct marketing consent from the consumer; and
    b. reasonably believes that the CDR consumer may benefit from the goods or services of the second accredited person.
17. The purpose of this provision is to facilitate instances where, in order to provide those goods or services, the second accredited person would be collecting data from the first accredited person.

Authorising use of CDR data for research

18. Prior to these amendments, the Rules restricted ADRs from using CDR data for purposes beyond what was reasonably needed in order to provide the requested goods or services.
19. The Amended Rules authorise an ADR that seeks to collect and use CDR data for the purpose of providing a good or service to the consumer, to also seek the consumer's consent de-identify some or all of the data to be used for general research purposes.
20. Seeking a consumer's consent to use CDR data for this purpose is subject to limitations. The ADR cannot seek to collect CDR data for this purpose beyond what it needs in order to provide the good or service to the consumer. Additionally, the ADR may only use the CDR data for general research once it has been de-identified in accordance with the CDR de-identification process (see rule 1.17) . In seeking such a consent, the ADR must inform the CDR consumer that it intends to use the de-identified data for the purposes of general research and provide a link to a description in its CDR policy of the research to be conducted, and any additional benefits to be provided to the consumer for consenting to the use.
21. That research does not need to relate to any provision of goods or services to any particular CDR consumer. It may be for a purpose unrelated to that CDR consumer, such as the ADR's product or business development.

Changes to data holder obligations

Joint accounts

22. The Rules contain obligations for data holders in relation to joint accounts. The Amended Rules expand those obligations in a number of ways.
23. Where a consumer has not previously set up preferences for sharing from a joint account (for example, where the consumer is initiating data sharing for the first time under the CDR), data holders will be required to allow consumers to set their preferences as part of the authorisation process. This will be required of all data holders from 1 November 2021. Transitional provisions will apply to for initial data holders and reciprocal data holders, which are required to comply with joint account rules before 1 November 2021 (see clause 6.7 of Schedule 3). This process will require compliance with any relevant consumer experience data standards.
24. Under the amended joint account rules, data holders are required to, at a minimum, offer a joint account management service online. Data holders may also choose to also offer that service through offline channels. The Amended Rules detail the requirements for the joint account management service, as well as notification requirements, formalising guidance on the existing Rules previously issued by the ACCC.

25. The Amending Instrument also expands the definition of joint accounts, from accounts held in the name of two individuals, to include joint accounts held in the name of two or more individuals.

26. The Amending Instrument also allows data holders to treat a joint account as if it was held in the name of one individual, where it considers this is necessary in order to prevent physical or financial harm or abuse.

Data holder dashboards and authorisation processes

27. The Amending Instrument increases transparency for consumers by requiring data holders to include additional information in the consumer dashboard and during the authorisation process. Further to including the name of the accredited person, the Amended Rules require the display of:

    a. additional information that is held in the Register, such as the software product name used by the accredited person, for the purpose of inclusion in the authorisation process or inclusion on the consumer dashboard; and

    b. additional information received through the data standards for the purpose of inclusion in the data holder's consumer dashboard, such as information to distinguish between consents where an accredited person utilises concurrent consents.

28. These requirements will apply at a time when the additional information is required by the Registrar to be provided as part of being on-boarded to the Register and/or when data standards are made for this purpose.

Changes to who may share CDR data

29. The Amending Instrument broadens the scope of consumers who may share CDR data. Prior to these amendments, sharing of CDR data was limited to account holders that were individuals (including sole traders) aged 18 or over, from accounts held singly or jointly with one other individual.

30. The Amended Rules additionally enable CDR data to be shared by non-individuals, in the context of business partnerships, and by secondary users. This functionality must be made available by initial data holders in respect of their primary brands[2] from 1 November 2021, and otherwise for all data from 1 November 2022.

Use of the CDR logo

31. The Amended Rules require an accredited person to ensure it is licensed or otherwise authorised to use any CDR logo approved by the ACCC, including as required by the data standards.

32. Where an accredited person is not licensed or otherwise authorised to use any CDR logo, this may constitute a ground for suspension or revocation of accreditation.

Clarifying rule amendments

The application of product data request rules to 'white labelled' products

33. The Amended Rules provide certainty about the applicability of product data request obligations to products known as 'white-labelled' products, when both the white labeller (the supplier of the product) and the brand owner (the retailer or distributor of the product) are data holders. These rules reflect previously issued guidance from the ACCC.

[2] I.e. NAB, CBA, ANZ and Westpac branded products

34. For these white label products, where more than one data holder is involved in offering the product, the data holder responsible for responding to product data requests is the data holder that enters into a contractual relationship with the consumer. The Rules do not preclude the other data holder from responding or from agreeing to respond on behalf of the data holder that enters into the contractual relationship with the consumer.

Closed accounts

35. The Amended Rules align data sharing requirements for closed accounts across transaction data, account data and product specific data so that a data holder is only required to share these categories of data if a request is made within 24 months of the account being closed.

Reporting and record keeping requirements

36. The Amended Rules provide further clarity regarding CDR participants' record keeping and reporting obligations. The amendments will improve the quality and format of the necessary information reported to the ACCC and Office of the Australian Information Commissioner. The Amended Rules also enhance a CDR consumer's access to their records as held by data holders and ADRs.

Required and voluntary product data disclosures

37. The Amended Rules clarify that the product data that a data holder is required to disclose may include not only information contained in a Product Disclosure Statement, but also information that is required to be disclosed under the National Consumer Credit Protection Act 2009, or that is otherwise required by law to be disclosed to a customer entering into a contract.

38. The Amended Rules require a data holder that discloses requested voluntary product data to do so through its product data request service and in accordance with the data standards. These provisions mirror those for the disclosure of required product data.

Functions and powers of the Accreditation Registrar

39. The Amended Rules provide the Accreditation Registrar (Registrar) with additional powers that can be exercised if the Registrar believes that it is necessary to protect the security, stability and integrity of the Register and the associated database, which contains information relating to data holders.

40. The Rules already provide for action to be taken in relation to accredited data recipients by decisions of the Data Recipient Accreditor to revoke or suspend accreditation where it is necessary to protect the security, stability and integrity of the Register, and for consequential action to be taken by the Registrar in those circumstances.

41. The Amended Rules will allow the Registrar to take steps to prevent the Register and associated database from being used to make consumer data requests to a data holder for a period up to 10 days. The steps taken by the Registrar may include amending the information in the associated data base relating to a data holder that is used to facilitate the making and processing of requests (for example, to change a data holder's status from 'active' to 'inactive'). The Registrar will also be able to take any other steps required to protect the security, integrity and stability of the Register. This would include revocation of PKI certificates issued to the data holder.

42. The Registrar will also be able to direct an accredited person not to make consumer data requests, or a data holder not to respond to consumer data requests, for a period of up to 10 days.

43. The exercise of these new powers will not be subject to merits review. This is because the powers are limited as they can only be exercised for a period of up to 10 days.

Scheduled commencement

44. The Amended Rules update the commencement dates of mandatory data sharing obligations for data holders. The amended table reflects existing exemptions made by the ACCC which exempt some data holders from particular obligations. The Amended Rules also remove references to 'voluntary participating ADIs'. Early data sharing by ADIs will be possible under on clause 6.5 of Schedule 3 of the rules, and by engaging with the ACCC in its capacity as the Registrar to be on-boarded as a data holder.

Authority for making the Amending Instrument

45. The Amending Instrument was made under section 56BA of the Competition and Consumer Act which enables the ACCC to make consumer data rules and, relying on subsection 33(3) of the *Acts Interpretation Act 1901* (Cth), includes the power to amend the rules.

46. The Minister consented to the ACCC making the Amending Instrument in accordance with section 56BR of the Competition and Consumer Act.

47. Before making consumer data rules, section 56BP of the Competition and Consumer Act requires the ACCC to have regard to certain matters outlined in section 56AD. These include the likely 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 process for making the Amending Instrument involved consideration of the matters outlined in section 56AD, including through public consultation on draft amendments.

Statement of compatibility with human rights

48. This statement is prepared in accordance with Part 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011* (Cth).

49. The Amending 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* (Cth).

Human right implications

50. The Amending Instrument is consistent with the right to protection from unlawful or arbitrary interference with privacy under Article 17 of the International Covenant on Civil and Political Rights (**ICCPR**).

51. The amendments relating to consent, the extension of data sharing rights to more CDR consumers, and new data holder obligations promote this right, as they give consumers greater control over their CDR data. The amendments that authorise the transfer of CDR data between accredited persons and the use of CDR data for research preserve the protections against unlawful or arbitrary interference with privacy, by making consumer consent a necessary precondition of such transfers, disclosures and uses.

52. The clarifying amendments and the amendments relating to the CDR logo do not alter the effect of the Rules with respect to Article 17. However, the effect of these amendments is to ensure that the overall operation of the Rules remains in line with the protections afforded by Article 17.

Conclusion

53. The Amending Instrument is compatible with human rights and freedoms.

Privacy impact assessment

54. An independently prepared draft of the Privacy Impact Assessment report was released for consultation alongside the draft rules on 30 September 2020. This was prepared as an update to the Privacy Impact Assessment dated March 2019, published by The Treasury and the Privacy Impact Assessment Update 1 dated 6 October 2020.
55. A final Privacy Impact Assessment report will be published on the ACCC's website.

Regulatory impact analysis

56. The Amending Instrument falls within the scope of the regulation impact assessment undertaken at the time of making the Rules. The Amended Rules do not depart significantly from the original consideration. On this basis, the Office of Best Practice Regulation advised that a Regulation Impact Statement was not required (OBPR reference ID 24996).

Consultation

57. Draft rules were released for consultation on 30 September 2020, for a period of 28 days. The ACCC received 53 public submissions.
58. The ACCC also consulted with the Information Commissioner, The Australian Securities and Investment Commission and the Australian Prudential Regulation Authority.
59. This satisfies the consultation requirements specified in section 56BQ of the Competition and Consumer Act.

Explanatory Notes

Schedule 1

Item 1: Rule 1.4

This item amends rule 1.4 and the simplified outline of the rules as it relates to CDR consumer data requests made on behalf of CDR consumers. The amendment replaces the paragraphs to reflect that consumer data requests can be made on behalf of CDR consumers by accredited persons to a CDR participant, where a CDR participant means both a data holder and an accredited data recipient. It also sets out that a consumer data request that is made to a data holder on behalf of a CDR consumer must be made in accordance with relevant data standards, using a specialised service provided by the data holder and that the CDR data is disclosed in machine readable form to the accredited person. Finally, it outlines that under the data minimisation principle, the accredited person may only collect and use CDR data in order to provide goods or services in accordance with a request from a CDR consumer, and may only use it for that purpose, or for a limited number of other purposes which require additional consent from the CDR consumer.

Item 2: Subrule 1.6(4)

This item amends subrule 1.6(4) by replacing the words “are made by accredited persons on behalf of such eligible CDR consumers” with the words “involve accredited persons” to reflect the expanded role of accredited persons in the collection, use and disclosure of CDR data.

Items 3-10: Subrule 1.7(1)

These items insert and amend a number of definitions in subrule 1.7(1) as part of the revisions and expansions made to the rules.

Item 11: Subrule 1.7(5)

This item is a minor amendment to replace “collecting consumer data” with “collecting CDR data” to ensure consistency with using defined terms. CDR data is a defined term in the Competition and Consumer Act.

Item 12: Paragraph 1.8(b)

This item replaces paragraph 1.8(b) to reflect that the second limb of the data minimisation principle applies equally to the use of CDR data for the provision of requested goods or services and the use of CDR data for any other purpose consented to by the relevant CDR consumer.

Item 13: Subrule 1.9(2) (definition of serious criminal offence*)*

This item amends subrule 1.9(2) to correct a typographical error by deleting the words “have been” from the definition of *serious criminal offence*.

Item 14: After rule 1.10, insert new rule 1.10A Types of consents.

This item inserts rule 1.10A. It details the types of consents that a CDR consumer can give an accredited person or an accredited data recipient.

A *collection consent* is a consent given by a CDR consumer for an accredited person to collect particular CDR data from a CDR participant for that CDR data.

A *use consent* is a consent given by a CDR consumer for an accredited data recipient of particular CDR data to use that CDR data in a particular way.

A *disclosure consent* is a consent given by a CDR consumer for an accredited data recipient of particular CDR data to disclose that CDR data to an accredited person in response to a consumer data request (an *AP disclosure consent*) or to an accredited person for the purposes of direct marketing.

A *direct marketing consent* is a consent given by a CDR consumer under these rules for an accredited data recipient of particular CDR data to use or disclose the CDR data for the purposes of direct marketing.

A *de-identification consent* is a consent given by a CDR consumer under these rules for an accredited data recipient of particular CDR data to de-identify some or all of the collected CDR data and do either or both of using the de-identified data for general research or disclosing (including by selling) the de-identified data.

Categories of consent are introduced in subrule (2) and are based on the types of consents detailed above. They are referred to throughout the rules. For example, rule 4.12(3)(a) provides that an accredited person must not ask for a consent that is not in a category of consents.

Item 15: Rule 1.11

This item amends rule 1.11, which provides a simplified outline of the Division, by replacing the words *"withdrawing consents and authorisations"* with the words *"**amending** or withdrawing consents, and for withdrawing authorisations."*

Items 16: and 17: At the end of subrule 1.13(1)

These items add requirements for the consumer data request service that must be provided by a data holder. The additional requirements apply in respect of three particular classes of consumers:

- non-individuals (such as limited companies);
- business partnerships with a partnership account; and
- account holders with accounts with the data holder in respect of which another person has (or other persons have) account privileges.

These additional service requirements are designed to facilitate the sharing of consumer data by non-individuals, business partnerships and secondary account users. This increased functionality aligns with the expansion of eligible CDR consumers able to request their CDR data.

The amendments require data holders to provide both non-individuals and business partnerships with a consumer data request service that enables these groups to nominate one or more individuals (such as an employee or a partner in a business partnership) to grant and revoke authorisations to disclose CDR data on their behalf. Note 3 clarifies that a nomination must be made if the sharing by such CDR consumers of their CDR data is to be enabled.

The amendments also require data holders to provide a consumer data request service with the functionality that enables account holders to make or revoke an instruction that allows a secondary user of the account to share CDR data related to the account on and from

1 November 2021 for initial data holders in respect of their primary brands, and otherwise 1 November 2022 for all data holders (see item 103).

Item 18: Subrule 1.14(1)

This item repeals and substitutes subrule 1.14(1). The rule now applies to all the types of consent.

Item 19: insert new subrule 1.14(2A)

This item outlines that on and from 1 July 2021, accredited persons may offer CDR consumers the functionality on the consumer dashboard to amend a consent. The delayed ability to rely on these rules allows time for consequential changes to the consumer experience data standards (if any) to be made.

Item 20: Subrule 1.14(3)

This item repeals and replaces subrule 1.14(3) which concerns the information an accredited person must provide in a CDR consumer's consumer dashboard. The new subrule reflects the introduction of different types of consent (see item 14, rule 1.10A) and recognises that an accredited person may have separate consents from a CDR consumer to collect CDR data, to use CDR data and to disclose CDR data. The new subrule expands the information to be included on the dashboard to encompass any amendments to consents, if the ADR offers that functionality.

Item 21: Rule 1.15

This item repeals and replaces rule 1.15 which concerns the consumer dashboard a data holder must provide to the CDR consumer.

The consumer dashboard must now also contain:

- any information in the data standards that is specified as information for the purposes of this rule;
- any information on the Register of Accredited Persons that is specified as information for the purposes of this rule; and
- any other details, and have any other functionality, required by a Schedule to these rules in relation to a particular designated sector (clause 4.14 of schedule 3 contains the details and functionality for the banking sector).

The Note at subrule (2) now refers to secondary users in addition to joint account holders.

Sub-rule (2A) mandates that the dashboard service must only allow nominated representatives to manage authorisations where the CDR consumer is not an individual or where the CDR data relates to a partnership account.

Subrules (5) – (7) relate to secondary users.

If the CDR consumer is a secondary user for an account, the data holder must also provide the account holder with an online service that contains the details of any authorisation to disclose given by the secondary user. That service must include functionality that enables an account holder to withdraw a secondary user instruction and indicate that they no longer approve a secondary user sharing CDR data relating to that account, as referred to in subparagraph 4.6A(a)(ii) (see Item 42) .If the account holder makes such an indication, the data holder will no longer be able to disclose CDR data relating to that account to that accredited person.

As part of the withdrawal process, the service also must display a message relating to the consequences of the withdrawal in accordance with the data standards.

This functionality must be simple and straightforward to use and no more complicated than the instruction and authorisation processes. A data holder does not contravene these requirements so long as it takes reasonable steps to ensure this functionality. In addition, these functions must be prominently displayed.

This subrule is a civil penalty provision.

If the data holder provides a consumer dashboard to the account holder, the online service must be included in that dashboard.

Item 22: Subdivision 1.4.4 (heading)

This items deletes "and accredited data recipients" from the heading of Subdivision 1.4.4.

Item 23: Paragraph 1.18(c)

This item simplifies the language of paragraph 1.18(c).

Item 24: Rule 2.3

This item inserts the words "*or on behalf of*" after the words "*offered by*". This accommodates the making of product data requests where there may be two data holders involved in offering a product, or where there may be a data holder who offers a product on behalf of another person, or a person who offers a product on behalf of a data holder. This clarifies data holder obligations for product data requests made in relation to white label products.

Item 25: insert new subrule 2.4(2A)

This item inserts a new subrule 2.4(2A) which requires a data holder that discloses voluntary product data to a requester to do so through its product data request service and in accordance with the data standards. This aligns with the existing drafting in rules 2.1 and 2.2.

This is a civil penalty provision.

Items 26 to 28: rule 2.4

Rule 2.4 deals with disclosures of product data in response to a product data request.

Item 28 adds new subrules 2.4(4) and (5), which recognise that two data holders may hold data about one product that they offer, for example in the case of 'white labelled products'.

White labelled products will often be provided by two data holders:

1. the 'brand owner', who typically brands and retails a white labelled product on behalf of; and
2. the 'white labeller', who typically creates and supplies the white labelled product.

The consumer will generally enter into a contractual arrangement with the white labeller, and the white labeller typically is responsible for compliance with regulatory obligations.

Subrule (4) applies if a data holder (the ***first data holder***) receives a request for CDR data that relates to a product and the first data holder offers the product on behalf of another data holder (the ***second data holder***), such that the second data holder is the data holder that enters into contracts with consumers to provide the product. In those circumstances, the first

data holder is not required to disclose the requested required product data as would otherwise be required under subrule (3) (see Item 26).

Subrule (5) allows the first data holder to respond to a request received by the second data holder if the data holders have agreed in writing that the first data holder will disclose the requested required product data.

Subrules (4) and (5) are intended to avoid unnecessary duplication across multiple data holders by allowing flexibility for the first data holder (i.e. the data holder who does not enter into a contractual relationship with the consumer) to also respond to product data requests that they receive if they choose to, or for the data holders to reach agreement on who will meet the obligation in practice, while ensuring there is certainty about which data holder retains the regulatory obligation.

Item 28 also adds subrule (6). This defines a 'disclosure document' for the purposes of the amendment to subrule 2.4(3)(b)(ii)(B) (Item 27) which substitutes 'disclosure document' for the narrower term 'Product Disclosure Statement'. Disclosure document is defined as a Product Disclosure Statement within the meaning of the *Corporations Act 2001*, or a key facts sheet within the meaning of the *National Consumer Credit Protection Act 2009*, or a similar document that is required by law to be disclosed to a customer prior to entering into a contract with that customer. These amendments provide additional clarity about what data must be disclosed in response to, for example:

- a product data request concerning a credit card (which may not be subject to the regulatory requirement to provide a product disclosure statement); or
- a product data request concerning a white labelled product for which product data may not be contained on the white labeller's website.

Item 29: Division 4.1 of Part 4

This item repeals and replaces Division 4.1 of Part 4. Division 4.1 sets out a simplified outline of Part 4 and reflects that consumer data requests can be made by accredited persons on behalf of CDR consumers to both a data holder and to an accredited data recipient (together referred to as CDR participants). It also provides a simplified outline of the steps a data holder must take if it receives a consumer data request from an accredited person, and what an accredited data recipient may do if it receives a consumer data request from an accredited person.

Items 30 and 31: Division 4.2

These items amend the Division heading to recognise that consumer data requests can be made to CDR participants and inserts a new rule 4.2 which provides a flowchart for how consumer data requests can be made by an accredited person to CDR participants. The flowchart illustrates how the process differs between a consumer data request being made to a data holder and a consumer data request being made to an accredited data recipient.

Item 32: Rules 4.3 and 4.4

Item 32 repeals rules 4.3 and 4.4 and substitutes them with new rules to accommodate the various amendments that allow for requests to be made to accredited persons, in addition to data holders, and which introduce different types and categories of consent and specifically the separation of a consent to collect from a consent to use.

In rule 4.3, references to data holders are replaced with references to CDR participants to clarify that an accredited person can make requests to both accredited data recipients and data holders.

Subrule (3) clarifies that a request is valid if the CDR consumer provides both a collection consent and a use consent for the CDR data. Subrule (4) provides that a request ceases to be valid if the **collection** consent is withdrawn. The Note clarifies that the use consent, if not withdrawn, continues to have effect (see paragraph 10 on page 2 above)

An accredited person must ask for consent in accordance with division 4.3 which now encompass provisions relating to all types and categories of consent.

Rule 4.4 is placed within a new subdivision 4.2.3, '*Consumer data requests by accredited persons to data holders*'. Amendments are made to clarify that this rule applies specifically to consumer data requests by an accredited person to a data holder, and to reflect the amendments made to rule 4.3 as noted.

Items 33 to 35: rule 4.5

These items clarify rule 4.5 by indicating that it applies if a data holder receives a consumer data request under rule 4.4 (formerly under Part 4). Notes that are no longer required have been removed.

Items 36 to 41: rule 4.6

Rule 4.6 applies if a consumer data request is made under rule 4.4 (formerly under Part 4). Subrules 4.6(2) and (4) are made subject to new rule 4.6A (See Item 42). Notes to these subrules provide guidance in relation to joint accounts in the banking sector as additional requirements contained in Part 4 of Schedule 3 need to be met for a disclosure to be authorised.

Item 42: new rule 4.6A

Item 42 inserts a new rule 4.6A which prevents a disclosure being made in relation to an account without the account holder's approval.

Subrule (a) provides that a data holder must not disclose requested CDR data if the request was made on behalf of a secondary user of the account and the account holder has indicated, through their consumer dashboard, that they no longer approve CDR data relating to that account being disclosed to that accredited person in response to consumer data requests made by that secondary user.

Subrule (b) allows for sector specific provisions to be made. For the banking sector, clause 4.13 of Schedule 3 (which is contained within item 92) applies.

Item 43: new subdivision 4.2.4

Item 43 adds a new subdivision 4.2.4 which contains new rules 4.7A and 4.7B. These rules provide for consumer data requests by accredited persons to accredited data recipients. [3]

Rule 4.7A allows an accredited person to make a consumer data request to an accredited data recipient. It mirrors rule 4.4, which allows an accredited person to make a consumer data request to a data holder.

Rule 4.7B allows an accredited data recipient to ask a CDR consumer for a disclosure consent to disclose CDR data to an accredited person in response to a consumer data request (an **AP disclosure consent**) if:

[3] In relation to the new rules about transfers between accredited persons, the terms 'accredited person' and 'accredited data recipient' are used in the rules and this Explanatory Statement to differentiate between the person requesting and receiving particular CDR data (the accredited person) and the person disclosing it (the accredited data recipient).

- it receives, or reasonably anticipates receiving, a consumer data request under rule 4.7A;
- there is no current AP disclosure consent for the accredited data recipient to disclose the requested data to the person who made the request; and
- the accredited data recipient reasonably believes that the request was or will be made by an accredited person on behalf of an eligible CDR consumer.

If an accredited data recipient asks for an AP disclosure consent, it must do so in accordance with Division 4.3. This is a civil penalty provision.

Item 44: Division 4.3

Item 44 repeals the previous Division 4.3 dealing with "consents to collect and use CDR data" and replaces it with a new Division 4.3 that deals with "giving and amending consents".

Rule 4.8 is expanded to include:

- disclosure consents; and
- the ability to amend consents.

Rule 4.9 now applies to all consents.

Rule 4.10 contains requirements relating to an accredited person's processes for seeking consent. An accredited person's processes for asking a CDR consumer to give and amend a consent must accord with consumer experience data standards. In relation to the application of other data standards, subrule 4.10(2) provides that these do not apply where the relevant consent being sought is for collection of CDR data from an accredited data recipient or a disclosure consent. Subrule 4.10(2) does not affect the application of other data standards in relation to any other processes for which an accredited person is responsible (for example data standards that may apply to encryption of data in transit in accordance with Schedule 2, Part 2 of the rules.)

During the consent process, an accredited person may refer to its CDR policy, so long as doing so would not be likely to reduce comprehensibility. This aligns with the provisions for seeking consent for general research, as information about that research and any benefits to be provided to the consumer must be included in the CDR policy and a link provided to that policy (see rule 4.15 below).

Rule 4.11 relates to asking a CDR consumer to give consent. New subrule (1A) provides that a disclosure consent for CDR data must not be sought unless a collection and use consent for that data has already been given. Subrule (1)(a) now applies to all consents.

A CDR consumer must be allowed to select, or an accredited person must clearly indicate, whether the consent would apply on a single occasion or over a specified period of time. For a disclosure consent, an accredited person must also allow the CDR consumer to select the person to whom the CDR data may be disclosed.

An accredited person must ask for the CDR consumer's express consent to the types of data, duration of consent, and if a disclosure consent, the person to whom data is to be disclosed, for each relevant category of consents.

If the accredited person intends to charge a fee for disclosure of CDR data, or pass on to the CDR consumer a fee charged by a data holder for disclosure of CDR data, it must clearly distinguish between the CDR data for which a fee will, and will not, be charged or passed on; and allow the CDR consumer to actively select or otherwise clearly indicate whether they

consent to the collection or disclosure, as appropriate, of the CDR data for which a fee will be charged or passed on.

Subrule (3)(e) now refers to a de-identification consent and so applies to de-identifying some or all of the collected CDR data and doing either or both of the following:

- using the de-identified data for general research; or
- disclosing (including by selling) the de-identified data.

Rule 4.12 now also provides that an accredited person must not ask for a consent that is not in a category of consents. This restricts the activities available to accredited data recipients to only those included within a category of consents.

Rule 4.12A provides that an amendment of a consent takes effect when the CDR consumer amends the consent.

Rule 4.12B allows an accredited person, from 1 July 2021, to invite a CDR consumer to amend a consent via its consumer dashboard or in writing directly to the CDR consumer. The accredited person may only make such an invitation if the amendment would:

- better enable the accredited person to provide the goods or services requested by the CDR consumer at paragraph 4.3(1)(a); or
- be consequential to an agreement between the accredited person and the CDR consumer to modify those goods or services and enable the accredited person to provide the modified goods or services. Modification, for these purposes, may include an invitation to extend the period over which the accredited person will provide the goods and services.

An invitation to amend the period referred to in paragraph 4.11(1)(b) must not be given:

- any earlier than a reasonable period before the current consent is expected to expire; or
- more than a reasonable number of times within this period.

It is not possible to extend a consent for more than a period of 12 months.

Example:

A CDR consumer has given a consent to an accredited data recipient in relation to CDR data for a period of three months. The accredited person invites the CDR consumer to extend the consent within the last three weeks of this period on two occasions. The accredited data recipient is in compliance with rule 4.12B(1).

Rule 4.12C contains provisions on the process of amending consents. If an ADR wishes to provide a CDR consumer with the ability to amend a consent, the process must follow the original process for giving a consent set out in subdivision 4.3.2. In the case of an amendment to a consent, the accredited person may also present certain details of the current consent as pre-selected options.

In addition to the information referred to in subrule 4.11(3), the accredited person must also give the CDR consumer statements that outline:

- the consequences of amending a consent; and
- the extent to which the accredited person will be able to continue to use any CDR data that has already been disclosed to it.

Example

Laypac offers consumers the ability to amend their consents to collect, in order to remove certain data types. Prior to making an amendment, Laypac tells a CDR consumer:

"If you amend your consent, we will no longer collect your account balance and details, but we will use the data we've already collected. Don't worry – when you withdraw your use consent or when it expires on 1 October, we will delete it, along with all your other data, in accordance with our CDR policy…"

Rule 4.13 is amended to apply to all the types of consents. Note 1 of rule 4.13 is amended to clarify that an authorisation to disclose the CDR data expires when a data holder is notified of the withdrawal of a collection consent.

Rule 4.14 is included under Subdivision 4.3.2C, which sets out the duration of consent. Rule 4.14 is amended to apply to all the types of consents.

Subrule 4.14(1A) is introduced and provides that a collection consent expires when the accredited person is notified of the withdrawal of the authorisation to disclose CDR data. Subrule 4.14(1B) provides that where a current collection and AP disclosure consent exist in respect of CDR data, if one of those consents expire, the other consent expires when the accredited person or accredited data recipient is notified of the first mentioned expiry.

Subrule 4.14(1C) provides that if an accredited person becomes a data holder, rather than an accredited data recipient, of particular CDR data as a result of subsection 56AJ(4) of the Competition and Consumer Act and related clause 7.2 of Schedule 3, all of that accredited person's consents given by a CDR consumer under these rules that relate to that CDR data expire.

Rule 4.15 is amended to include additional information that must be provided in relation to a de-identification consent: a CDR consumer must be informed if an accredited person would use de-identified data for general research and must be provided with a link to a description in the accredited person's CDR policy of the research to be conducted and any additional benefit to be provided to the CDR consumer for consenting to the use. In subclause (b), the words "**that** it would disclose (by sale or otherwise) the de-identified data" are replaced with "**if** it would disclose (by sale or otherwise) the de identified data" as such a disclosure will not necessarily occur. If a disclosure occurs, the CDR consumer must be informed of that fact, as well as the matters in subclauses (b)(ii) and (b)(iii).

Rule 4.16 now applies to all types of consents.

Rule 4.17(1) is amended to clarify that it applies in relation to subparagraph 4.11(3)(h)(i).

Rule 4.18 is amended to include a disclosure consent as a trigger for a CDR receipt to be provided to a CDR consumer, as well as where a collection, use or disclosure consent is amended. CDR receipts must, in the case of a disclosure consent—include the name of the person the CDR consumer has consented to the disclosure of the CDR data to.

CDR receipts must be provided for all amendments, including where additional accounts are added or removed.

Rule 4.18A applies if, in relation to particular goods or services an accredited person is providing, as referred to in subrule 4.3(1), the collection consent expires, but the use consent is current. The accredited person must notify the CDR consumer as soon as practicable that, at any time, the CDR consumer may withdraw the use consent and may make the election to delete redundant data in respect of that CDR data under rule 4.16. This subrule is a civil

penalty provision. The notification must be given in writing otherwise than through the CDR consumer's consumer dashboard but may also be included in the consumer dashboard.

Rule 4.18B applies if:

- an accredited person has a collection consent relating to particular CDR data and a particular accredited data recipient; and
- the accredited data recipient has an AP disclosure consent relating to that CDR data and that accredited person.

If one of those consents expires, the accredited person or accredited data recipient must notify the other as soon as practicable of the first mentioned expiry. These subrules are civil penalty provisions.

Rule 4.18C applies where an accredited person has a collection consent in relation to a particular CDR participant which is amended. The accredited person must notify the CDR participant of the fact that the consent has been amended. Once a data holder receives this notice it must ask the CDR consumer to correspondingly amend the authorisation, as provided for in rule 4.22A. If the CDR participant is a data holder, the notice must be in accordance with the data standards. If the CDR participant is an accredited data recipient, the notice must be given as soon as practicable. This subrule is a civil penalty provision.

Rule 4.20 applies to the ongoing notification requirement to inform a CDR consumer that collection or use consents are current. The rule now extends to amendments of consents.

Item 45: Division 4.4

Item 45 repeals Division 4.4 and substitutes it with a new Division 4.4 containing a limited number of amendments.

Rule 4.22A is inserted and provides that if a data holder has received a notice under rule 4.18C, it must, in accordance with Division 4.4, invite the CDR consumer to amend the authorisation to disclose CDR data accordingly. An amendment of an authorisation to disclose CDR data other than in accordance with subrule 4.22A(1) is of no effect. However, subrule 4.22A(2) does not impact the ability for data holders to allow CDR consumers to add or remove accounts; this functionality remains at the discretion of data holders.

Rules 4.21 to 4.24 are amended to encompass the functionality of amending authorisations. Subrule 4.26(1)(g) now includes the ending of an amended authorised period of disclosure as a time at which an authorisation may expire.

A new subrule 4.23(2) is inserted and provides that a data holder must also give a CDR consumer any information that the Register of Accredited Persons holds in relation to an accredited person that makes a consumer data request, that is specified as information for the purposes of rule 4.23. This requirement will apply at a time when that kind of information is accommodated in the Register and sought by the Registrar as part of the on-boarding process. Subrule 4.23(1)(a) is subject to subrule 4.23(2).

Example:
Umbel offers an app named TaxCap. Umbel could require '*TaxCap by Umbel*' to be displayed during related authorisation processes.

Note 1 of rule 4.25 is amended to clarify that a consent for the accredited person to collect CDR data expires when the data holder notifies the accredited person that the authorisation to disclose that CDR data is withdrawn.

A new rule 4.28 is inserted and applies where a secondary user amends or withdraws an authorisation, or an authorisation given by the secondary user expires. In such circumstances, the data holder must, as soon as practicable, notify the account holder through its ordinary means of contacting them. This subclause is a civil penalty provision.

Item 46 and 47: Subrule 5.10(1) and 5.10(2)

Item 46 repeals subrule 5.10(1) and replaces it with a new subrule 5.10(1) and (1A). These amendments clarify that the Data Recipient Accreditor may impose any other condition on an accreditation and vary or remove any conditions imposed under this rule or rule 5.9, at the time of accreditation under subsection 56CA(1) of the Competition and Consumer Act or at any time after accreditation.

Item 47 substitutes the words “exercising a power” in place of the words “imposing or varying a condition” in subrule 5.10(2) so that it applies to the full range of powers available to the Accreditor under the rule (e.g. the removal of a condition of accreditation).

Item 48: new subrule 5.12(1)(f)

Item 48 adds a new subrule 5.12(1)(f) which provides that a person who is accredited at the “unrestricted” level must ensure that it is licensed or otherwise authorised to use any CDR logo, as defined in rule 1.7(1) in accordance with Item 6, including as required by the data standards.

Item 49: new rules 5.33 and 5.34

Item 49 adds two new rules into Part 5 which provide the Accreditation Registrar with certain powers intended to protect the security, integrity and stability of the Register of Accredited Persons and associated database.

Rule 5.33 deals with temporary restrictions on the use of the Register in relation to a data holder. It allows the Accreditation Registrar to take steps to prevent the Register of Accredited Persons and associated database from being used to make consumer data requests to a data holder, for a period of up to 10 days, if the Accreditation Registrar reasonably believes it is necessary to do so to ensure the security, integrity and stability of the Register or associated database. The Registrar may amend information in the associated database relating to a data holder to facilitate the making and processing of requests.

Before, or as soon as practicable after taking steps to prevent the Register of Accredited Persons and associated database from being used, the Accreditation Registrar must inform the data holder of the steps being taken and give the data holder a reasonable opportunity to be heard in relation to the matter.

A data holder is not required to disclose CDR data in response to a request where to do so would require using the Register of Accredited Persons or associated database in a way that is not available to the data holder at that time by reason of the steps taken by the Accreditation Registrar.

Rule 5.34 deals with a temporary direction to refrain from processing consumer data requests. It allows the Accreditation Registrar to direct an accredited person not to make consumer data requests, or direct a data holder not to respond to consumer data requests for a period of up to 10 days if the Accreditation Registrar reasonably believes it is necessary to ensure the security, integrity and stability of the Register or associated database.

The notice must specify the period of application and whether the direction applies to all consumer data requests or to consumer data requests made to a particular data holder or by a particular accredited person.

Before, or as soon as practicable after giving a direction, the Accreditation Registrar must give the accredited person or the data holder a reasonable opportunity to be heard in relation to the matter.

An accredited person must not make a consumer data request contrary to a direction it has received and a data holder must not disclose CDR data in response to a consumer data request contrary to a direction it has received. This is a civil penalty provision.

Item 50: new paragraph 7.2(4)(ca)

Item 50 inserts a new paragraph 7.2(4)(ca) that requires an accredited person who wishes to undertake general research using CDR data to include in its CDR Policy a description of the research to be conducted and a description of any additional benefit to the CDR consumer for consenting to the use of their CDR data for general research. As defined in rule 1.7(1), general research can only be conducted using de-identified CDR data. This aligns with the new information required to be presented to the CDR consumer under new subrule 4.15(c) (see Item 44)

Item 51 subparagraph 7.2(4)(e)(i) and paragraphs 7.2(5)(a) and 7.2(5)(b)

This item substitutes references to “accredited persons” with ‘”accredited data recipient” and is intended to clarify that certain rules relating to privacy safeguard 1 and the CDR Policy apply to accredited data recipients specifically.

Item 52: Rule 7.4

This item simplifies how rule 7.4 refers to collection consents.

Item 53: Paragraph 7.4(c)

This item substitutes the words “the CDR participant for the CDR data from which the CDR data was collected” in place of the words “the data holder of the CDR data” at rule 7.4(c) to reflect that CDR data may be collected not only from a data holder but also from an accredited person

Item 54: Paragraphs 7.5(1)(a), (b) and (c)

This item amends subrule 7.5(1) concerning permitted uses or disclosures (that do not relate to direct marketing) to recognise the distinction between collection consents, use consents and disclosure consents.

It also inserts two new permitted uses and disclosures. The first, paragraph 7.5(1)(aa), permits an accredited data recipient to de-identify a CDR consumer’s CDR data in accordance with the CDR data de-identification process and then use the de-identified data for general research or disclose (including by selling) the de-identified data. This must be done in accordance with a current use consent. The second, new paragraph 7.5(1)(ca), permits, subject to rule 7.5A, disclosure of the CDR consumer’s CDR data in accordance with a current disclosure consent.

Item 55: new subrule 7.5(1)(g)

This item inserts a new permitted use or disclosure to include disclosing CDR data to an accredited person, if the CDR consumer has given the accredited person a use consent and a collection consent to collect the CDR data from an accredited data recipient, and the CDR

consumer has given the accredited data recipient an AP disclosure consent to disclose the CDR data to the accredited person.

Item 56 and 57: new subparagraphs 7.5(3)(a)(iv) and 7.5(3)(aa)

Items 56 and 57 inserts a new permitted use and disclosure that relates to direct marketing. An accredited data recipient can, in accordance with a direct marketing consent, send information to a CDR consumer about other goods or services provided by another accredited person, if the accredited data recipient reasonably believes that the CDR consumer might benefit from those other goods or services and sends such information to the CDR consumer on no more than a reasonable number of occasions.

Then, and in accordance with a direct marketing consent, the accredited data recipient can disclose CDR data to the accredited person to enable the accredited person to provide the goods or services if the CDR consumer has given the accredited person a collection consent to collect the CDR data from the accredited data recipient and a use consent, and has given the accredited data recipient a disclosure consent to disclose the CDR data to the accredited person.

Items 58 and 59: Paragraphs 7.5(3)(b) and (c)

These items insert into the respective subparagraphs, reference to paragraph 7.5(3)(aa), which is introduced by the amendment in item 57.

Item 60: repeal of subrule 7.5(4)

This item repeals subrule 7.5(4), as the meaning of 'direct marketing consent' is introduced as a defined term (see Items 10 and 14).

Item 61: new rule 7.5A

The rule provides that a disclosure of CDR data to an accredited person under a disclosure consent is not a permitted use or disclosure until the earlier of 1 July 2021 or the day the Data Standards Chair makes consumer experience data standards for disclosure of CDR data accredited persons (which is referred to in a new paragraph inserted into subrule 8.11(1) by item 68).

Items 62 to 64: Rule 7.9

Item 64 inserts a new subrule 7.9(2) which requires that an accredited data recipient that discloses CDR data to an accredited person must, as soon as practicable after such disclosure, update each consumer dashboard that relates to the request to indicate what CDR data was disclosed, when the CDR data was disclosed, and the name of the accredited person to whom the CDR data was disclosed. An accredited person must be identified in accordance with any entry in the Register of Accredited Persons specified as being for that purpose.

Item 62 amends rule 7.9 to insert (1) before "For" to create subrule 7.9(1) and item 63 amends paragraph 7.9(1)(c) to recognise that the accredited data recipient must be identified in accordance with any entry on the Register of Accredited Persons specified as being for that purpose.

Items 65 to 67: Subrule 7.10(1) and note 2

These items amend the subrule and following note by replacing references to a data holder with references to a CDR participant. This recognises that accredited data recipients may disclose CDR data and, accordingly, have responsibilities under privacy safeguard 10 in the

Competition and Consumer Act to ensure the quality of CDR data. They must also take the steps set out in subrule 7.10(1) if the CDR participant becomes aware that the CDR data disclosed was incorrect. There is also an amendment to note 2 to include a reference to rule 1.14.

Item 68: new subparagraph 8.11(1)(c)(iii)

This item inserts 8.11(1)(c)(iii), which provides that the Data Standards Chair must make one or more data standards about the disclosure and security of CDR data, including consumer experience data standards for disclosure of CDR data to accredited persons.

Item 69: Subrules 9.3(1) and (2)

This item amends these subrules concerning records to be kept and maintained by a data holder and by an accredited data recipient.

For data holders, the amendments extend their existing record keeping obligations to also keep and maintain records that record and explain:

- amendments to authorisations to disclose CDR data;
- any written agreements they have entered into with another data holder relating to the disclosure of product data; and
- the processes by which they ask CDR consumers for their authorisation to disclose CDR data and for an amendment to their authorisation (including a video of each process).

The amendment to paragraph 9.3(1)(e) seeks to clarify a data holder's existing obligation to keep and maintain records of instances in which it refused to disclose CDR data by aligning the language in this subrule to the relevant rules which allow for refusal.

The addition of paragraph 9.3(1)(g) is intended to mirror the record keeping requirement accredited data recipients have under rule 9.3(2)(h). The effect of this amendment is that data holders must keep a record, including in a video form, of the processes it uses in seeking an authorisation and in seeking an amendment to an authorisation from a CDR consumer. Data holders are not required to keep a video of every individual consumer data authorisation or amendment process in which it is engaged. Rather, data holders must keep a record of its current and historic approaches to seeking authorisations and amendments to authorisations from CDR consumers.

For accredited data recipients, the amendments extend their existing record keeping obligations to also keep and maintain records that record and explain:

- amendments to consents by CDR consumers;
- disclosures of CDR data to accredited persons under the rules and the accredited persons to which any CDR data was disclosed;
- the processes by which the accredited data recipient asks CDR consumers for an amendment to their consent (including a video of that process).

Subrule 9.3(2) is updated to reflect the rule amendments introducing the concept of different types of consents.

Item 70: paragraph 9.4(1)(d)

This item repeals and substitutes a new paragraph 9.4(1)(d), which sets out the information to be included in data holder reports about refusals to disclose CDR data. The amendment clarifies that a data holder is to report for: product data requests; consumer data requests

made by an eligible CDR consumer; and consumer data requests made by an accredited person on behalf of a CDR consumer, the number of times the data holder has refused to disclose CDR data, the rule or data standard relied upon to refuse to disclose that data and the number of times the data holder has relied on each of those rules or data standards as a ground of refusal.

Item 71: Paragraph 9.4(2)(f) and (g)

This item amends accredited data recipients' reporting requirements. The new paragraph 9.4(2)(f) extends what an accredited data recipient must include in their bi-annual reports. The amendment requires accredited data recipients to report on the:

- number of consumer data requests the accredited data recipient received from an accredited person on behalf of a CDR consumer during the reporting period;
- number of times the accredited data recipient disclosed CDR data to an accredited person in response to such a request during the reporting period; and
- total number of CDR consumers the accredited data recipient provided goods or services to using CDR data during the reporting period.

Item 72: Subrule 9.5(1)

This item amends subrule 9.5(1) to allow a CDR consumer to request from a data holder copies of records relating to withdrawals of authorisations to disclose CDR data that relates to the CDR consumer.

Item 73: Subrule 9.5(2)

This items amends subrule 9.5(2) to expand the categories of records that a CDR consumer can request and access from an accredited data recipient that relate to them as a CDR consumer.

Item 74: Subrule 9.7(3)

This items amends subrule 9.7(3) to correct a typographical error.

Item 75 and 76: Amendments of listed provisions – repeals

This items amends rule 9.8 to repeal references to those subrules that have been repealed, and to insert references to new and amended subrules.

Item 77: Rule 9.8 (note)

This item inserts a reference to subrule 5.34(4) in the note which lists additional civil penalty provisions within the meaning of the Regulatory Powers Act (refer to item 49 which inserts the new rule 5.34).

Items 78 to 82: clause 2.1(1) of Schedule 1

These items make amendments to Schedule 1 to allow the Data Recipient Accreditor more flexibility to accept assurance reports submitted by a person for the purposes of the ongoing default conditions of accreditation relating to information security reporting.

The Data Recipient Accreditor can accept an assurance report:

- made in accordance ASAE 3150;[4] or
- made in accordance with an approved standard, report or framework, where that standard, report or framework has been approved by the Data Recipient Accreditor in guidelines issued by the Data Recipient Accreditor.

The amendments reflect the flexibility for accepting assurance reports as outlined in the current guidelines for accreditation issued by the ACCC.

The items also amends the rules to provide more flexibility for reporting periods to recognise a reporting period being either a financial year or a calendar year. The Data Recipient Accreditor will determine the relevant reporting period for the accredited person.

Item 83: Clause 1.2 of Schedule 3 (definition of joint account*)*

This item inserts a new definition for joint account. Joint account means a joint account with a data holder for which there are two or more joint account holders, each of which is an individual who, so far as the data holder is aware, is acting in their own capacity and not on behalf of another person, and is not a partnership account.

This amendment expands the scope of joint accounts to include joint accounts with more than two joint account holders and clarifies that it does not include partnership accounts.

Item 84: Clause 1.2 of Schedule 3 (definition of joint account management service)

This item replaces the reference to "subclause 4.2(3)" with a reference to "subclause 4.6(2)". (see item 92).

Items 85: Clause 1.2 of Schedule 3 (definition of voluntarily participating ADI)

The item repeals the definition of "voluntarily participating ADI" as it is no longer a term used in the Schedule.

Item 86: Subclause 2.1(2) of Schedule 3

This item amends the meaning of 'eligible' in relation to the banking sector. The amendment extends the definition of who can be considered to be an eligible CDR consumer to include: a person who is not an individual, a secondary user for an account, and a partner in a partnership for which there is a partnership account with a data holder.

Item 87: new clause 2.2 of Schedule 3

This item adds a new clause 2.2 which defines "account privileges'" for the banking sector. A person has account privileges in relation to an account with a data holder if the account is for a phase 1, a phase 2 or a phase 3 product; and the person is able to make transactions on the account. "Account privileges" are an element of the definition of a secondary user and are referred to at 1.13(e) (see item 16).

Item 88: Subparagraph 3.2(1)(b)(ii) of Schedule 3

This item amends the meaning of 'required consumer data' in relation to the banking sector. The amendment extends the type of account data that is to be considered 'required

[4] ASAE 3150 is a standard entitled 'Assurance Engagements on Controls' and published by the Auditing and Assurance Standards Board. It could, in 2020, be downloaded from the Auditing and Assurance Standards Board's website (https://www.auasb.gov.au/admin/file/content102/c3/Jan15_ASAE_3150_Assurance_Engagements_on_Controls.pdf).

consumer data' to include account data relating to: an account held by a CDR consumer in their name alone, a joint account, or a partnership account.

Items 89 to 90: Subclause 3.2(1) of Schedule 3 (note 1) and (note 3)

Item 89 clarifies that Subclause 3.2(1) of Schedule 3 (note 1), refers to sub-subparagraph (b)(ii)(B).

Item 90 clarifies that the operation of closed accounts is subject to subclauses (4) and (5).

Item 91: Subclauses 3.2(3) and (4) of Schedule 3

This item amends subclauses 3.2(3) and (4) and inserts a new subclause (5).

The amendments to subclause 3 provide clarity on what is *required consumer data* or *voluntary consumer data* in relation to partnership accounts and secondary users.

The provisions of former subclause 4, which dealt with both open and closed accounts, are now separated into subclauses 4 and 5 which deal with open and closed accounts respectively. Additionally, for an account that has been closed for more than 24 months before a particular time, the following CDR data is not required consumer data at that time:

- account data that relates to the account;
- transaction data that relates to any transaction on the account; and
- product specific data in relation to a product relating to any such account.

Item 92: Part 4 of Schedule 3

Division 4.1

This amendment specifies that Part 4 applies in relation to requests for disclosure of CDR data relating to one or more joint accounts held by eligible joint account holders within the banking sector.

This amendment also inserts a simplified outline of Part 4. It sets out that CDR data relating to joint accounts can only be disclosed if a disclosure option applies to the account and that all joint account holders must indicate the same disclosure option in order for a disclosure option to apply. It also outlines the process for accredited persons making consumer data requests in relation to joint accounts and such requests made on behalf of secondary users of joint accounts.

Clause 4.4 of Division 4.2

This clause contains a simplified outline of Division 4.2. It outlines the disclosure options that can apply to joint accounts and provides an overview of the pre and co-approval options. It also outlines the data holder obligations to offer pre-approval options and a joint account management service.

Clause 4.5 of Division 4.2

This clause outlines the disclosure options applicable to joint accounts. A pre-approval option requires that all joint account holders have indicated they want that disclosure option to apply. If a pre-approval option applies, CDR data on the joint account can be disclosed without additional input from the other account holders.

A co-approval option requires all joint account holders to indicate they want that disclosure option to apply, and consequently CDR data relating to that joint account can only be

disclosed to an accredited person with the approval of all account holders. However, if a co-approval option is in place and a joint account holder amends an authorisation, re-approval from all relevant account holders is not required. Instead, data holders must provide notifications to all relevant account holders as per clause 4.16(1)(c).

A disclosure option is not in place if an account holder has indicated that they no longer want the disclosure option to apply.

Clause 4.6 of Division 4.2

This clause amends and replaces former clause 4.2 of division 4.1 relating to the joint account management service. Data holders must provide a joint account management service that allows joint account holders to indicate, change or withdraw disclosure options. A joint account management service must allow joint account holders to indicate whether they would like a pre-approval option to apply and may also allow joint account holders to indicate whether they would like a co-approval option to apply.

The joint account management service must be provided online, and may be provided as part of the data holder's consumer dashboard for a joint account holder. Data holders may also provide an offline joint account management service in addition to an online service.

This clause also outlines that the joint account management service, when allowing a joint account holder to indicate a disclosure option, must not:

- add any requirements to the process beyond those specified in the data standards and rules;
- offer additional or alternative services as part of the process;
- include or refer to other documents, or provide any other information, so as to reduce comprehensibility; or
- offer pre-selected options.

This amendment also provides that when a joint account holder is indicating a disclosure option the joint account management service must notify them of the information outlined in subclause 4.6(7). As part of outlining the effect of the disclosure option applying, data holders should provide information to joint account holders about how on-disclosures of CDR data will operate. The joint account management service must also accord with the data standards (if any).

Clause 4.7 of Division 4.2

This clause outlines the requirements on a data holder when a joint account holder indicates a disclosure option, or no disclosure option, via the joint account management service.

Subdivision 4.3.1 of Division 4.3

Clause 4.8 sets out that Division 4.3 deals with consumer data requests for disclosure of account data, transaction data and product specific data relating to joint accounts. Clause 4.9 defines the terms requester, relevant account holders and joint account data.

Clause 4.10 of Division 4.3

This clause provides that if a joint account holder requests that CDR data be disclosed from a joint account and no disclosure option exists, the data holder must ask the requesting joint account holder to indicate a disclosure option (this is commonly called an 'in-flow election').

Clause 4.11 of Division 4.3

This clause outlines that if a co-approval option applies to a joint account and a joint account holder requests CDR data be disclosed, the data holder must contact the other relevant account holders to, amongst other things, ask the relevant account holders whether they approve of the relevant joint account data being disclosed.

Clause 4.12 of Division 4.3

This clause provides that any relevant joint account holder may remove an approval at any time. It also outlines that if each relevant account holder approves the disclosure in accordance with Division 4.3, the approval is applicable while the authorisation is current unless the approval is removed sooner.

Clause 4.13 of Division 4.3

This clause provides that data holders must not disclose joint account data unless:

- the requester has authorised the data holder to disclose that CDR data under Division 4.4; and
- one of the following applies:
    - a pre-approval disclosure option is in place; or
    - a co-approval disclosure option is in place, and:
        - each relevant account holder has approved the disclosure, or
        - the data holder considers it necessary to avoid seeking the approval of the relevant account holder in order to prevent physical or financial harm or abuse; or
    - no disclosure option is in place, but the data holder considers it necessary to avoid inviting the relevant account holder(s) to choose a disclosure option in order to prevent physical or financial harm or abuse.

Clause 4.14 of Division 4.3

This clause provides that if a disclosure option applies to a joint account, or has previously applied to a joint account, the data holder must provide functionality that allows relevant account holders to have oversight of CDR data sharing and manage approvals to disclose CDR data (where relevant) as part of the data holder's consumer dashboard for the relevant account holder. However, subclause 4.14(4) provides that the data holder may not provide a relevant account holder with a consumer dashboard or update the consumer dashboard if the data holder considers it necessary to do either in order to prevent physical or financial harm or abuse.

Clause 4.15 of Division 4.3

This clause provides that if one account holder's dashboard contains details of approvals under clause 4.14 these details must also be reflected in the dashboards of other joint account holders. This clause does not override the data holder's ability to not update the consumer dashboard in the circumstances outlined in subclause 4.14(4).

Clause 4.16 of Division 4.3

This clause outlines notification requirements for joint accounts. Notifications must be through a data holder's ordinary means for contacting the account holder. This could include, for example, in writing via email, text message, or internet banking notifications.

If a requester gives, amends or withdraws an authorisation, or an authorisation expires in relation to a joint account, the data holder must notify each relevant account holder as soon as practicable of the new authorisation, amended authorisation, or withdrawn or expired authorisation (as relevant).

If the requester is a secondary user and no disclosure option applies, the data holder must ask the relevant account holders to indicate a disclosure option they would like to apply to the account.

If a co-approval option applies to the account, and an amendment to an authorisation is made, the data holder must also notify the relevant account holders of the nature of the amendment and how they may remove an approval to prevent further data relating to the joint account from being disclosed.

If a relevant account holder gives or removes an approval, or does not provide an approval within the specified time frame, the data holder must notify the requester and any other relevant account holder of the relevant fact. This clause requires notification to a secondary user where the secondary user is the requester only.

A data holder is not required to give a notification to a particular account holder if the data holder considers it necessary not to do so in order to prevent physical or financial harm or abuse.

Item 93: Clause 6.1 of Schedule 3

The terms “brand request” and ‘non-brand request’ for initial data holders are repealed. .

Instead, the commencement table at clause 6.6 of Schedule 3 (see the ‘Data holder’ column) clarifies when primary brands and non-primary brands come into scope for the initial data holders: NAB, CBA, ANZ and Westpac.

The Phase 3 product definition is also removed to simplify the drafting of the commencement table, which now refers to ‘all product phases’ when Phase 3 products are brought in scope, rather than ‘Phase 1, Phase 2, Phase 3’.

Items 94 to 98: Clauses 6.2 and 6.3 of Schedule 3

Item 98 repeals former clause 6.3 of Schedule 2 that created a “voluntarily participating ADI” category of data holder. Early data sharing by a data holder is facilitated under clause 6.5 of Schedule 3 (see item 101).

In light of repealing this clause, several consequential changes remove references to the term ‘voluntarily participating ADI’ (items 94 – 97 above).

Items 99 and 100: Paragraph 6.4(1) of Schedule 3

Item 99 clarifies that if a product data or consumer data request is made to a data holder of the kind referred to in column 1 of the commencement table, the data holder may have data sharing obligations at the time. Item 100 is a consequential amend to Item 102, which inserts an updated version of the commencement table in the rules.

Item 101: Clause 6.5 of Schedule 3

New clause 6.5 replaces the former clause 6.5 and similarly provides that a data holder that has or will have data sharing obligations under the CDR regime is permitted to respond to requests ahead of when the commencement schedule requires the data holder to respond to certain requests for data. For example, an accredited ADI is required to start sharing data from phase 1 products from 1 March 2021. Under clause 6.5, an accredited ADI could

respond to requests in respect of phase 1, 2 and 3 products prior to 1 March 2021, should it choose to provide this capability early. If it chooses to disclose, it must do so in accordance with the relevant rule requirements.

Item 102: Clause 6.6 of Schedule 3

Clause 6.6 inserts an updated version of the commencement table in the rules. The amended table reflects existing exemptions made by the ACCC which exempt some data holders from particular obligations. The commencement table sets out when certain kinds of data holders are required to share certain CDR data. As above at item 101, these data holders are also permitted to start sharing CDR data earlier than is required by the table, should they wish.

The amended commencement table applies a 12 month delay between the obligations that apply to the initial data holders and the default obligations that apply to other ADIs. It also includes a delay to the commencement of consumer data sharing for reciprocal data holders and accredited ADIs. However, the timetable remains the same if an ADI becomes accredited: its consumer data sharing obligations commence earlier (1 March 2021) than would otherwise apply under the 'default' timeline for non-major ADIs (1 July 2021).

Item 103: new Clause 6.7 of Schedule 3

New clause 6.7 provides that initial data holders must bring CDR consumers that are not individuals or that are partnerships, nominated representatives, or secondary users, in scope from 1 November 2021 in respect of their primary brands, and remaining data holders must do this from 1 November 2022.

Item 104: Repeal of paragraph 7.2(3)(a) of Schedule 3

This item repeals clause 7.2(3)(a) of Schedule 3. Clause 7.2(3)(a) provided that where a person becomes a data holder rather than an accredited data recipient of CDR data as a result of subsection 56AJ(4) of the Act and clause 7.2 of the rules, any consents to collect CDR data under the consumer data request expire. While the clause has been repealed, the provision has instead been included under the duration of consent rules (see rule 4.14(1C)) along with the other rules around expiry of consent. Rule 4.14 then becomes a complete list of instances where consent may expire.

Item 105: Transitional provisions

Items 105(1), (2) and (3) of the Amending Instrument provide that existing consents, authorisations and de-identification elections continue in effect after the Amendment Rules come into force. These terms are defined in Item 105(7).

In relation to rules about data sharing from joint accounts under Part 4 of Schedule 3, item 105(4) is a transitional provision about compliance for:

- initial data holders;
- and any data holder that is a reciprocal data holder due to being an accredited person,

that are required to enable data sharing from joint accounts before 1 November 2021.[5]

These data holders, are taken to comply with Part 4 of Schedule 3 as set out in the Amending Instrument (i.e. they are taken to be complying with the 'new' joint account rules),

[5] This transitional provision does not apply to a data holder that chooses to disclose pre-application CDR data relating to a joint account, in accordance with Clause 6.5 of Schedule 3. Such a data holder would be required to disclose that data in accordance with the joint account rules set out in the Amending Instrument.

if they comply with the former Part 4 of Schedule 3, as set out in rules before the Amendment Rules come into force (i.e. the 'old' joint account rules.)

For these purposes, Item 105(4) provides that the former Part 4 of Schedule 3 is 'varied to the extent reasonably necessary so that it operates in accordance with these rules as amended' by the Amending Instrument. The effect of this provision is that former Part 4 of Schedule 3 will continue to apply to these particular data holders, with appropriate modification where that is necessary to allow for former Part 4's concurrent operation with the rest of the Amendment Rules after they come into force.

This transitional provision has effect until 31 October 2021, meaning these data holders must comply with the 'new' joint account rules on and from 1 November 2021.

Finally, items 105(5) and (6) provide that any joint election made under the former Part 4 of Schedule 3 is taken as an indication that the joint account holders would like the pre-approval option (as defined in the Amendment Rules) to apply to their account from 1 November 2021.