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

Dated

CDR Amendments Exposure Draft

Jane Hume [DRAFT ONLY: NOT FOR SIGNATURE]
Minister for Superannuation, Financial Services and the Digital Economy

……..

Contents

1 Name

This instrument is the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020*.

2 Commencement

(1) Each provision of this instrument specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information

Column 1	Column 2	Column 3
Provisions	**Commencement**	**Date/Details**
1. Sections 1 to 4	The day after this instrument is registered	
2. Schedule 1, etc	[tba]	

Note: This table relates only to the provisions of this instrument as originally made. It will not be amended to deal with any later amendments of this instrument.

(2) Any information in column 3 of the table is not part of this instrument. Information may be inserted in this column, or information in it may be edited, in any published version of this instrument.

3 Authority

This instrument is made under section 56BA of the *Competition and Consumer Act 2010*.

4 Schedules

Each instrument that is specified in a Schedule to this instrument is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this instrument has effect according to its terms.

Schedule 1—Amendments relating to sponsored accreditation

Competition and Consumer (Consumer Data Right) Rules 2020

1 Subrule 1.6 (11)

Omit "persons accredited at the "unrestricted" level", substitute "accredited persons".

2 Subrule 1.7 (1)

Insert in the appropriate alphabetical position:

affiliate has the meaning given by by rule 1.10D.

3 Subrule 1.7 (1)

Insert in the appropriate alphabetical position:

level, in relation to accreditation, has the meaning given by rule 5.1A.

sponsor has the meaning given by rule 1.10D.

sponsored accreditation means accreditation at the sponsored level mentioned in rule 5.1A.

Note: See also rules 1.10D and 5.1B.

sponsorship arrangement has the meaning given by rule 1.10D.

unrestricted accreditation means accreditation at the unrestricted level mentioned in rule 5.1A.

4 Before the heading to Division 1.4, in Division 1.3

Insert:

1.10D Meaning of *sponsorship arrangement*, *sponsor* and *affiliate*

(1) A ***sponsorship arrangement*** is a written contract between a person with unrestricted accreditation (the ***sponsor***) and another person (the ***affiliate***), under which:

(a) the sponsor agrees to disclose to the affiliate, in response to a consumer data request made by the affiliate in accordance with rule 5.1B(2), CDR data that it holds as an accredited data recipient; and

(b) the affiliate undertakes to provide the sponsor with such information and access to its operations as is needed for the sponsor to fulfil its obligations as a sponsor.

Note: A person does not need to have sponsored accreditation to enter into a sponsorship arrangement as an affiliate, but will need it to make the consumer data requests mentioned in paragraph (a)

(2) A sponsorship arrangement may also provide for the sponsor to:

(a) make consumer data requests at the request of the affiliate; or
(b) use or disclose CDR data at the request of the affiliate.

5 After paragraph 1.14(3)(h)

Insert:

(ha) if the accredited person is an affiliate and the CDR data will be collected by a sponsor at its request;
(i) the sponsor's name; and
(ii) the sponsor's accreditation number;

6 After subrule 4.3(2)

Insert:

(2A) If the accredited person is an affiliate and the CDR data will be collected by a sponsor at its request:
(a) the request for a collection consent must specify that fact; and
(b) a consent for the affiliate to collect the CDR data is taken to be consent for the sponsor to so collect it.

7 After paragraph 4.11(3)(h)

Insert:

(i) if the accredited person is an affiliate and the CDR data will be collected by a sponsor at its request;
(i) a statement of that fact; and
(ii) the sponsor's name; and
(iii) the sponsor's accreditation number; and
(iv) a link to the sponsor's CDR policy; and
(v) a statement that the CDR consumer can obtain further information about such collections or disclosures from the sponsor's CDR policy if desired.

8 Before subdivision 5.2.1

Insert:

Subdivision 5.2.1A—Levels of accreditation

5.1A Levels of accreditation

Accreditation may be at either of the following ***levels***:
(a) unrestricted;
(b) sponsored.

5.1B Sponsored accreditation

(1) A person with sponsored accreditation must not make a consumer data request under these rules unless it has a sponsorship arrangement with a sponsor.

Note: This subrule is a civil penalty provision (see rule 9.8).

(2) A person with sponsored accreditation must not make a consumer data request under these rules otherwise than:

(a) to an accredited data recipient under rule 4.7A; or

(b) through a sponsor acting at its request under a sponsorship arrangement.

Note: This subrule is a civil penalty provision (see rule 9.8).

(3) A person with sponsored accreditation must not engage a provider under an outsourced service arrangement to collect CDR data from a CDR participant on its behalf.

Note: This subrule is a civil penalty provision (see rule 9.8).

(4) A person with sponsored accreditation must not have a CDR representative.

Note: This subrule is a civil penalty provision (see rule 9.8).

(5) The accreditation of a person with sponsored accreditation lapses if the person does not have a sponsor for a period of 4 months.

9 Rule 5.2, note after heading

Repeal.

10 After paragraph 5.2(2)(a)

Insert:

(aa) indicate the level of accreditation that is sought; and

11 Rule 5.5, heading

Omit "—unrestricted level".

12 Rule 5.5, note after heading

Omit " This rule specifies those criteria for the "unrestricted" level of accreditation.".

13 Rule 5.5

Omit "at the "unrestricted" level".

14 Rule 5.12, heading

Omit "at the "unrestricted" level".

15 Subrule 5.12(1)

Omit "A person who is accredited at the "unrestricted" level", substitute "An accredited person".

16 Subrule 5.12(2)

Omit "A person who is accredited at the "unrestricted" level", substitute "An accredited person".

17 Subrule 5.12(1)

After "comparable guarantee," insert "appropriate to the level of accreditation,".

18 After paragraph 5.14(b)

Insert:

(ba) the person becomes a sponsor of an affiliate;

(bb) where the accredited person is a sponsor of an affiliate—the sponsorship arrangement is suspended, expires, or is terminated;

19 Subparagraph 5.15(a)(vi)

Note: This amendment relates partly to sponsored accreditation and partly to CDR representatives—see the corresponding amendment in Schedule 2. The final forms of the two amendments will be settled when the commencement order of the two Schedules is settled.

Substitute:

(vi) a notification under paragraph 5.14(ba), (bb) or (c), or subclause 2.3(3) of Schedule 1; and

20 Table in subrule 5.17(1)

Add at the end:

11	for a person with sponsored accreditation—the accreditation of one or more of the person's sponsors is suspended or revoked;	may, in writing: (a) suspend; or (b) revoke; the person's accreditation, as appropriate.

21 Paragraph 5.18(1)(a)

After "accredited person" insert "and any associate".

22 Paragraph 5.18(1)(b)

After "accredited person" insert "and any associate".

23 Subrule 5.18(2)

After "notify the person" insert "and any associate".

24 After subrule 5.18(2)

Insert:

(3) For this rule, each of the following is an ***associate*** of the accredited person:

(a) any sponsor;

(b) any affiliate.

25 After paragraph 5.24(b)

Insert:

(ba) for a person with sponsored accreditation—any sponsor;

(bb) for a sponsor—each affiliate;

26 Rule 5.24, Note 2

Repeal.

27 After paragraph 7.2(4)(a)

Insert:

(aa) include a list of the accredited persons with whom the accredited data recipient has a sponsorship arrangement; and

(ab) for each such arrangement—include the nature of the services one party provides to the other party; and

28 Rule 7.4

Add at the end, before the note:

; and

(d) if the accredited person is an affiliate and the CDR data was collected by a sponsor—that fact.

29 Paragraph 7.5(1)(d)

After "outsourcing arrangement" insert ", or to the other party in a sponsorship arrangement".

30 After rule 7.6(2)

Insert:

(3) For this rule any CDR data collected by an accredited person at the request of an affiliate is taken also to have been collected by the affiliate.

31 Subparagraph 9.3(2)(i)

After "providers" (each occurrence), insert "or sponsors".

32 Subparagraph 9.3(2)(ii)

After "providers", insert "or sponsors".

33 Rule 9.8

Note: References to inserted provisions noted as being subject to a civil penalty will be added here, and references to provisions being repealed will be removed.

Insert in appropriate alphanumeric position:

(xx) subrule xx;

… …….

34 Schedule 1, subclause 2.1(1), definitions of *assurance report* and *attestation statement*

Substitute:

assurance report means:

(a) for a person with unrestricted accreditation—a report that is made in accordance with:

(i) ASAE 3150; or

(ii) an approved standard, report or framework; and

Note: See the *CDR Accreditation Guidelines*, which could in 2020 be downloaded from the Commission's website (https://www.accc.gov.au).

ASAE 3150 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).

(b) for a person with sponsored accreditation—an assessement of its capacity to comply with Schedule 2 that is made in accordance with any approved requirements;

that does not include the information that must be provided in an attestation statement.

attestation statement means:

(a) for a person with unrestricted accreditation—a statement in the form of a responsible party's statement on controls and system description that is made in accordance with ASAE 3150; and

(b) for a person with sponsored accreditation—a statement about its compliance with Schedule 2 that is made in accordance with any approved requirements.

35 Schedule 1, After clause 2.1

Insert:

2.2 Conditions on sponsors and potential sponsors

(1) An accredited person that proposes to become the sponsor of a person that has, or proposes to apply for, sponsored accreditation must:

(a) undertake due diligence to ensure that the proposed affiliate is a suitable person for that role; and

(b) provide any appropriate assistance or training in technical and compliance matters.

(2) The sponsor of an affiliate must:

(a) continue to provide any appropriate assistance or training in technical and compliance matters; and

(b) take reasonable steps to ensure that the affiliate complies with its obligations as an accredited person.

36 Schedule 2, paragraph 1.5(1)(a)

After “complies with the”, insert “applicable”.

37 Schedule 2, table in clause 2.2

Subsitute:

	Control requirements		Minimum controls	Description of minimum controls
(1)	An accredited data recipient must have processes in place to limit the risk of inappropriate or unauthorised access to its CDR data environment.	(a)	Multi-factor authentication or equivalent control	Multi-factor authentication or equivalent control is required for all access to CDR data. Note: This minimum control does not apply to access to CDR data by CDR consumers.
		(b)	Restrict administrative privileges	Administrative privileges are granted only on an as needs basis for users to perform their duties and only for the period they are required for. Privileges granted on an ongoing basis are regularly reviewed to confirm their ongoing need.
		(c)	Audit logging and monitoring	Critical events are identified, logged and retained to help ensure traceability and accountability of actions. These logs are reviewed regularly to identify irregularities and deviations from expected processing. Note: In relation to retention, see paragraph 9.3(2)(l) of these rules.
		(d)	Access security	Processes, including automatic processes, are implemented to limit unauthorised access to the CDR data environment. At the minimum these include: (a) provision and timely revocation for users who no longer need access; and

	Control requirements		Minimum controls	Description of minimum controls
				(b) monitoring and review of the appropriateness of user access privileges on at least a quarterly basis.
		(e)	Limit physical access	Physical access to facilities where CDR data is stored, hosted or accessed (including server rooms, communications rooms, and premises of business operation) is restricted to authorised individuals.
		(f)	Role based access	Role-based access is implemented to limit user access rights to only that necessary for personnel to perform their assigned responsibilities. Role-based access is assigned in accordance with the principle of least necessary privileges and segregation of duties.
		(g)	Unique IDs	Use of generic, shared and/or default accounts is restricted to those necessary to run a service or a system. Where generic, shared and/or default accounts are used, actions performed using these accounts are monitored and logs are retained. Note: In relation to retention, see paragraph 9.3(2)(l) of these rules.
		(h)	Password authentication	Strong authentication mechanisms are enforced prior to allowing users to access systems within the CDR data environment, including, but not limited to, general security requirements relating to password complexity, account lockout, password history, and password ageing.
		(i)	Encryption in transit	Implement robust network security controls to help protect data in transit, including: encrypting data in transit and authenticating access to data in accordance with the data standards (if any) and industry best practice,

	Control requirements		Minimum controls	Description of minimum controls
				implementing processes to audit data access and use, and implementing processes to verify the identity of communications.
(2)	An accredited data recipient of CDR data must take steps to secure their network and systems within the CDR data environment.	(a)	Encryption	Encryption methods are utilised to secure CDR data at rest by encrypting file systems, end-user devices, portable storage media and backup media. Cryptographic keys are securely stored, backed-up and retained. Appropriate user authentication controls (consistent with control requirement 1) are in place for access to encryption solutions and cryptographic keys.
		(b)	Firewalls	Firewalls are used to limit traffic from untrusted sources. This could be achieved by implementing a combination of strategies including, but not limited to: (a) restricting all access from untrusted networks; and (b) denying all traffic aside from necessary protocols; and (c) restricting access to configuring firewalls, and review configurations on a regular basis.
		(c)	Server hardening	Processes are in place to harden servers running applications, databases and operating systems in accordance with accepted industry standards.
		(d)	End-user devices	End-user devices, including bring-your-own-device (BYOD) systems, are hardened in accordance with accepted industry standards.
		(e)	Data Segregation	CDR data that is stored or hosted on behalf of an accredited data recipient or CDR representative is segregated from other CDR data to ensure it is

	Control requirements		Minimum controls	Description of minimum controls
				accessible only by the accredited data recipient for whom consent was given and remains directly attributable to that accredited data recipient.
(3)	An accredited data recipient must securely manage information assets within the CDR data environment over their lifecycle.	(a)	Data loss prevention	Data loss and leakage prevention mechanisms are implemented to prevent data leaving the CDR data environment, including, but not limited to: (a) blocking access to unapproved cloud computing services; and (b) logging and monitoring the recipient, file size and frequency of outbound emails; and (c) email filtering and blocking methods that block emails with CDR data in text and attachments; and (d) blocking data write access to portable storage media.
		(b)	CDR data in non-production environments	CDR data is secured from unauthorised access by masking data, prior to being made available in non-production environments.
		(c)	Information asset lifecycle (as it relates to CDR data)	The accredited data recipient must document and implement processes that relate to the management of CDR data over its lifecycle, including an information classification and handling policy (which must address the confidentiality and sensitivity of CDR data) and processes relating to CDR data backup, retention, and, in accordance with rules 7.12 and 7.13, deletion and de-identification.
(4)	An accredited data recipient must implement a formal vulnerability	(a)	Security patching	A formal program is implemented for identifying, assessing the risk of and applying security patches to applications and operating as soon as practicable.

	Control requirements		Minimum controls	Description of minimum controls
	management program to identify, track and remediate vulnerabilities within the CDR data environment in a timely manner.	(b)	Secure coding	Changes to the accredited data recipient's systems (including its CDR data environment) are designed and developed consistent with industry accepted secure coding practices, and are appropriately tested prior to release into the production environment.
		(c)	Vulnerability management	A formal vulnerability management program is designed and implemented, which includes regular vulnerability scanning and penetration testing on systems within the CDR data environment.
(5)	An accredited data recipient must take steps to limit prevent, detect and remove malware in regards to their CDR data environment.	(a)	Anti-malware anti-virus	Anti-virus and anti-malware solutions are implemented on endpoint devices and on servers to detect and remove malware from the CDR data environment and are updated on a regular basis. End-user systems are updated with the latest virus definitions when they connect to the network. Reports or dashboards highlighting compliance metrics are regularly generated and monitored, and non-compliant items are actioned as soon as practicable.
		(b)	Web and email content filtering	Solutions are implemented to identify, quarantine and block suspicious content arising from email and the web.
		(c)	Application whitelisting	Download of executables and installation of software on infrastructure and end-user devices (including on BYOD devices) is restricted to authorised software only.
(6)	An accredited data recipient must implement a formal	(a)	Security training and awareness	All users undergo mandatory security and privacy training prior to interacting with the CDR data environment, with 'refresher courses' provided at least annually.

	Control requirements		Minimum controls	Description of minimum controls
	information security training and awareness program for all personnel interacting with CDR data.			
		(b)	Acceptable use of technology	A policy relating to the CDR data environment is created, implemented, communicated and agreed to by all personnel prior to being able to access the CDR data environment. This policy sets out the responsibilities of these personnel in interacting with the CDR data environment and is regularly made aware to personnel.
		(c)	Human resource security	Background checks are performed on all personnel prior to being able to access the CDR data environment. These may include, but are not limited to, reference checks and police checks.
(7)	A sponsor must implement a third party management framework	(a)	Implementation and maintenance of a third-party management framework	Affiliates must be managed by the sponsor in line with a defined third-party management framework, which should include requirements and activities relating to: • due diligence prior to establishing new relationships or contracts; • contractual agreements reflective of responsibilities for the CDR data and data environment; • annual review and assurance activities; • reporting requirements; • post-contract requirements.

Schedule 2—Amendments relating to CDR representatives

Competition and Consumer (Consumer Data Right) Rules 2020

1 Subrule 1.7 (1)

Insert in the appropriate alphabetical position:

CDR representative has the meaning given by rule 1.10AA.

CDR representative arrangement has the meaning given by rule 1.10AA.

CDR principal has the meaning given by rule 1.10AA.

2 Subrule 1.7 (1), definition of "service data"

Substitute:

service data:

(a) in relation to a CDR outsourcing arrangement—has the meaning given by rule 1.10; and

(b) in relation to a CDR representative arrangement— has the meaning given by rule 1.10AA.

3 Paragraph 1.10(2)(a)

Substitute:

(a) the provider will do one or both of the following:

(i) collect CDR data from a CDR participant in accordance with these rules on behalf of the principal;

(ii) provide goods or services to the principal using CDR data that it has collected on behalf of the the principal or that has been disclosed to it by the principal; and

4 Subparagraph 1.10(2)(b)(iv)

Repeal.

5 After rule 1.10

Insert:

1.10AA Meaning of *CDR representative* and related terms

Note: From the point of view of a CDR consumer who is the customer of a CDR representative, the consumer deals only with the CDR representative, as if it were an accredited person. The consumer requests the goods or services from the CDR representative; the CDR representative identifies the CDR data that it needs in order to provide the goods and services; the consumer gives their consent to the CDR

representative for the collection and use of the CDR data. The consumer is informed that the CDR principal will do the actual collecting, but as a background detail.

(1) For these rules, where two persons are the principal and the representative in a CDR representative arrangement, the representative is a ***CDR representative*** of the principal.

(2) For these rules, a ***CDR representative arrangement*** is a written contract between a person with unrestricted accreditation (the ***principal***) and a person without accreditation (the ***representative***) under which:

(a) where the representative has obtained the consent of a CDR consumer to the collection and use of CDR data in accordance with rule 4.3A:

(i) the principal will:

(A) make any appropriate consumer data request; and

(B) disclose the relevant CDR data to the representative; and

(ii) the representative will use the CDR data to provide the relevant goods or services to the CDR consumer; and

(b) the representative must not enter into another CDR representative arrangement;

(c) the representative is required to comply with the following requirements in relation to any service data:

(i) in holding, using or disclosing the service data, the representative must comply with:

(A) section 52EE of the Act (privacy safeguard 2);

(b) section 52EG of the Act (privacy safeguard 4);

(C) subsection 56EN(2) of the Act (privacy safeguard 11);

(D) section 56EO of the Act (privacy safeguard 12); and

(E) subsection 56EP(2) of the Act (privacy safeguard 13);

as if it were the principal;

(ii) the representative must take the steps in Schedule 2 to protect the service data as if it were the principal; and

(iii) the representative must not use or disclose the service data other than in accordance with a contract with the principal;

(iv) the representative must, when so directed by the principal, do any of the following:

(A) delete any service data that it holds in accordance with the CDR data deletion process;

(B) provide, to the principal, records of any deletion that are required to be made under the CDR data deletion process;

(C) direct any outsourced service provider to which it has disclosed CDR data to take corresponding steps;

(d) the representative is required to adopt and comply with the principal's CDR policy in relation to the service data.

Note: See rule 1.18 for the definition of "CDR data deletion process".

(3) For these rules, the ***service data*** in relation to a CDR representative arrangement consists of any CDR data that:

(a) was disclosed to the CDR representative for the purposes of the arrangement; or
(b) directly or indirectly derives from such CDR data.

6 Rule 1.10A

Add at the end:

Consents in relation to CDR representatives

(4) For an accredited person with a CDR representative, a consent given by a CDR consumer under these rules to the CDR representative for the accredited person to collect particular CDR data from a CDR participant for that CDR data and disclose it to the CDR representative is also a ***collection consent***.

(5) In this rule, other than in relation to subparagraph (1)(c)(i), a reference to an accredited data recipient of particular CDR data includes a reference to a CDR representative that holds the CDR data as service data.

7 Subrule 1.14(1)

Omit "An accredited person", substitute "Subject to subrule (5), an accredited person".

8 After subrule 1.14(4)

Insert:

Dashboard in relation to CDR representative

(5) Where a CDR principal makes a consumer data request at the request of a CDR representative, it may arrange for the CDR representative to provide the consumer dashboard on its behalf.

9 After rule 1.16

Insert:

1.16A Obligations relating to CDR representative arrangements

(1) If an accredited person is the principal in a CDR representative arrangement, it must ensure that the CDR representative complies with its requirements under the arrangement.

Note: This rule is a civil penalty provision (see rule 9.8).

(2) The accredited person must keep and maintain records that cover and explain:
(a) each CDR representative arrangement;
(b) the use and management of data by each CDR representative; and
(c) steps taken to ensure that any CDR representatives comply with their requirements under the arrangements.

Note: This rule is a civil penalty provision (see rule 9.8).

10 Rule 4.1

After "must have first asked the accredited person", insert ", or a CDR representative of the accredited person,".

11 After rule 4.3

Insert:

4.3A Request for accredited person to seek to collect CDR data, made to CDR representative

(1) This rule applies if:

(a) a CDR consumer requests a CDR representative to provide goods or services to the CDR consumer or to another person; and

(b) the CDR representative needs to:

(i) request its CDR principal to collect the CDR consumer's CDR data from a CDR participant under these rules; and

(ii) use it in order to provide those goods or services.

(2) The CDR representative may, in accordance with Division 4.3, ask the CDR consumer to give:

(a) a collection consent for the CDR principal to collect their CDR data from the CDR participant; and

(b) a use consent for:

(i) the CDR principal to disclose that data to the CDR representative; and

(ii) for the CDR representative to use it in order to provide those goods or services.

Note 1: In order to provide goods or services in accordance with the CDR consumer's request, it might be necessary for the accredited person to request CDR data from more than 1 CDR participant.

Note 2: The CDR data may be collected and used only in accordance with the data minimisation principle: see rule 1.8.

(3) In giving the consents, the CDR consumer gives the CDR principal a ***valid*** request to seek to collect that CDR data from the CDR participant.

Note: If an accredited person seeks to collect CDR data under this Part without a valid request, it will contravene privacy safeguard 3 (a civil penalty provision under the Act): see section 56EF of the Act.

(4) The request ceases to be ***valid*** if the collection consent is withdrawn.

Note: So long as the use consent is not also withdrawn, the CDR principal could continue to disclose CDR data it had already collected to the CDR representative, and the CDR representative could use it in order to provide the requested goods or services. However, the notification requirement of rule 4.18A would apply.

4.3B Modifications of Division 4.3 in relation to CDR representative

The CDR principal must ensure that, when the CDR representative asks for the CDR consumer's consents, it does so in accordance with Division 4.3, applied with the following modifications:

(a) replace references to the accredited person with references to the CDR representative, except in Subdivision 4.3.5;

(b) in Subdivision 4.3.5, replace references to the accredited person with references to the CDR principal;

(c) replace references to the goods and services provided by the accredited person with references goods or services provided by the CDR representative;

(d) replace references to the consumer dashboard provided by the accredited person with references to the consumer dashboard provided by the principal;

(e) replace references to the accredited person's CDR policy with references to the CDR principal's CDR policy;

(f) replace references to an outsourced service provider of the accredited person with references to an outsourced service provider of the CDR principal or of the CDR representative;

(g) replace subrule 4.11(1A) with the following:

"(1A) A CDR representative must not ask a CDR consumer to give a disclosure consent for disclosure of CDR data by the CDR representative unless the consumer has already given the collection and use consents required for the data to be collected by the CDR principal and disclosed to and used by CDR representative.";

(h) omit paragraph 4.11(3)(b);

(i) replace paragraph 4.11(3)(i) with the following:

"(i) the fact that the person is a CDR representative and that the CDR data will be collected by its CDR principal at its request;

(j) if the CDR representative is not located in Australia—the country in which it is located;

(k) the principal's name; and

(l) the prinicpal's accreditation number; and

(m) a link to the principal's CDR policy; and

(n) a statement that the CDR consumer can obtain further information about such collections or disclosures from the principal's CDR policy if desired.";

(j) replace subrules 4.14(1C) and (2) with the following:

"(1C) If a CDR principal becomes a data holder, rather than an accredited data recipient, of particular CDR data as a result of subsection 56AJ(4) of the Act, all of the CDR representative's consents given under these rules that relate to that CDR data expire.

"(2) If a CDR principal's accreditation is revoked or surrendered in accordance with rule 5.17, all of the consents of any CDR representative expire when the revocation or surrender takes effect.";

(k) replace subrules 4.16(2) and (3) with the following:

"(2) The CDR consumer may make the election:

(a) by communicating it to the CDR principal or CDR representative in writing; or

(b) by using the CDR principal's consumer dashboard.

(3) This rule does not apply if, when seeking the consent, the CDR representative informs the CDR consumer that they and the CDR principal have a general policy of deleting CDR data when it becomes redundant data.";

(l) add the following rule to Subdivision 4.3.5:

"***4.20A Application of subdivision to CDR principal and CDR representative***

Where an accredited person who is a CDR principal is required under this subdivision to give a notice to a CDR consumer in relation to a consumer data request made at the request of a CDR representative, the notice may be given through the CDR representative.".

Note: This rule is a civil penalty provision (see rule 9.8).

12 Subparagraph 5.15(a)(vi)

Note: This amendment relates partly to sponsored accreditation and partly to CDR representatives—see the corresponding amendment in Schedule 1. The final forms of the two amendments will be settled when the commencement order of the two Schedules is settled.

Substitute:

(vi) a notification under paragraph 5.14(ba), (bb) or (c), or subclause 2.3(3) of Schedule 1; and

13 Before paragraph 5.24(c)

Insert:

(bc) the name, ABN and business address of any CDR representative;

14 Before paragraph 7.2(4)(b)

Insert:

(ac) include a list of the CDR representatives of the accredited data recipient; and

15 Subrule 7.2(8)

After "by means of which the CDR participant", insert ", or a CDR representative of the CDR participant,".

16 Rule 7.3

At the beginning, insert "(1)", at the end add:

(2) A CDR principal breaches this subrule if its CDR representative fails to comply with section 56EE of the Act in relation to service data of a CDR consumer as if it were an accredited person.

Note 1: See rule 1.10 for the definition of "service data" in relation to a CDR representative arrangement.

Note 2: This subrule is a civil penalty provision (see rule 9.8).

(3) For subrule (2), it is irrelevant whether the action of the CDR representative in relation to the service data is in accordance with the CDR representative arrangement.

7.3A Rule relating to privacy safeguard 4—destruction of unsolicited data—CDR representative

(1) A CDR principal breaches this subrule if its CDR representative fails to comply with section 56EG of the Act in relation to service data of a CDR consumer as if;

(a) it were an accredited person; and

(b) it had collected the service data.

Note 1: See rule 1.10 for the definition of "service data" in relation to a CDR representative arrangement.

Note 2: This subrule is a civil penalty provision (see rule 9.8).

(2) For subrule (2), it is irrelevant whether the action of the CDR representative in relation to the service data is in accordance with the CDR representative arrangement.

17 After paragraph 7.5(1)(g)

Insert:

(h) where the accredited person is a CDR principal—disclosing the CDR data to a CDR representative for the purposes of a use or disclosure by the the CDR representative that would be a permitted use or disclosure under paragraphs (a) to (g) if the CDR representative were an accredited person that had collected the CDR data under the consumer data request.

18 Subrule 7.6(2), note

Substitute:

Note: See rule 1.10 for the definition of "service data" in relation to a CDR outsourcing arrangement.

19 Rule 7.6

Add at the end:

(4) For this rule:

(a) any use or disclosure of service data by a CDR representative is taken to have been by the CDR principal; and

(b) it is irrelevant whether the use or disclosure is in accordance with the CDR representative arrangement.

Note: See rule 1.10 for the definition of "service data" in relation to a CDR representative arrangement.

20 Rule 7.9

At the end, add:

(5) For this rule, where an accredited data recipient is a CDR principal, a disclosure of service data by a CDR representative is taken to be a disclosure by the CDR principal.

21 After rule 7.10

Insert:

7.10A Rule relating to privacy safeguard 11—quality of data—CDR representative

(1) A CDR principal breaches this subrule if its CDR representative fails to comply with subsection 56EN(2) of the Act in relation to service data of a CDR consumer as if it were an accredited person.

Note 1: See rule 1.10 for the definition of "service data" in relation to a CDR representative arrangement.

Note 2: This subrule is a civil penalty provision (see rule 9.8).

(2) For subrule (2), it is irrelevant whether the action of the CDR representative in relation to the service data is in accordance with the CDR representative arrangement.

22 Rule 7.11

At the beginning, insert "(1)", at the end add:

(2) For this rule, where an accredited data recipient is a CDR principal, a failure by a CDR representative to comply with Schedule 2 in relation to service data is taken to be a failure by the CDR principal.

23 Rule 7.12

At the end add:

(3) For this rule, where an accredited data recipient is a CDR principal, a failure by a CDR representative to comply with subsection 56EO(2) of the Act in relation to service data as if it were a CDR entity is taken to be a failure by the CDR principal.

24 After rule 7.15

Insert:

7.15A Rule relating to privacy safeguard 13—correction of data—CDR representative

(1) A CDR principal breaches this subrule if its CDR representative fails to comply with subsection 56EP(2) of the Act in relation to service data of a CDR consumer as if it were an accredited person.

Note 1: See rule 1.10 for the definition of "service data" in relation to a CDR representative arrangement.

Note 2: This subrule is a civil penalty provision (see rule 9.8).

(2) For subrule (2), it is irrelevant whether the action of the CDR representative in relation to the service data is in accordance with the CDR representative arrangement.

25 Rule 9.8

Note: References to inserted provisions noted as being subject to a civil penalty will be added here, and references to provisions being repealed will be removed.

Insert in appropriate alphanumeric position:

(xx) subrule xx;

… …….

26 Schedule 1

At the end add:

2.3 Conditions in relation to CDR representatives

(1) This rule applies in relation to an accredited person that is, or proposes to become, the CDR principal in a CDR representative arrangement.

(2) Within 30 business days of entering into the arrangement, the person must notify the Data Recipient Accreditor that they have done so.

(3) The notification must include the following:

(a) the name, ABN and Australian business address of the CDR representative;

(b) the names and contact details of the directors or any persons responsible for the CDR representative;

(c) the nature of any goods and services to be provided by CDR representative using CDR data;

(e) any information specified in writing by the Data Recipient Accreditor for the purposes of this paragraph as being necessary for the purposes of evaluating the CDR representative.

Schedule 3—Amendments relating to trusted advisers and insights

Competition and Consumer (Consumer Data Right) Rules 2020

1 Subrule 1.7 (1)

Insert in the appropriate alphabetical position:

CDR insight, in relation to an insight disclosure consent, means the CDR data subject to the consent.

insight disclosure consent has the meaning given by rule 1.10A.

TA disclosure consent has the meaning given by rule 1.10A.

trusted adviser has the meaning given by rule 1.10B.

2 Paragraph 1.10A(1)(c)(ii)

Omit "; and", substitute:

; or

(iii) to a trusted adviser of the CDR consumer (a ***TA disclosure consent***); or

(iv) to a specified person in accordance with an insight disclosure consent; and

3 Subrule 1.10A(2)

Add at the end:

;

(f) TA disclosure consents;

(g) insight disclosure consents.

4 After subrule 1.10A(2)

Insert:

(3) For these rules, an ***insight disclosure consent*** is a consent given by a CDR consumer under these rules for an accredited data recipient of particular CDR data to disclose it to a specified person for one of the following purposes:

(a) identifying the consumer;

(b) verifying the consumer's account balance;

(c) verifying the consumer's income;

(d) verifying the consumer's expenses.

5 After rule 1.10A

Insert:

1.10C Trusted advisers

(1) An accredited person may invite a CDR consumer to nominate one or more persons as ***trusted advisers*** of the CDR consumer for the purposes of this rule.

(2) A trusted adviser must belong to one of the following classes:

(a) qualified accountants within the meaning of the *Corporations Act 2001*;

(b) 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;

(c) registered tax agents, BAS agents and tax (financial) advisers within the meaning of the *Tax Agent Services Act 2009*;

(d) financial counselling agencies within the meaning of the *ASIC Corporations (Financial Counselling Agencies) Instrument 2017/792*;

(e) relevant providers within the meaning of the *Corporations Act 2001* who would not contravene subsection 923C(1) or (2) of the *Corporations Act 2001* if they were to assume or use the expression "financial adviser" or "financial planner" in relation to a financial services busness or a financial service they carry on or provide;

(f) mortgage brokers within the meaning of the *National Consumer Credit Protection Act 2009*.

(3) The accredited person must not make:

(a) the nomination of a trusted adviser; or

(b) the nomination of a particular person as a trusted adviser; or

(c) the giving of a TA disclosure consent;

a condition for supply of the goods or services requested by the CDR consumer.

6 Paragraph 1.14(1)(b)

After "subrule (3)", insert "and the information specified in subrule (3A)".

7 After paragraph 1.14(3)(e)

Insert:

(ea) for an insight disclosure consent—a description of the CDR insight and to whom it was disclosed;

8 After subrule 1.14(3)

Insert:

(3A) For paragraph (1)(b), the other information is:

(a) a statement that the CDR consumer is entitled to request further records in accordance with rule 9.5; and

(b) information about how to make such a request.

9 After paragraph 4.11(3)(c)

Insert:

(ca) in the case of an insight disclosure consent—an explanation of the CDR insight that will make clear to the CDR consumer what the CDR insight would reveal or describe;

10 Rule 7.5A

At the beginning, insert "(1)", at the end add:

(2) Despite paragraph 7.5(1)(ca), disclosure of CDR data to a trusted adviser under a TA disclosure consent is not a ***permitted use or disclosure*** until the earlier of the following:

(a) [date tba];

(b) the day the Data Standards Chair makes the data standard about the matter referred to in subparagraph 8.11(1)(c)(iv).

(3) Despite paragraph 7.5(1)(ca), disclosure of CDR data to a trusted adviser under a TA disclosure consent is not a ***permitted use or disclosure*** unless the accredited data recipient has taken reasonable steps to confirm that the trusted adviser is currently a member of a class of trusted advisers mentioned in subrule 1.10C(2).

(4) Despite paragraph 7.5(1)(ca), disclosure of a CDR insight under an insight disclosure consent is not a ***permitted use or disclosure*** until the earlier of the following:

(a) [date tba];

(b) the day the Data Standards Chair makes the data standard about the matters referred to in subrule 8.11(1A).

(5) Despite paragraph 7.5(1)(ca), disclosure of a CDR insight under an insight disclosure consent is not a ***permitted use or disclosure*** if the CDR insight includes or reveals sensitive information within the meaning of the *Privacy Act 1988*.

11 Afte rule 7.9(2)

At the end, add:

(3) For subsection 56EM(2) of the Act, an accredited data recipient that discloses CDR data to a trusted adviser must, as soon as practicable, update each consumer dashboard that relates to the request to indicate:

(a) what CDR data was disclosed; and

(b) when the CDR data was disclosed; and

(c) the trusted adviser.

(4) For subsection 56EM(2) of the Act, an accredited data recipient that discloses a CDR insight must, as soon as practicable, update each consumer dashboard that relates to the request to indicate:

(a) what CDR data was disclosed; and

(b) when the CDR data was disclosed; and

(c) the person to whom it was disclosed.

12 After paragraph 8.11(1)(c)(iii)

Insert:

; and

(iv) consumer experience data standards for disclosure of CDR data to trusted advisers;

(v) consumer experience data standards for disclosure of CDR insights;

13 After subrule 8.11(1)

Insert:

(1A) The standards for the purposes of paragraph (1)(a)(ii) that relate to obtaining insight disclosure consents must include provisions that cover the following:

(a) how the accredited person can meet the requirement to explain a CDR insight in accordance with paragraph 4.11(3)(ca);

(b) ensuring that the CDR consumer is made aware that their data will leave the CDR system when it is disclosed.

14 After paragraph 9.3(2)(ea)

Insert:

(eb) disclosures of CDR data to trusted advisers, and trusted advisers to whom CDR data was disclosed;

(ec) the steps taken to confirm that a trusted advisor is a member of a class of trusted advisors for paragraph 7.5A(3);

(ed) disclosures of CDR insights, including a copy of each CDR insight disclosed, to whom it was disclosed and when;

15 Subparagraph 9.4(2)(f)(vi)

Substitute:

(vi) the number of consents received from CDR consumers during the reporting period to disclose CDR data to trusted advisers;

(vii) for each class of trusted advisers—the number of trusted advisers to whom CDR data was disclosed during the reporting period;

(viii) the number of insight disclosure consents received from CDR consumers during the reporting period.

16 Subrule 9.5(2)

After “(eb),”, insert “(ec),”.

Schedule 4—Amendments relating to joint accounts

Competition and Consumer (Consumer Data Right) Rules 2020

1 Subrule 1.7 (1)

Insert in the appropriate alphabetical position:

co-approval option has the meaning given by rule 4A.4.

disclosure option has the meaning given by rule 4A.4.

disclosure option management service has the meaning given by rule 4A.5.

joint account:

(a) means a joint account with a data holder for which there are 2 or more joint account holders, each of which is an individual who:

(i) so far as the data holder is aware, is acting in their own capacity and not on behalf of another person; and

(ii) is eligible in relation to the data holder; but

(b) does not include a partnership account with a data holder.

non-disclosure option has the meaning given by rule 4A.4.

pre-approval option has the meaning given by rule 4A.4.

2 Subrule 1.7 (1)—definition of *consumer dashboard*

Omit "rule 1.15", substitute "rules 1.15 and 4A.15".

3 Paragraph 1.15(1)(d))

Substitute:

(d) contains any other details, and has any other functionality, required by a provision of these rules.

4 After Part 4

Insert:

Part 4A—Joint accounts

Note: When this Part commences, it will be subject to transitional provisions that operate until April 2022.

Division 4A.1—Preliminary

4A.1 Purpose of Part

Special rules apply in relation to consumer data requests under Part 4 under which there is a request for disclosure of CDR data that relates to one or more joint accounts. This Part sets out those rules.

4A.2 Simplified outline of this Part

CDR data that relates to a joint account can be disclosed under these rules only in accordance with the disclosure option that applies to the account. Division 4A.2 sets out:

- the three disclosure options, with the default option being the pre-approval option; and
- an obligation for data holders to provide a service (a disclosure option management service) for all joint accounts to which this Part applies through which joint account holders can change the disclosure option that applies to the account, or propose a change to the other account holders.
- when one joint account holder proposes to change the disclosure option—a process by which the other joint account holders can either agree with or reject the proposal; and
- some associated notification requirements.

Any joint account holder can choose that the non-disclosure option will apply.

If the pre-approval option applies, any joint account holder can choose that the co-approval option will apply.

A change from the non-disclosure option to another option, or a change from the co-approval option to the pre-approval option, requires the agreement of all the joint account holders.

When an accredited person makes a consumer data request under Part 4 on behalf of a CDR consumer, and the request includes CDR data relating to one or more joint accounts of which the CDR consumer is a joint account holder, Division 4A.3 deals with how the request is processed.

Division 4A.3 also deals with how requests are processed when the accredited person makes a consumer data request on behalf of a secondary user of the joint account.

Division 4A.2A— Disclosure options

4A.3 Simplified outline of this Division

This Division sets out the disclosure options that can apply to a joint account. These disclosure options are relevant when an accredited person makes a consumer data request on behalf of one joint account holder or a secondary user under Part 4 .

The default is the pre-approval option. If this option applies, CDR data relating to the joint account can be disclosed in response to the request without the

approval of the other account holders, but the other account holders can revoke the pre-approval in relation to a particular consumer data request at any time.

Another option is the non-disclosure option. If this option applies, CDR data relating to the joint account cannot be disclosed under these rules.

The third option is the co-approval option. If this option applies, CDR data relating to the joint account can be disclosed under these rules only with the approval of the all the account holders.

Data holders must offer the pre-approval option and non-approval option on joint accounts, and may offer the co-approval option.

The process for changing the disclosure option is set out in this Division.

For each joint account to which this Part applies, a data holder must offer a disclosure option management service that can be used by joint account holders to select and manage these disclosure options.

4A.4 Disclosure options for joint accounts

Disclosure options

(1) Disclosure of CDR data relating to a joint account to which this Part applies may be authorised only as permitted by the ***disclosure option*** that applies to the joint account. This may be any of the following:

(a) the ***pre-approval option***, under which CDR data relating to the joint account may be disclosed in response to a valid consumer data request by one joint account holder on the authorisation of that joint account holder without the approval of other account holders;

(b) the ***co-approval option***, under which CDR data relating to the joint account may be disclosed in response to a valid consumer data request by one joint account holder only after:

(i) that joint account holder has authorised the disclosure; and

(ii) each of the other joint account holders has approved the disclosure;

(c) the ***non-disclosure option***, under which CDR data relating to the joint account may not be disclosed in response to a valid consumer data request by a joint account holder.

(2) The data holder must provide for the pre-approval and non-disclosure options to be available for a joint account

(3) The data holder may provide for the co-approval option to be available for a joint account.

(4) For the purposes of rule 4A.13, where the pre-approval option applies to a joint account and a joint account holder authorises the disclosure of CDR data that relates to the account in response to a valid consumer data request:

(a) each relevant account holder is taken to have approved the disclosure; and

(b) if an approval is withdrawn, the CDR data relating to the joint account may not be disclosed despite the authorisation.

Default option

(5) Unless a sector Schedule provides otherwise, the pre-approval option applies to a joint account by default.

(6) The disclosure option that applies to a joint account may be changed in accordance with rule 4A.8.

4A.5 Obligation to provide disclosure option management service

Obligation to provide disclosure option management service

(1) For each joint account to which this Part applies, the data holder must provide a service to each joint account holder that allows the joint account holder to:

(a) change the disclosure option that applies to the account in accordance with rule 4A.7; and

(b) propose a change in the disclosure option to the other joint account holders in accordance with rule 4A.8; and

(c) respond to a proposal by another joint account holder to change the disclosure option.

Note: This subrule is a civil penalty provision (see rule 9.8).

(2) Such a service is a ***disclosure option management service***.

Requirements for disclosure option management service

(3) The service must be provided online and, if there is a data holder's consumer dashboard for a joint account holder, may be included in the dashboard.

(4) The service may, but need not, also be provided other than online.

(5) The service must give effect to a change in the disclosure option as soon as practicable.

(6) The service must not do any of the following in relation to the processes that it provides for proposing to change the disclosure option that applies to the joint account, or responding to such a proposal (the ***processes***):

(a) add any requirements to the processes beyond those specified in the data standards and these rules;

(b) offer additional or alternative services as part of the processes;

(c) include or refer to other documents, or provide any other information, so as to reduce comprehensibility;

(d) offer any pre-selected options.

(7) The service must notify the joint account holder:

(a) of the matters mentioned in subrule 4A.6(1); and

(b) which disclosure option currently applies.

(8) The service must be in accordance with the data standards.

4A.6 Obligation to inform joint account holders

(1) A data holder must notify each joint account holder:
  (a) what disclosure options are available in relation to the joint account;
  (b) the effect of each disclosure option and how it operates, including, if there is a secondary user for the joint account, how it operates in relation to the secondary user;
  (c) that the pre-approval option applies by default;
  (d) that they can at any time:
    (i) choose to change the disclosure option on the joint account to the non-disclosure option; or
    (ii) propose to the other joint account holders to change the disclosure option to either co-approval or pre-approval;
  (e) how they can make such a choice or proposal;
  (f) how they can respond to such a proposal by another joint account holder;
  (g) that when CDR data relating to the joint account is disclosed under these rules, the data holder will ordinarily provide each joint account holder and, if applicable, each secondary user, with a consumer dashboard through which they will be able to see information about disclosures relating to the account.

(2) The notification must be done:
  (a) if the account is opened on or after [the commencement day]—at the time the account is opened; and
  (b) otherwise—within 7 business days after [the commencement day].

(3) The notification must be in accordance with the data standards.

4A.7 Changing to a more restrictive non-disclosure option

(1) A joint account holder may at any time choose that the non-disclosure option will apply to the joint account, using the disclosure option management service.

(2) If the pre-approval option applies to a joint account, a joint account holder may at any time choose that the co-approval option will apply to the joint account, using the disclosure option management service.

(3) If a joint account holder (***account holder A***) changes the non-discloure option that applies to the account in accordance with this rule, the data holder must, through its ordinary methods for contacting the other joint account holders:
  (a) explain to each of them what the consumer data right is; and
  (c) inform them which disclosure option previously currently applied to the account; and
  (b) inform them that account holder A has changed the disclosure option, and of the disclosure option that now applies; and
  (d) explain to them the mechanisms for changing the disclosure option again.

Note: This subrule is a civil penalty provision (see rule 9.8).

4A.8 Obtaining agreement on change to a less restrictive disclosure option

Application of rule

(1) This rule applies in relation to a particular joint account if:

(a) the non-disclosure option applies to the account, and a joint account holder (***account holder A***) proposes, using the disclosure option management service, to change to the co-approval or pre-approval disclosure option; or

(b) the co-approval option applies to the account, and a joint account holder (***account holder A***) proposes, using the disclosure option management service, to change to the pre-approval option.

Inviting other account holders to respond to proposal

(2) The data holder must, through its ordinary methods for contacting the other joint account holders:

(a) explain to each of them what the consumer data right is; and

(c) inform them which disclosure option currently applies to the account; and

(b) inform them that account holder A has proposed that the co-approval or pre-approval option apply to the account, as the case may be; and

(d) explain to them that this change requires the agreement of all account holders; and

(e) explain to them any alternative options for change that are available and how they can be made; and

(f) invite them to either agree to or reject the proposal within a specified period.

Note: This subrule is a civil penalty provision (see rule 9.8).

(3) At the end of the specified period, the data holder must inform the joint account holders whether:

(a) all the joint account holders have approved the change, and as a result the new disclosure option applies to the joint account; or

(c) not all the joint account holders have approved the change, and as a result the disclosure option is unchanged.

Note: This subrule is a civil penalty provision (see rule 9.8).

Division 4A.3—Consumer data requests that relate to joint accounts

Subdivision 4A.3.1—Preliminary

4A.9 Application of Division

(1) This Division applies in relation to a consumer data request to a data holder under Part 4 that is for disclosure of CDR data in relation to a particular joint account of a kind specified for the purposes of this paragraph in a sector Schedule.

(2) This Division applies whether or not the request is also for disclosure of other CDR data.

(3) If a particular consumer data request to a data holder under Part 4 relates to more than one joint account to which this Part applies, this Division applies separately in relation to each such joint account.

4A.10 Interpretation

For this Division:

(a) the ***requester*** is the person on whose behalf the consumer data request referred to in rule 4A.9 was made; and

(b) the ***relevant account holders*** are:

(i) if the requester is a secondary user—all joint account holders; and

(ii) if the requester is a joint account holder—the other joint account holders; and

(c) the ***joint account data*** is the CDR data that was the subject of the request referred to in subrule 4A.8(1).

Subdivision 4A.3.2—How consumer data requests to data holders under Part 4 that relate to joint accounts are handled

4A.11 How data holder is to deal with a consumer data request

When the data holder receives the consumer data request referred to in rule 4A.9:

(a) if the pre-approval disclosure option applies to the joint account—the data holder must respond to the request as if it were not a joint account and the requester were the only account holder; and

(b) if the co-approval option applies to the joint account—the data holder must:

(i) ask the requester for authorisation in accordance with rule 4.5 and Division 4.4; and

(ii) if the authorisation is given, invite the approval of the relevant account holders in accordance with rule 4A.12; and

(iii) if all the relevant account holders give their approval, comply with rules 4.6 and 4.7; and

(c) if the non-disclosure option applies—the data holder must refuse to disclose the requested CDR data.

4A.12 Asking relevant account holders for approval to disclose joint account data

(1) This rule applies if:

(a) the requester has authorised, under Division 4.4, the disclosure of the joint account data; and

(b) a co-approval option applies to the joint account.

Note: The data holder must provide each relevant account holder with consumer dashboard in accordance with rule 4A.15.

(2) The data holder must, through its ordinary methods for contacting each relevant account holder:

(a) indicate that an accredited person has requested disclosure of CDR data that relates to the joint account (the ***requested data***) on behalf of the requester; and

(b) outline the matters referred to in subrule (1); and

(c) indicate the matters referred to in paragraphs 4.23(a), (b), (c), (d) and (e) so far as they relate to the request; and

(d) ask the relevant account holder to approve or not approve disclosure of the joint account data, using their consumer dashboard; and

(e) specify the time by which the data holder needs to receive any approval, and inform them that if an approval is not received by that time, the joint account data will not be disclosed; and

(f) inform them that any one of them may, at any time, withdraw the approval using their consumer dashboard; and

(g) indicate what the effect of removing the approval would be.

Note: For removal of an approval, see rule 4A.13.

4A.13 Continuation and removal of approvals

(1) If a relevant account holder:

(a) approves of the disclosure of joint account data in accordance with this Division; or

(b) is taken to have approved of the disclosure under the pre-apporval option;

the approval is taken to apply while the authorisation referred to in paragraph 4A.11(b) is current, unless withdrawn sooner in accordance with this Division.

(2) Any relevant account holder may withdraw an approval given under this Division at any time, using their consumer dashboard.

4A.14 Joint account data the data holder is authorised to disclose

(1) For paragraph 4A.6(2) , the data holder must not disclose joint account data to the accredited person unless:

(a) the requester has authorised the data holder to disclose that CDR data under Division 4.4; and

(b) subrule (2), (3) or (4) applies.

Pre-approval option

(2) This subrule applies if:

(a) the pre-approval option applies to the joint account; and

(b) no relevant account holder has withdrawn their approval using their consumer dashboard.

Co-approval option

(3) This subrule applies if:

(a) the co-approval option applies to the joint account; and

(b) for each relevant account holder, either:

(i) the relevant account holder approved the disclosure in accordance with rule 4A.12 within the time specified and has not withdrawn the approval using their consumer dashboard; or

(ii) 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.

Note: Under subrule 4A.4, data holders are required to offer the pre-approval disclosure option, which applies by default. Data holders may, but are not required to, offer the co-approval option.

Pre-approval option does not apply but circumstances of physical or financial harm or abuse might exist

(4) This subclause applies if:

(a) the pre-disclosure option does not apply to the joint account; and

(b) the data holder considers it necessary, in order to prevent physical or financial harm or abuse, to avoid inviting at least one of the relevant account holders to either approve a change to the disclosure option or approve disclosure under the co-approval option.

4A.15 Consumer dashboard for joint account holders

Note: Where this Division applies, the data holder must provide a consumer dashboard for the requester under rule 1.15. This rule provides for the provision of a similar consumer dashboard for each relevant account holder in some circumstances and requires additional functionality on the dashboards.

Obligation for data holder to provide relevant account holders with consumer dashboard

(1) Where:

(a) this Division applies in relation to a consumer data request; and

(b) either the co-approval option or the pre-approval option applies, or has applied, to the joint account;

the data holder must ensure that each relevant account holder has an online service that:

(c) contains the details referred to in paragraph 1.15(1)(b) that relate to the joint account data; and

(d) has a functionality that:

(i) can be used by the relevant account holder to manage approvals in relation to each authorisation to disclose joint account data made by a requester; and

(ii) allows for withdrawal, at any time, of such an approval; and

(iii) is simple and straightforward to use; and

(iv) is prominently displayed; and

(v) as part of the withdrawal process, displays a message relating to the consequences of the withdrawal in accordance with the data standards.

Note: This subrule is a civil penalty provision (see rule 9.8).

(2) Such a service is the data holder's ***consumer dashboard*** for the relevant account holder.

(3) A data holder does not contravene subrule (1) in relation to subparagraphs (1)(c)(ii) and (iii) so long as it takes reasonable steps to ensure that the functionality complies with those subparagraphs.

Common information on consumer dashboard

(4) For paragraph 1.15(1)(d) , if a relevant account holder's consumer dashboard contains details of approvals under this Division, the dashboards of the other joint account holders must contain those details.

Exception in the case of physical or financial harm or abuse

(5) Despite this rule, the data holder may decline:

(a) to provide a relevant account holder with a consumer dashboard; or

(b) to reflect details mentioned in paragraph (1)(d) or subrule (4) in the dashboard of a joint account holder;

if it considers it necessary to do either in order to prevent physical or financial harm or abuse.

4A.16 Notification requirements for consumer data requests on joint accounts

(1) For this rule, an ***approval notification*** is a notice given by the data holder:

(a) to a relevant account holder, to inform them that the requester has given, amended or withdrawn an authorisation, or that the authorisation has expired; or

(b) to the requester, to inform them that:

(a) one or more of the relevant account holders has not given their approval for disclosure within the time frame referred to in paragraph 4A.12(2)(e); or

(b) a relevant account holder has withdrawn an approval previously given;

in accordance with the data standards.

(2) Subject to this rule, the data holder must make the appropriate approval notifications when the events mentioned in subrule (1) occur, through its ordinary means of contacting the joint account holders.

Note: This subrule is a civil penalty provision (see rule 9.8).

(3) The data holder must, in accordance with any relevant data standards:

(a) provide for alternative notification mechanisms;

(a) give each joint account holder a means of selecting such an alternative, and of changing a selection; and

(b) make approval notifications in accordance with the selections.

Note: This subrule is a civil penalty provision (see rule 9.8).

(4) However, an approval notification to a particular account holder under this rule is not required if the data holder considers it necessary to avoid notifying that account holder in order to prevent physical or financial harm or abuse.

5 Subrule 7.9(1), Note 2

Substitute:

Note 2: If a consumer data request is made that relates to a joint account, the other joint account holder's consumer dashboard may not be required to be similarly updated. See clause 4A.15.

6 Schedule 3, clause 1.2, definitions of *joint account* and *joint account management service*

Repeal.

7 Schedule 3, Part 4

Repeal.

8 Rule 9.8

Note: References to inserted provisions noted as being subject to a civil penalty will be added here, and references to provisions being repealed will be removed.

Insert in appropriate alphanumeric position:

……..

Schedule 5—Amendments relating to staged implementation

Competition and Consumer (Consumer Data Right) Rules 2020

1 Schedule 3, subclause 6.4(3)

Substitute:

(3) Where a table cell includes the term ***JAE*** (for "joint accounts excepted"), despite these rules, the data holder is not required to disclose required consumer data about a product that relates to joint accounts.

(4) Where a table cell includes the term ***CODE*** (for "certain other data excepted"), despite these rules, the data holder is not required to disclose required consumer data about a phase 1 product that:

(a) relates to any of the following:

(i) closed accounts;

(ii) direct debits;

(iii) scheduled payments;

(iv) payees; or

(b) is "get account detail" or "get customer detail" data within the meaning of the data standards.

2 Schedule 3, clause 6.6

Substitute:

6.6 Commencement table

(1) For this Part, the ***commencement table*** is:

Data holder	Data sharing obligations	Start date to 31 Jan 2021	1 Feb 2021 to 28 Feb 2021	1 Mar 2021 to 30 Jun 2021	1 Jul 2021 to 31 Oct 2021	1 Nov 2021 to 31 Jan 2022	1 Feb 2022 to 31 Mar 2022	1 Apr 2022 onward
Initial data holders (NAB, CBA, ANZ, Westpac branded products)	Part 2	All product phases	All product phases	All product phases	All product phases	All product phases	All product phases	All product phases
	Part 3	-	-	-	-	-	-	-
	Part 4	Phase 1 Phase 2	All product phases	All product phases	All product phases	All product phases	All product phases	All product phases
Any other relevant ADI and initial data holders for non-primary brands	Part 2	Phase 1	Phase 1 Phase 2	Phase 1 Phase 2	All product phases	All product phases	All product phases	All product phases
	Part 3	-	-	-	-	-	-	-
	Part 4	-	-	-	Phase 1 JAE CODE	Phase 1 Phase 2 JAE	All product phases JAE	All product phases
Accredited ADI and accredited non-ADI (reciprocal data holder)	Part 2	All product phases	All product phases	All product phases	All product phases	All product phases	All product phases	All product phases
	Part 3	-	-	-	-	-	-	-
	Part 4	-	-	Phase 1 JAE CODE	All product phases JAE	All product phases JAE	All product phases JAE	All product phases

Schedule 6—Transitional

Competition and Consumer (Consumer Data Right) Rules 2020

1 Transitional provisions

Note: A set of joint account provisions in relation to the banking sector was included in the principal rules as made (Part 4 of Schedule 3). These are the "former joint account provisons" for this item. The earlier amendment rules replaced that Part, but the transition provisions allowed data holders to continue to apply the former joint account provions for some time. This item allows those data holders to continue to use the former transition provisions until 1 April 2022, when they must begin to comply with the current Part 4A inserted by these amendment rules.

Compliance with Part 4A before 1 April 2022

(1) A particular data holder is taken to comply with the current Part 4A if the data holder:

(a) either:

(i) was required, before the amendment date, to comply with Part 4 of Schedule 3 as it stood immediately before the amendment date; or

(ii) before the amendment date, complied with the former joint account provisions in order to satisfy paragraph 105(4)(b) of Schedule 1 to the earlier amendment rules; or

(iii) is an accredited person; and

(b) between the amendment date and 31 March 2022, complies with the former joint account provisions (as varied to the extent reasonably necessary so that it operates in accordance with these rules as amended by these rules instead of the current Part 4A.

Application of Part 4A to existing joint account

(2) Subitems (3) and (4) apply in relation to a joint account with a data holder that is in existence immediately before the following day (the ***Part 4A day***):

(a) if the data holder does not make use of paragraph (1)(b) in relation to the account (an ***unaffected*** account)—the day when the data holder is first required to comply with the current Part 4A; or

(b) if the data holder makes use of paragraph (1)(b) in relation to the account (an ***affected account***)—the earlier of:

(i) the day that data holder ceases to make use of paragraph (1)(b); and

(ii) 1 April 2022.

(3) For an affected account to which a disclosure option has at any time applied under the former joint account provisions:

(a) if a disclosure option applied immediately before the Part 4A day—the equivalent disclosure option under the current Part 4A applies to the account on and after the Part 4A day; and

(b) if no disclosure option applied to the account immediately before the Part 4A day—the non-disclosure option applies to the account on and after the Part 4A day.

(4) For an unaffected account, or an affected account to which a disclosure option has never applied:

(a) the non-disclosure option applies to the account on and after the Part 4A day for 7 business days; and

(b) after the seventh business day, the pre-disclosure option applies to the account unless, before that day:

(i) an account holder applies the non-disclosure option to the account; or

(ii) an account holder proposes the co-disclosure option to apply to the account and the other account holders approve the disclosure option.

(5) The data holder must inform each joint account holders of the following, through its ordinary means of contacting them:

(a) that the current Part 4A now applies to the account;

(b) that the data holder is providing the disclosure option management service, with instructions on how to access it;

(c) the matters mentioned in paragraphs 4.6A(1)(a), (b) and (c) to (f) of the principal rules (obligation to inform joint account holders);

(d) of the disclosure option that currently applies to the account as a result of subitem (3) or (4) and the effect of that subitem.

Definitions

(6) In this item:

amendment date means the day Schedule 1 to these rules commenced.

current Part 4A means Part 4A of the principal rules as in force on and from the amendment date.

earlier amendment rules means the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020*.

former joint account provisions means Part 4 of Schedule 3 to the principal rules as in force immediately before the commencement of Schedule 1 to the earlier amendment rules.

principal rules means the *Competition and Consumer (Consumer Data Right) Rules 2020*.