Competition and Consumer (Consumer Data Right) Rules 2020

The Australian Competition and Consumer Commission makes the following rules.

Dated

IMPORTANT NOTE

Consultation draft of April 2020

This is a mock-up of the *Competition and Consumer (Consumer Data Right) Rules 2020* (the rules) as proposed to be amended.

This mock-up has been prepared for the purposes of consultation on the proposed amendments.

This is ***not*** a version of the rules as currently in force, and should not be relied on as a statement of the law.

It does not include amendments relating to changes in the staged commencement process. These will be addressed separately by the Commission.

For the rules as currently in force, see Federal Register of Legislation, https://www.legislation.gov.au/.

The Australian Competition and Consumer Commission

Contents

Part 1—Preliminary

Division 1.1—Preliminary

1.1 Name

This instrument is the *Competition and Consumer (Consumer Data Right) Rules 2020*.

1.2 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**
The whole of this instrument	The day after this instrument is registered.	

Note: This table relates only to the provisions of this instrument as originally made.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.

1.3 Authority

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

CONSULTATION DRAFT

Division 1.2—Simplified outline and overview of these rules

1.4 Simplified outline of these rules

There are 3 ways to request CDR data under these rules.

Product data requests
Any person may request a data holder to disclose CDR data that relates to products offered by the data holder. Such a request is called a product data request.

A product data request is made in accordance with relevant data standards, using a specialised service provided by the data holder. Such a request cannot be made for CDR data that relates to a particular identifiable CDR consumer. The data is disclosed, in machine-readable form, to the person who made the request. The data holder cannot impose conditions, restrictions or limitations of any kind on the use of the disclosed data.

Consumer data requests made by CDR consumers
A CDR consumer who, in accordance with a Schedule to these rules, is eligible to do so may directly request a data holder to disclose CDR data that relates to them. Such a request is called a consumer data request.

A consumer data request that is made directly to a data holder is made using a specialised online service provided by the data holder. The data is disclosed, in human-readable form, to the CDR consumer who made the request.

Consumer data requests made on behalf of CDR consumers
A CDR consumer who, in accordance with a Schedule to these rules, is eligible to do so may request an accredited person to request a data holder to disclose CDR data that relates to the consumer. The request made by the accredited person is called a consumer data request.

A consumer data request that is made on behalf of a CDR consumer by an accredited person must be made in accordance with relevant data standards, using a specialised service provided by the data holder. The data is disclosed, in machine-readable form, to the accredited person.

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.

These rules only apply in relation to certain classes of product and consumer CDR data that are set out in Schedules to these rules which relate to different designated sectors. Schedule 3 relates to the banking sector. Initially, these rules

will apply only in relation to certain products that are offered by certain data holders within the banking sector. These rules will then apply to a progressively broader range of data holders and products.

These rules also deal with a range of ancillary and related matters.

1.5 What these rules are about

(1) These rules set out details of how the consumer data right works.

(2) These rules should be read in conjunction with the following:
   (a) the *Competition and Consumer Act 2010* (the Act), and in particular, Part IVD of the Act, which sets out the general framework for how the consumer data right works;
   (b) designation instruments made under section 56AC of the Act;
   (c) guidelines made by the Information Commissioner under section 56EQ of the Act;
   (d) data standards made under section 56FA of the Act;
   (e) regulations made under section 172 of the Act.

1.6 Overview of these rules

(1) Part 1 of these rules deals with preliminary matters, such as:
   (a) definitions of terms that are used in these rules; and
   (b) the usage, in these rules, of certain terms that are defined in the Act.

   The other provisions of these rules should be read together with these definitions and other interpretive provisions. Part 1 also deals with services that must be provided by data holders and accredited persons that allow consumers to make and manage requests for CDR data.

(2) Part 2 of these rules deals with product data requests, and should be read in conjunction with relevant Schedules to these rules that deal with particular designated sectors.

(3) Part 3 of these rules deals with consumer data requests that are made by CDR consumers, and should be read in conjunction with relevant Schedules to these rules that deal with particular designated sectors. Only CDR consumers who are eligible to do so may make such requests. Schedule 3 to these rules sets out eligibility criteria for the banking sector.

(4) Part 4 of these rules deals with consumer data requests that are made by accredited persons on behalf of such eligible CDR consumers, and should be read in conjunction with relevant Schedules to these rules that deal with particular designated sectors.

(5) Part 5 of these rules deals with how persons can become accredited persons. It also deals with ancillary matters, such as revocation and suspension of accreditation, obligations of accredited persons, and the Register of Accredited Persons. The rules set out in this Part should be read in conjunction with Division 3 of Part IVD of the Act.

(6) Part 6 of these rules deals with dispute resolution.

(7) Part 7 of these rules deals with rules relating to the privacy safeguards. The rules set out in this Part should be read in conjunction with Division 5 of Part IVD of the Act. Part 7 also sets out some additional civil penalty provisions that protect the privacy or confidentiality of CDR consumers' CDR data.

(8) Part 8 of these rules deals with data standards. The rules set out in this Part should be read in conjunction with Division 6 of Part IVD of the Act.

(9) Part 9 of these rules deals with miscellaneous matters, such as review of decisions, reporting, record keeping and audit, and civil penalty provisions of the consumer data rules.

(10) Schedule 1 to these rules deals with default conditions on accreditations.

(11) Schedule 2 to these rules sets out detailed steps for privacy safeguard 12 (subsection 56EO(1) of the Act and rule 7.11 of these rules). These steps are also relevant to persons who receive CDR data under a CDR outsourcing arrangement, and are an element of the ongoing obligations of persons accredited at the "unrestricted" level (see paragraph 5.12(1)(a)).

(12) Schedule 3 to these rules contains details that are relevant to the banking sector. Schedule 3:

(a) sets out the specific CDR data in respect of which requests under these rules may be made; and

(b) sets out the circumstances in which CDR consumers are eligible in relation to requests for banking sector CDR data that relates to themselves; and

(c) deals with the progressive application of these rules to the banking sector.

It is intended that these rules will be amended at a later time to deal with additional sectors of the economy.

Division 1.3—Interpretation

1.7 Definitions

Note 1: A number of expressions used in this instrument are defined in the Act, including the following:

- Accreditation Registrar;
- accredited data recipient;
- accredited person;
- Australian Consumer Law;
- binding data standard;
- CDR consumer;
- CDR data;
- CDR participant;
- collects;
- Commission;
- court/tribunal order;
- data holder;
- Data Recipient Accreditor;
- data standard;
- Data Standards Body;
- Data Standards Chair;
- designated sector;
- directly or indirectly derived;
- privacy safeguards;
- Regulatory Powers Act.

Note 2: ***Information Commissioner*** has the same meaning as in the Act: see section 3A of the *Australian Information Commissioner Act 2010* and paragraph 13(1)(b) of the *Legislation Act 2003*.

(1) In this instrument:

accreditation applicant means a person who has applied to be an accredited person under rule 5.2.

accreditation number of an accredited person has the meaning given by rule 5.6.

accredited data recipient has a meaning affected by subrule (2).

Note: The term "accredited data recipient" is defined in the Act: see section 56AK of the Act. Subrule (2) deals with the usage of this term in these rules.

accredited person request service has the meaning given by subrule 1.13(3).

Act means the *Competition and Consumer Act 2010*.

addresses for service means both of the following:

(a) a physical address for service in Australia;

(b) an electronic address for service.

ADI (short for authorised deposit-taking institution) has the meaning given by the *Banking Act 1959*.

associated person, of another person, means any of the following:

(a) a person who:
  (i) makes or participates in making, or would (if the other person were an accredited person) make or participate in making, decisions that affect the management of CDR data by the other person; or
  (ii) has, or would have (if the other person were an accredited person), the capacity to significantly affect the other person's management of CDR data;

(b) if the other person is a body corporate—a person who:
  (i) is an associate (within the meaning of the *Corporations Act 2001*) of the other person; or
  (ii) is an associated entity (within the meaning of the *Corporations Act 2001*) of the other person.

CDR complaint data, in relation to a CDR participant, means the following:

(a) the number of CDR consumer complaints received by the CDR participant;
(b) the number of such complaints for each complaint type, in accordance with the CDR participant's complaints handling process;
(c) the number of such complaints resolved;
(d) the average number of days taken to resolve CDR consumer complaints through internal dispute resolution;
(e) the number of CDR consumer complaints referred to a recognised external dispute resolution scheme;
(f) the number of CDR consumer complaints resolved by external dispute resolution;
(g) the number of complaints made to the CDR participant by other CDR participants in relation to compliance with:
  (i) Part IVD of the Act; or
  (ii) these rules; or
  (iii) binding data standards.

Note 1: Paragraphs (a) to (d) include complaints that are resolved through internal dispute resolution within 5 business days.

Note 2: Complaints covered by paragraph (g) are not "CDR consumer complaints".

CDR consumer has a meaning affected by subrule (2).

Note: The term "CDR consumer" is defined in the Act: see subsection 56AI(3) of the Act. Subrule (2) deals with the usage of this term in these rules.

CDR consumer complaint means any expression of dissatisfaction made by a CDR consumer to or about a CDR participant:

(a) that relates to:

(i) the CDR participant's obligations under or compliance with:
(A) Part IVD of the Act; or
(B) these rules; or
(C) binding data standards; or
(ii) the provision to the CDR consumer, by the CDR participant, of the goods or services in respect of which the consumer granted consent under Part 4; and

(b) for which a response or resolution could reasonably be expected.

Note: Complaints of a kind referred to in sub-subparagraph (a)(i)(B) include a complaint relating to the participant's obligations under, or compliance with, rules dealing with the handling of CDR consumer complaints.

CDR data de-identification process has the meaning given by rule 1.17.

CDR data deletion process has the meaning given by rule 1.18.

CDR logo means the registered trade mark with registration number XXX.

Note: Registered trade marks can be viewed at https://www.ipaustralia.gov.au/.

Note: An application for registration of the trade mark has been made, and the application is pending approval at this time.

CDR logo licensing conditions means the conditions for use of the CDR logo published by the Commission, as in force from time to time.

Note: The CDR logo licensing conditions could, in 2020, be viewed on the Commission's website (https://www.accc.gov.au/).

CDR outsourcing arrangement has the meaning given by rule 1.10.

CDR participant has a meaning affected by subrule (2).

Note: The term "CDR participant" is defined in the Act: see subsection 56AL(1) of the Act. Subrule (2) deals with the usage of this term in these rules.

CDR policy means a policy that a CDR participant has and maintains in compliance with subsection 56ED(3) of the Act.

consumer dashboard:

(a) in relation to an accredited person—has the meaning given by rule 1.14; and
(b) in relation to a data holder—has the meaning given by rule 1.15.

consumer data request:

(a) by a CDR consumer—has the meaning given by rule 3.3; and
(b) by an accredited person on behalf of a CDR consumer—has the meaning given by rule 4.4.

current:

(a) a consent to collect and use particular CDR data is ***current*** if it has not expired in accordance with rule 4.14; and
(b) an authorisation to disclose particular CDR data is ***current*** if it has not expired in accordance with rule 4.26.

data holder has a meaning affected by subrule (2).

Note: The term "data holder" is defined in the Act: see subsection 56AJ of the Act. Subrule (2) deals with the usage of this term in these rules.

data minimisation principle has the meaning given by rule 1.8.

Data Standards Advisory Committee has the meaning given by rule 8.2.

direct request service has the meaning given by subrule 1.13(2).

eligible, in relation to a particular designated sector, has the meaning set out in a Schedule to these rules that relates to that sector.

Note: For the banking sector, see clause 2.1 of Schedule 3 to these rules.

fit and proper person criteria has the meaning given by rule 1.9.

foreign entity means a person who:
(a) is not a body corporate established by or under a law of the Commonwealth, of a State or of a Territory; and
(b) is neither an Australian citizen, nor a permanent resident (within the meaning of the *Australian Citizenship Act 2007*).

Note: See subsection 56CA(2) of the Act.

goods includes products.

law relevant to the management of CDR data means any of the following:
(a) the Act;
(b) any regulation made for the purposes of the Act;
(c) these rules;
(d) the *Corporations Act 2001* and the *Corporations Regulations 2001*;
(e) the *Privacy Act 1988*;
(f) in relation to a particular designated sector—any law that is specified for the purposes of this paragraph in a Schedule to these rules that relates to that designated sector.

Note: In relation to paragraph (f), for the banking sector, see clause 7.1 of Schedule 3.

local agent, in relation to a foreign entity, means a person who:
(a) is appointed by the foreign entity; and
(b) has addresses for service; and
(c) is authorised to accept service of documents on behalf of the foreign entity.

meet the internal dispute resolution requirements, in relation to the banking sector, has the meaning given by clause 5.1 of Schedule 3.

outsourced service provider has the meaning given by rule 1.10.

product data request has the meaning given by rule 2.3.

product data request service has the meaning given by rule 1.12.

recognised external dispute resolution scheme means a dispute resolution scheme that is recognised under section 56DA of the Act.

redundant data has the meaning given by paragraph 56EO(2)(a) of the Act.

Register of Accredited Persons means the Register of Accredited Persons established under subsection 56CE(1) of the Act.

requester, in relation to a product data request, means the person who made the request under rule 2.3.

required consumer data, in relation to the banking sector, has the meaning given by clause 3.2 of Schedule 3.

required product data, in relation to the banking sector, has the meaning given by clause 3.1 of Schedule 3.

restricted ADI means an ADI that has an authority under section 9 of the *Banking Act 1959* to carry on a banking business in Australia for a limited time specified in accordance with section 9D of that Act.

type of CDR data means a type of data that is identified in the data standards.

Note: See paragraph 8.11(1)(d).

valid has the meaning given by subrule 3.3(3) or subrule 4.3(3) as appropriate.

voluntary consumer data, in relation to the banking sector, has the meaning given by clause 3.2 of Schedule 3.

voluntary product data, in relation to the banking sector, has the meaning given by clause 3.1 of Schedule 3.

(2) The table has effect:

Meaning of references to certain terms

	A reference, in a particular provision of these rules, to:	**is, depending on the context, a reference to:**
1	a CDR consumer	(a) a CDR consumer for any CDR data; or (b) a CDR consumer for the particular CDR data that is dealt with in relation to the reference.

Meaning of references to certain terms		
	A reference, in a particular provision of these rules, to:	**is, depending on the context, a reference to:**
2	a data holder	(a) a data holder of any CDR data; or (b) the data holder of the particular CDR data that is dealt with in relation to the reference.
3	an accredited data recipient	(a) an accredited data recipient of any CDR data; or (b) the accredited data recipient of the particular CDR data that is dealt with in relation to the reference.
4	a CDR participant	(a) a CDR participant for any CDR data; or (b) the CDR participant for the particular CDR data that is dealt with in relation to the reference.

*References to **data holder***

(3) In these rules, depending on the context, a reference to a data holder is a reference to a data holder that would be required or that is authorised to disclose CDR data in response to a product data request or a consumer data request that is made in accordance with these rules.

Note: These rules will progressively apply to a broader range of data holders within the banking sector: see Part 6 of Schedule 3 to these rules.

References to a person's CDR data

(4) In these rules, a reference to a person's CDR data is a reference to the CDR data for which that person is a CDR consumer.

1.8 Data minimisation principle

Note: The data minimisation principle is relevant when:

- a CDR consumer requests an accredited person to provide goods or services to the CDR consumer or to another person; and
- the accredited person needs to access the CDR consumer's CDR data in order to provide those goods or services.

The data minimisation principle is also relevant when an accredited person uses CDR data to provide requested goods or services to a CDR consumer.

The data minimisation principle limits the CDR data that an accredited person can collect, and also limits the uses that the accredited person can make of collected CDR data.

An accredited person complies with ***the data minimisation principle*** if:

(a) when making a consumer data request on behalf of a CDR consumer, it does not seek to collect:
   (i) more CDR data than is reasonably needed; or
   (ii) CDR data that relates to a longer time period than is reasonably needed;

   in order to provide the goods or services requested by the CDR consumer; and

(b) when providing the requested goods or services, it does not use the collected CDR data, or CDR data derived from it, beyond what is reasonably needed in order to provide the requested goods or services.

1.9 Fit and proper person criteria

(1) For these rules, the ***fit and proper person criteria***, in relation to a person, are the following:

(a) whether the person, or any associated person, has, within the previous 10 years, been convicted of:
   (i) a serious criminal offence; or
   (ii) an offence of dishonesty;

   against any law of the Commonwealth or of a State or a Territory, or a law of a foreign jurisdiction;

(b) whether the person, or any associated person, has been found to have contravened:
   (i) a law relevant to the management of CDR data; or
   (ii) a similar law of a foreign jurisdiction;

(c) whether the person, or any associated person, has been the subject of:
   (i) a determination under paragraph 52(1)(b) or any of paragraphs 52(1A)(a), (b), (c) or (d) of the *Privacy Act 1988*; or
   (ii) a finding or determination of a similar nature under a similar law of a foreign jurisdiction;

(d) if the person is a body corporate—whether any of the directors (within the meaning of the *Corporations Act 2001*) of the person, or any associated person:
   (i) has been disqualified from managing corporations; or
   (ii) is subject to a banning order;

(e) whether the person, or any associated person, has a history of insolvency or bankruptcy;

(f) whether the person, or any associated person, has been the subject of a determination made under an external dispute resolution scheme that:
   (i) included a requirement to pay monetary compensation; and
   (ii) was, at the time the determination was made:
      (A) recognised under the *Privacy Act 1988*; or
      (B) a recognised external dispute resolution scheme;

(g) any other relevant matter, including but not limited to the objects of Part IVD of the Act.

Note: The objects of Part IVD are set out in section 56AA of the Act.

(2) In this rule:

banning order has the same meaning as in the *Corporations Act 2001*.

serious criminal offence means an offence for which, if the act or omission had taken place in the Jervis Bay Territory, a person would have been be liable, on first conviction, to imprisonment for a period of not less than 5 years.

Note: Jervis Bay Territory is mentioned because it is a jurisdiction in which the Commonwealth has control over the criminal law.

1.10 Meaning of *outsourced service provider* and *CDR outsourcing arrangement*

(1) For these rules, an ***outsourced service provider*** is a person to whom an accredited person discloses CDR data under a CDR outsourcing arrangement.

(2) For these rules, a person (the ***discloser***) discloses CDR data to another person (the ***recipient***) under a ***CDR outsourcing arrangement*** if it does so under a written contract between the discloser and the recipient under which:

(a) the recipient will provide, to the discloser, goods or services using CDR data; and

(b) the recipient is required to comply with the following requirements in relation to any CDR data disclosed to it by the discloser:

(i) the recipient must take the steps in Schedule 2 to protect that CDR data, and any CDR data that it directly or indirectly derives from that CDR data, as if it were an accredited data recipient; and

(ii) the recipient must not use or disclose any such CDR data other than in accordance with a contract with the discloser; and

(iii) the recipient must, when so directed by the discloser, do any of the following:

(A) return to the discloser CDR data that the discloser disclosed to it;

(B) delete CDR data that it holds in accordance with the CDR data deletion process;

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

(D) direct any other person to which it has disclosed CDR data to take corresponding steps; and

(iv) the recipient must not disclose any such CDR data to another person, otherwise than under a CDR outsourcing arrangement; and

(v) if the recipient does disclose such CDR data in accordance with subparagraph (iv), it must ensure that the other person complies with the requirements of the CDR outsourcing arrangement.

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

CONSULTATION DRAFT

Division 1.4—General provisions relating to data holders and to accredited persons

Subdivision 1.4.1—Preliminary

1.11 Simplified outline of Division

This Division sets out:

- general obligations of data holders which relate to product data requests and consumer data requests; and
- general obligations for data holders and accredited persons to provide CDR consumers with consumer dashboards, which contain information relating to consumer data requests, and a functionality for withdrawing consents and authorisations under these rules.

CONSULTATION DRAFT

Subdivision 1.4.2—Services for making requests under these rules

1.12 Product data request service

(1) A data holder must provide an online service that:
  (a) can be used to make product data requests; and
  (b) enables requested data to be disclosed in machine-readable form; and
  (c) conforms with the data standards.

Note 1: See rule 2.3 for the meaning of "product data request".

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

(2) Such a service is a ***product data request service***.

1.13 Consumer data request service

(1) A data holder must provide:
  (a) an online service that:
    (i) can be used by eligible CDR consumers to make consumer data requests directly to the data holder; and
    (ii) allows a request to be made in a manner that is no less timely, efficient and convenient than any of the online services that are ordinarily used by customers of the data holder to deal with it; and
    (iii) enables requested data to be disclosed in human-readable form; and
    (iv) sets out any fees for disclosure of voluntary consumer data; and
    (v) conforms with the data standards; and
  (b) an online service that:
    (i) can be used by accredited persons to make consumer data requests, on behalf of eligible CDR consumers, to the data holder; and
    (ii) enables requested data to be disclosed in machine-readable form; and
    (iii) conforms with the data standards.

Note 1: See rule 3.3 for the meaning of "consumer data request" in relation to a request made by a CDR consumer directly to a data holder.

Note 2: See rule 4.4 for the meaning of "consumer data request" in relation to a request made by an accredited person to a data holder on behalf of a CDR consumer.

Note 3: This subrule is a civil penalty provision (see rule 9.8).

(2) The service referred to in paragraph (1)(a) is the data holder's ***direct request service***.

(3) The service referred to in paragraph (1)(b) is the data holder's ***accredited person request service***.

(4) A data holder does not contravene subrule (1) in relation to subparagraph (1)(a)(ii) so long as it takes reasonable steps to ensure that the online service complies with that subparagraph.

Subdivision 1.4.3—Services for managing consumer data requests made by accredited persons

1.14 Consumer dashboard—accredited person

(1) An accredited person must provide an online service that:

(a) can be used by each eligible CDR consumer on whose behalf the accredited person makes a consumer data request to manage:

(i) such requests; and

(ii) associated consents to collect and use CDR data; and

(b) contains the details of each consent to collect and use CDR data given by the CDR consumer specified in subrule (3); and

(c) has a functionality that:

(i) allows a CDR consumer, at any time, to:

(A) withdraw consents to collect and use CDR data; and

(B) elect that redundant data be deleted in accordance with these rules and withdraw such an election; and

(ii) is simple and straightforward to use; and

(iii) is prominently displayed.

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

(2) Such a service is the accredited person's ***consumer dashboard*** for that consumer.

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

(a) details of the CDR data to which the consent relates;

(b) details of the specific use or uses for which the CDR consumer has given their consent;

(c) when the CDR consumer gave the consent;

(d) whether the CDR consumer gave the consent for collection of CDR data:

(i) on a single occasion; or

(ii) over a period of time;

(e) if the CDR consumer gave the consent for collection of CDR data over a period of time:

(i) what that period is; and

(ii) how often data has been, and is expected to be, collected over that period;

(f) if the consent is current—when it is scheduled to expire;

(g) if the consent is not current—when it expired;

(h) information relating to CDR data that was collected pursuant to the consent (see rule 7.4).

Note 1: For paragraph (f), consents to collect and use CDR data expire at the latest 12 months after they are given: see paragraph 4.14(1)(d).

Note 2: For the specific uses that are possible, see the data minimisation principle (rule 1.8).

CONSULTATION DRAFT

Note 3: The consumer dashboard could contain other information too, for example, the written notices referred to in rule 7.15 (which deals with correction requests under privacy safeguard 13, section 56EP of the Act).

(4) An accredited person does not contravene subrule (1) in relation to subparagraph (1)(c)(ii) so long as it takes reasonable steps to ensure that the functionality complies with that subparagraph.

1.15 Consumer dashboard—data holder

(1) If a data holder receives a consumer data request from an accredited person on behalf of a CDR consumer, the data holder must provide an online service to the CDR consumer that:

(a) can be used by the CDR consumer to manage authorisations to disclose CDR data in response to the request; and

(b) contains the details of each authorisation to disclose CDR data specified in subrule (3); and

(c) has a functionality that:

(i) allows for withdrawal, at any time, of authorisations to disclose CDR data; and

(ii) is simple and straightforward to use; and

(iii) is no more complicated to use than the process for giving the authorisation to disclose CDR data; 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 that consumer.

Note: For the banking sector, if an accredited person makes a consumer data request that relates to a joint account, the other joint account holder may also need to be provided with a consumer dashboard: see clause 4.4 of Schedule 3.

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

(a) details of the CDR data that has been authorised to be disclosed;

(b) when the CDR consumer gave the authorisation;

(c) the period for which the CDR consumer gave the authorisation;

(d) if the authorisation is current—when it is scheduled to expire;

(e) if the authorisation is not current—when it expired;

(f) information relating to CDR data that was disclosed pursuant to the authorisation (see rule 7.9);

(g) for a disclosure of CDR data that relates to the authorisation but that was pursuant to a request under subsection 56EN(4) of the Act—that fact.

Note 1: For paragraph (d), authorisations to disclose CDR data expire at the latest 12 months after they are given: see paragraph 4.26(1)(e).

Note 2: The consumer dashboard could contain other information too, for example, the written notice referred to in rules 7.10 (which deals with quality of CDR data under privacy safeguard 11, section 56EN of the Act) and 7.15 (which deals with correction requests under privacy safeguard 13, section 56EP of the Act).

(4) 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.

CONSULTATION DRAFT

Subdivision 1.4.4—Other obligations of accredited persons and accredited data recipients

1.16 Obligation relating to CDR outsourcing arrangements

An accredited person must ensure that, if it discloses CDR data to another person under a CDR outsourcing arrangement, the recipient complies with its requirements under the arrangement.

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

Subdivision 1.4.4A—Use of the CDR logo

1.16A Authorisation for accredited persons and data holders to use CDR logo

(1) If the data standards indicate that the CDR logo may be used in particular circumstances, accredited persons and data holders are authorised to use the CDR logo:

(a) in those circumstances; and

(b) in accordance with:

(i) the CDR logo licensing conditions; and

(ii) the requirements (if any) of the data standards.

(2) An accredited person must not use the CDR logo other than as authorised under this rule.

Note 1: If an accredited person uses the CDR logo other than as authorised, this could, for example, result in:

- their accreditation being suspended or revoked in accordance with item 3, item 6 or item 7 of the table to rule 5.17; or
- infringement of the CDR logo (which is protected as a trade mark under the *Trade Marks Act 1995*); or
- a contravention of provisions of the Australian Consumer Law.

Note 2: If a data holder uses the CDR logo other than as authorised, this could, for example, result in:

- infringement of the CDR logo (which is protected as a trade mark under the *Trade Marks Act 1995*); or
- a contravention of provisions of the Australian Consumer Law.

Subdivision 1.4.5—Deletion and de-identification of CDR data

1.17 CDR data de-identification process

(1) This rule sets out the ***CDR data de-identification process*** for particular CDR data (the ***relevant data***).

Note: This process is applied by an accredited data recipient when de-identifying CDR data in accordance with a consent from a CDR consumer (see Subdivision 4.3.3) and when de-identifying redundant data for the purposes of privacy safeguard 12 (see rule 7.12).

(2) First, the accredited data recipient must consider whether, having regard to the following:

(a) the DDF;

(b) the techniques that are available for de-identification of data;

(c) the extent to which it would be technically possible for any person to be once more identifiable, or reasonably identifiable, after de-identification in accordance with such techniques;

(d) the likelihood (if any) of any person once more becoming so identifiable, or reasonably identifiable from the data after de-identification;

it would be possible to de-identify the relevant data to the extent (the ***required extent***) that no person would any longer be identifiable, or reasonably identifiable, from:

(e) the relevant data after the proposed de-identification; and

(f) other information that would be held, following the completion of the de-identification process, by any person.

(3) If this is possible, the accredited data recipient must:

(a) determine the technique that is appropriate in the circumstances to de-identify the relevant data to the required extent; and

(b) apply that technique to de-identify the relevant data to the required extent; and

(c) delete, in accordance with the CDR data deletion process, any CDR data that must be deleted in order to ensure that no person is any longer identifiable, or reasonably identifiable, from the information referred to in paragraphs (2)(e) and (f); and

(d) as soon as practicable, make a record to evidence the following:

(i) its assessment that it is possible to de-identify the relevant data to the required extent;

(ii) that the relevant data was de-identified to that extent;

(iii) how the relevant data was de-identified, including records of the technique that was used;

(iv) any persons to whom the de-identified data is disclosed.

(4) If this is not possible, the accredited data recipient must delete the relevant data and any CDR data directly or indirectly derived from it in accordance with the CDR data deletion process.

Note: For the CDR data deletion process, see rule 1.18.

(5) For this rule, the ***DDF*** is *The De-Identification Decision-Making Framework* published by the Office of the Information Commissioner and Data61, as in force from time to time.

Note: The *De-Identification Decision-Making Framework* could in 2020 be downloaded from Data61's website (https://www.data61.csiro.au/).

1.17A Identification of otherwise redundant data that is not to be deleted

(1) Where the accredited data recipient has identified CDR data as redundant, it must identify whether any of the following provisions of the Act apply to the CDR data:

(a) paragraphs 56BAA(2)(a), (b) or (c) of the Act (deletion request by consumer);

(b) paragraphs 56EO(2)(b) or (c) of the Act (privacy safeguard 12).

(2) Where one of those provisions applies, the accredited person must retain the CDR data while that provision applies.

(3) For the purposes of paragraph 56BAA(2)(c) of the Act, in relation to CDR data of a CDR consumer, the person may:

(a) request the CDR consumer to state whether or not proceedings of the kind mentioned in that paragraph are current or anticipated; and

(b) rely on that statement.

1.18 CDR data deletion process

For these rules, the ***CDR data deletion process*** in relation to a person that holds CDR data that is to be deleted consists of the following steps:

(a) delete, to the extent reasonably practicable, that CDR data and any copies of that CDR data;

(b) make a record to evidence the deletion; and

(c) direct any other person to which it has disclosed that CDR data to:

(i) delete, to the extent reasonably practicable, any copies of that CDR data, or any CDR data directly or indirectly derived from it, that it holds; and

(ii) make a record to evidence the steps taken to delete the CDR data; and

(iii) notify the person who gave the direction of the deletion.

Note: The CDR data deletion process is applied by an accredited data recipient when deleting CDR data in accordance with a CDR consumer's right to deletion (see Subdivision 4.3.4) and when deleting redundant data for the purposes of privacy safeguard 12 (see rule 7.13).

Part 2—Product data requests

2.1 Simplified outline of this Part

This Part deals with product data requests. Such requests are made using a data holder's product data request service.

A product data request may be for required product data, voluntary product data, or both. Schedule 3 to these rules provides for what is required product data and voluntary product data for the banking sector.

When requested in accordance with this Part, a data holder:

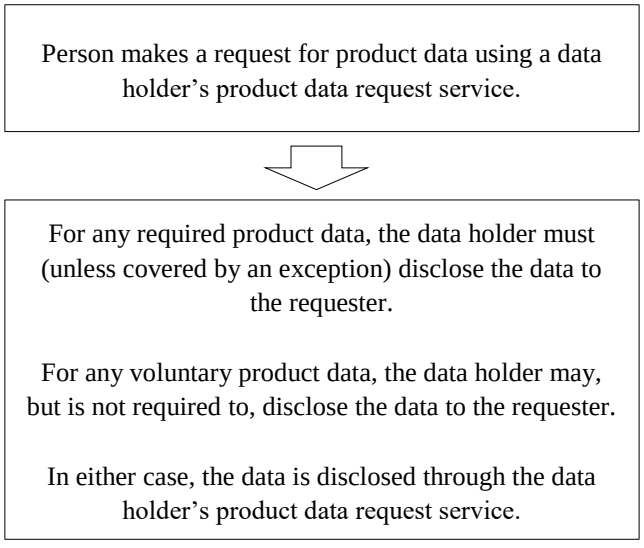
- must, subject to an exception outlined in this Part, disclose required product data; and
- may, but is not required to, disclose voluntary product data.

In either case, the data is disclosed to the person who made the request, in machine-readable form and in accordance with the data standards. A data holder must not impose conditions, restrictions or limitations of any kind on the use of the disclosed data.

A fee cannot be charged for the disclosure of required product data, but could be charged for the disclosure of voluntary product data.

2.2 Making product data requests—flowchart

The following is a flowchart for how product data requests are made:



CONSULTATION DRAFT

2.3 Product data requests

(1) A person may:

(a) using the data holder's product data request service; and

(b) in accordance with the data standards;

request a data holder to disclose some or all of the CDR data that relates to one or more products that are offered by the data holder.

Note: These rules will progressively permit product data requests to be made to a broader range of data holders within the banking sector, and in relation to a broader range of CDR data, according to the timetable set out in Part 6 of Schedule 3.

(2) Such a request is a ***product data request***.

Note: A fee cannot be charged for making a product data request.

2.4 Disclosing product data in response to product data request

(1) This rule applies if a data holder has received a product data request.

(2) The data holder may disclose any requested voluntary product data to the requester.

Note: See rule 1.7 for the definition of "voluntary product data", and see clause 3.1 of Schedule 3 for the definition of "voluntary product data" in relation to the banking sector.

(3) The data holder must, subject to rule 2.5:

(a) disclose the requested required product data to the requester:

(i) through its product data request service; and

(ii) in accordance with the data standards; and

(b) include in the disclosed data any required product data that is:

(i) the subject of the product data request; and

(ii) contained:

(A) on the data holder's website; or

(B) in a product disclosure statement that relates to the product.

Note 1: See rule 1.7 for the definition of "required product data", and see clause 3.1 of Schedule 3 for the definition of "required product data" in relation to the banking sector.

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

Note 3: A fee cannot be charged for the disclosure of required product data: see section 56BU of the Act.

2.5 Refusal to disclose required product data in response to product data request

(1) Despite subrule 2.4(3), the data holder may refuse to disclose required product data in response to the request in circumstances (if any) set out in the data standards.

(2) The data holder must inform the requester of such a refusal in accordance with the data standards.

Civil penalty:

(a) for an individual—$50,000; and

(b) for a body corporate—$250,000.

2.6 Use of data disclosed pursuant to product data request

A data holder that discloses CDR data in response to a product data request must not impose conditions, restrictions or limitations of any kind on the use of the disclosed data.

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

CONSULTATION DRAFT

Part 3—Consumer data requests made by eligible CDR consumers

Division 3.1—Preliminary

3.1 Simplified outline of this Part

This Part deals with consumer data requests that are made directly by eligible CDR consumers to data holders. Such requests are made using the data holder's direct request service.

A request may be for the CDR consumer's required consumer data, their voluntary consumer data, or both. Schedule 3 to these rules:

- provides for what is required consumer data and voluntary consumer data for the banking sector; and
- sets out the circumstances in which CDR consumers are eligible to request their banking sector CDR data.

When validly requested in accordance with this Part, a data holder:

- must, subject to an exception outlined in this Part, disclose required consumer data; and
- may, but is not required to, disclose voluntary consumer data.

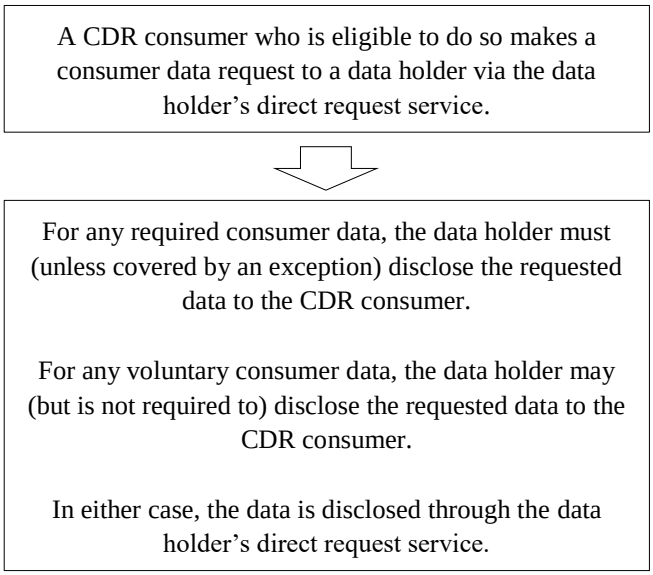
In either case, the data is disclosed to the CDR consumer who made the request, in human-readable form and in accordance with the data standards.

For the banking sector, special rules apply to joint accounts with 2 individual joint account holders. These are set out in Part 4 of Schedule 3.

A fee cannot be charged for the disclosure of required consumer data, but could be charged for the disclosure of voluntary consumer data.

3.2 How an eligible CDR consumer makes a consumer data request—flowchart

The following is a flowchart for how an eligible CDR consumer makes a consumer data request under this Part:



Division 3.2—Consumer data requests made by CDR consumers

3.3 Consumer data requests made by CDR consumers

(1) A CDR consumer may, using the data holder's direct request service, request a data holder to disclose some or all of their CDR data.

Note: These rules will progressively permit consumer data requests to be made to a broader range of data holders within the banking sector, and in relation to a broader range of CDR data, according to the timetable set out in Part 6 of Schedule 3.

(2) Such a request is a ***consumer data request*** made by a CDR consumer.

Note: A fee cannot be charged for the disclosure of required consumer data: see section 56BU of the Act.

(3) A consumer data request made under this Part is ***valid*** if it is made by a CDR consumer who is eligible to make the request.

Note: See subrule 1.7(1) for the meaning of "eligible". For the banking sector, see clause 2.1 of Schedule 3 for when a CDR consumer is eligible.

3.4 Disclosing consumer data in response to a valid consumer data request

(1) This rule applies if a data holder has received a request that it reasonably believes to be a valid consumer data request made under this Part, for disclosure of CDR data of which it is the data holder.

(2) The data holder may disclose any requested voluntary consumer data to the CDR consumer who made the request.

Note: See rule 1.7 for the definition of "voluntary consumer data", and see clause 3.2 of Schedule 3 for the definition of "voluntary consumer data" in relation to the banking sector.

(3) The data holder must, subject to these rules, disclose any requested required consumer data to the CDR consumer who made the request:

(a) through its direct request service; and

(b) in accordance with the data standards.

Note 1: See rule 1.7 for the definition of "required consumer data", and see clause 3.2 of Schedule 3 for the definition of "required consumer data" in relation to the banking sector.

Note 2: For the banking sector, for a request that relates to a joint account, see clause 4.3 of Schedule 3 for an additional circumstance in which data relating to the joint account might not be disclosed under these rules.

Note 3: This subrule is a civil penalty provision (see rule 9.8).

Note 4: A fee cannot be charged for the disclosure of required consumer data: see section 56BU of the Act.

Note 5: For exceptions to this subrule, see rule 3.5 and subrules 5.33(4) and 5.34(4).

3.5 Refusal to disclose required consumer data in response to consumer data request

(1) Despite subrule 3.4(3), the data holder may refuse to disclose required consumer data in response to the request:

(a) if the data holder considers this to be necessary to prevent physical or financial harm or abuse; or

(aa) in relation to an account that is blocked or suspended; or

(b) in circumstances (if any) set out in the data standards.

(2) The data holder must inform the CDR consumer of such a refusal in accordance with the data standards.

Civil penalty:

(a) for an individual—$50,000; and

(b) for a body corporate—$250,000.

CONSULTATION DRAFT

Part 4—Consumer data requests made by accredited persons

Division 4.1—Preliminary

4.1 Simplified outline of this Part

This Part deals with consumer data requests that are made to data holders by accredited persons on behalf of CDR consumers. Such requests are made using the data holder's accredited person request service.

In order for such a request to be made, the CDR consumer must have first asked the accredited person to provide goods or services to the CDR consumer or to another person, where provision of those goods or services requires the use of the CDR consumer's CDR data.

Before making a consumer data request on behalf of a CDR consumer, the consumer must first have consented to the accredited person collecting and using specified CDR data to provide the requested goods or services.

Subject to certain limitations, the requested data can be any CDR data that relates to the CDR consumer.

Collection and use of CDR data under this Part is limited by the data minimisation principle, under which the accredited person:

(a) must not collect more data than is reasonably needed in order to provide the requested goods or services; and

(b) may use the collected data only as consented to by the consumer, and only as reasonably needed in order to provide the requested goods or services.

A request may be for the CDR consumer's required consumer data, their voluntary consumer data, or both. Schedule 3 to these rules:

- provides for what is required consumer data and voluntary consumer data for the banking sector; and
- sets out the circumstances in which CDR consumers are eligible in relation to a request for their banking sector CDR data.

Subject to exceptions outlined in this Part, the data holder:

- must seek the CDR consumer's authorisation to disclose required consumer data; and
- must seek the CDR consumer's authorisation to disclose any voluntary consumer data that it intends to disclose.

The data holder then must disclose, to the accredited person, the required consumer data it is authorised to disclose, and may (but is not required to) disclose the voluntary consumer data it is authorised to disclose. The data is disclosed in machine-readable form and in accordance with the data standards.

For the banking sector, special rules apply where there are joint account holders. These are set out in Part 4 of Schedule 3.

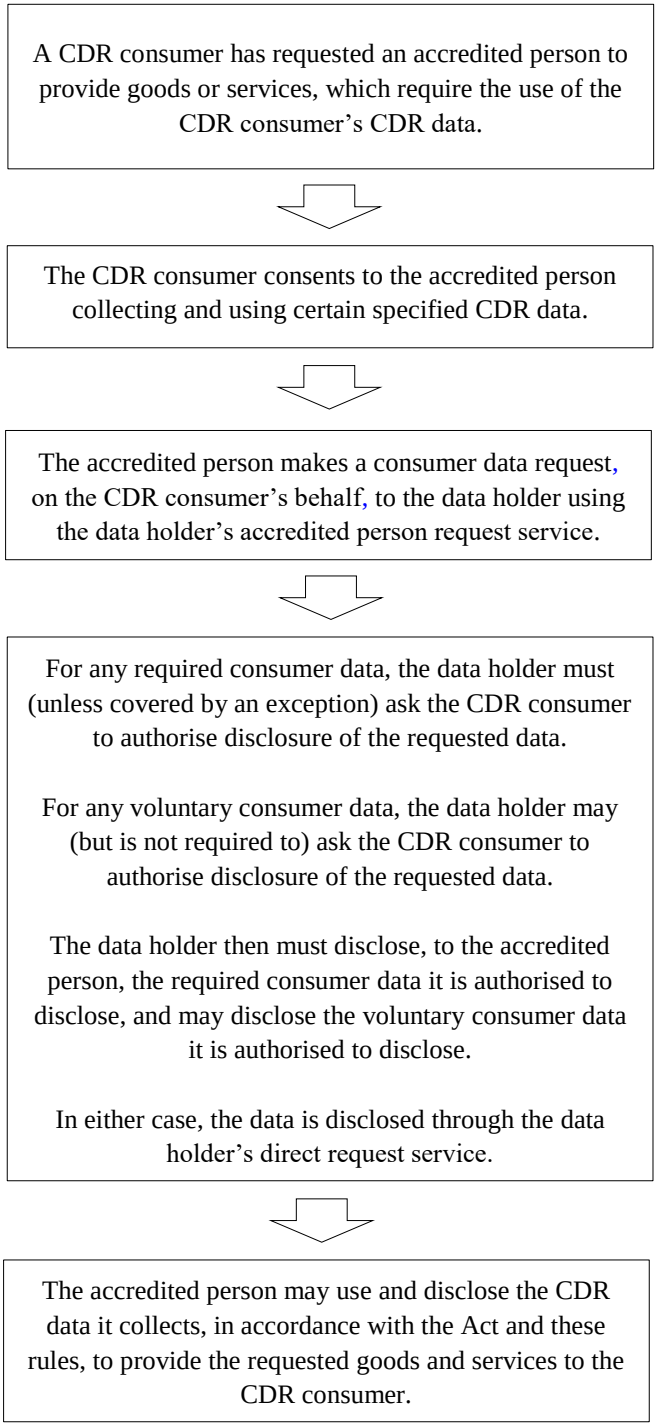
A fee cannot be charged for the disclosure of required consumer data, but could be charged for the disclosure of voluntary consumer data.

CONSULTATION DRAFT

4.2 Consumer data requests made by accredited persons—flowchart

The following is a flowchart for how an accredited person makes a consumer data request under this Part:

CONSULTATION DRAFT



CONSULTATION DRAFT

Division 4.2—Consumer data requests made by accredited persons

4.3 Request for accredited person to seek to collect CDR data

(1) This rule applies if:

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

(b) the accredited person needs to access the CDR consumer's CDR data in order to provide those goods or services.

(2) The accredited person may, in accordance with Subdivision 4.3.2, ask the CDR consumer to give their consent to the accredited person collecting and using their CDR data 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 data holder.

Note 2: The accredited person is able to collect and use CDR data only in accordance with the data minimisation principle: see rule 1.8.

(3) In giving the consent in response to such a request, the CDR consumer gives the accredited person a ***valid*** request to seek to collect that CDR data from a data holder.

Note: If the 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 consent is withdrawn.

(5) If an accredited person asks for a CDR consumer's consent to collect and use CDR data for the purpose of making a consumer data request under this Part, the accredited person must do so in accordance with Subdivision 4.3.2.

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

4.4 Consumer data requests by accredited persons

(1) If:

(a) a CDR consumer has given an accredited person a valid request under rule 4.3; and

(b) the consent referred to in rule 4.3 is current;

the accredited person may request the relevant data holder to disclose, to the accredited person, some or all of the CDR data that:

(c) is the subject of the relevant consent to collect and use CDR data; and

(d) it is able to collect and use in compliance with the data minimisation principle.

Note: See rule 1.8 for the definition of the "data minimisation principle".

(2) Such a request is a ***consumer data request*** by an accredited person on behalf of a CDR consumer.

Note 1: An accredited person might need to make consumer data requests to several data holders in order to provide the goods or services requested by the CDR consumer, and might need to make regular consumer data requests over a period of time in order to provide those goods or services.

Note 2: These rules will progressively permit consumer data requests to be made in relation to CDR data held by a broader range of data holders within the banking sector, and in relation to a broader range of CDR data, according to the timetable set out in Part 6 of Schedule 3.

(3) An accredited person must, if it makes a consumer data request under this Part, make the request:

(a) using the data holder's accredited person request service; and

(b) in accordance with the data standards.

Note 1: A data holder cannot charge an accredited person a fee for making a consumer data request in relation to required consumer data.

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

4.5 Data holder must ask eligible CDR consumer to authorise disclosure

(1) This rule applies if:

(a) a data holder receives a consumer data request under this Part; and

(b) there is no current authorisation for the data holder to disclose the requested data to the person who made the request; and

(c) the data holder reasonably believes that the request was made by an accredited person on behalf of an eligible CDR consumer.

Note: See subrule 1.7(1) for the meaning of "eligible". For the banking sector, see clause 2.1 of Schedule 3 for when a CDR consumer is eligible.

(2) If the data holder is considering disclosing any of the requested voluntary consumer data, the data holder must ask the CDR consumer on whose behalf the request was made to authorise the disclosure:

(a) in accordance with Division 4.4; and

(b) in accordance with the data standards.

Note 1: See rule 1.7 for the definition of "voluntary consumer data", and see clause 3.2 of Schedule 3 for the definition of "voluntary consumer data" in relation to the banking sector.

Note 2: For the banking sector, for requests that relate to joint accounts, in some cases, the data holder might need to seek an authorisation from the other joint account holder: see clause 4.5 of Schedule 3 to these rules.

Note 3: This subrule is a civil penalty provision (see rule 9.8).

(3) The data holder must, subject to these rules, ask the CDR consumer on whose behalf the request was made to authorise the disclosure of any requested required consumer data:

(a) in accordance with Division 4.4; and

(b) in accordance with the data standards.

Note 1: See rule 1.7 for the definition of "required consumer data", and see clause 3.2 of Schedule 3 for the definition of "required consumer data" in relation to the banking sector.

Note 2: For the banking sector, for requests that relate to joint accounts, in some cases, the request might be refused without the data holder needing to seek authorisation under this rule: see clause 4.3 of Schedule 3.

Note 3: For the banking sector, for requests that relate to joint accounts, in some cases, the data holder might need to seek an authorisation from the other joint account holder: see clause 4.5 of Schedule 3 to these rules.

Note 4: This subrule is a civil penalty provision (see rule 9.8).

Note 5: For exceptions to this subrule, see rule 4.7 and subrules 5.33(4) and 5.34(5).

4.6 Disclosing consumer data in response to a consumer data request

(1) This rule applies if:

(a) a data holder has received a consumer data request made under this Part for disclosure of CDR data; and

(b) the CDR consumer on whose behalf the request was made has given the data holder a current authorisation to disclose some or all of that CDR data.

(2) The data holder may disclose, to the person who made the request, any of the requested voluntary consumer data that it is authorised to disclose.

Note: See rule 1.7 for the definition of "voluntary consumer data", and see clause 3.2 of Schedule 3 for the definition of "voluntary consumer data" in relation to the banking sector.

(3) It must do so:

(a) through its accredited person request service; and

(b) in accordance with the data standards.

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

(4) The data holder must, subject to these rules, disclose, to the person who made the request, the requested required consumer data that it is authorised to disclose:

(a) through its accredited person request service; and

(b) in accordance with the data standards.

Note 1: See rule 1.7 for the definition of "required consumer data", and see clause 3.2 of Schedule 3 for the definition of "required consumer data" in relation to the banking sector.

Note 2: For the banking sector, for a request that relates to a joint account, see clause 4.3 of Schedule 3 for additional circumstances in which CDR data relating to the joint account might not be disclosed under these rules.

Note 3: A fee cannot be charged for the disclosure of required consumer data: see section 56BU of the Act.

Note 4: Rule 7.4 (which deals with privacy safeguard 5, paragraph 56EH(a) of the Act) requires the accredited person to update its consumer dashboard for the CDR consumer on whose behalf the request was made to indicate the CDR data that was collected.

CONSULTATION DRAFT

Note 5: Rule 7.9 (which deals with privacy safeguard 10, paragraph 56EM(1)(a) of the Act) requires the data holder to update its consumer dashboard for the CDR consumer on whose behalf the request was made to indicate the CDR data that was disclosed.

Note 6: This subrule is a civil penalty provision (see rule 9.8).

Note 7: For exceptions to this subrule, see rule 4.7 and subrules 5.33(4) and 5.34(4).

4.7 Refusal to disclose required consumer data in response to consumer data request

(1) Despite subrules 4.5(3) and 4.6(4), a data holder may refuse to ask for an authorisation in relation to the relevant CDR data, or refuse to disclose required consumer data in response to the request:

(a) if the data holder considers this to be necessary to prevent physical or financial harm or abuse; or

(b) if the data holder has reasonable grounds to believe that disclosure of some or all of that data would adversely impact the security, integrity or stability of:

(i) the Register of Accredited Persons; or

(ii) the data holder's information and communication technology systems; or

(c) in relation to an account that is blocked or suspended; or

(d) in circumstances (if any) set out in the data standards.

(3) The data holder must inform the accredited person of such a refusal in accordance with the data standards.

Civil penalty:

(a) for an individual—$50,000; and

(b) for a body corporate—$250,000.

Division 4.3—Consents to collect and use CDR data

Subdivision 4.3.1—Preliminary

4.8 Purpose of Division

This Division deals with consents to collect and use CDR data.

4.9 Object

The object of this Division is to ensure that a consent given by a CDR consumer to collect and use CDR data is:

(a) voluntary; and
(b) express; and
(c) informed; and
(d) specific as to purpose; and
(e) time limited; and
(f) easily withdrawn.

CONSULTATION DRAFT

Subdivision 4.3.2—Consents and their duration and withdrawal

Note: Under rule 4.3, if an accredited person asks a CDR consumer for their consent to collect and use their CDR data, it must do so in accordance with this Subdivision, and in particular, rules 4.10, 4.11 and 4.12. A failure to do so could contravene one or more civil penalty provisions: see section 56EF of the Act and rule 4.3.

4.10 Requirements relating to accredited person's processes for seeking consent

An accredited person's processes for asking a CDR consumer to give consent:

(a) must:

(i) accord with the data standards; and

(ii) having regard to any consumer experience guidelines developed by the Data Standards Body, be as easy to understand as practicable, including by use of concise language and, where appropriate, visual aids; and

(b) must not:

(i) include or refer to other documents so as to reduce comprehensibility; or

(ii) bundle consents with other directions, permissions, consents or agreements.

4.11 Asking CDR consumer to give consent to collect and use CDR data

Asking CDR consumer for consent

(1) When asking a CDR consumer to consent to the collection and use of their CDR data, an accredited person must:

(a) allow the CDR consumer to choose the types of CDR data to be collected and used by enabling the CDR consumer to actively select or otherwise clearly indicate:

(i) which of the particular types of CDR data they are consenting to the accredited person collecting; and

(ii) the specific uses of that data to which they are consenting; and

(b) allow the CDR consumer to choose the period over which CDR data will be collected and used by enabling the CDR consumer to actively select or otherwise clearly indicate whether the CDR data would be:

(i) collected on a single occasion and used over a specified period of time; or

(ii) collected and used over a specified period of time; and

(c) ask for the CDR consumer's express consent:

(i) for the accredited person to collect those types of CDR data over that period of time; and

(ii) for those uses of the collected CDR data; and

(iii) to any direct marketing the accredited person intends to undertake;

(d) if:

(i) the request covers voluntary consumer data; and

(ii) the data holder charges a fee for disclosure; and

(iii) the accredited person is intending to pass that fee onto the CDR consumer;

do the following:

(iv) clearly distinguish between the required consumer data and the voluntary consumer data;

(v) if the data holder charges a fee for disclosure of any such voluntary consumer data—allow the CDR consumer to actively select or otherwise clearly indicate whether to consent to the collection of that data; and

(e) allow the CDR consumer to make an election in relation to deletion of redundant data in accordance with rule 4.16.

Example: An accredited person could present the CDR consumer with a set of un-filled boxes corresponding to different types of data, and permit the CDR consumer to select the boxes that correspond to the data they consent to the accredited person collecting.

Note 1: An accredited person could not infer consent, or seek to rely on an implied consent.

Note 2: For paragraph (b), the specified period may not be more than 12 months: see subrule 4.12(1). After the end of the period, redundant data would need to be dealt with in accordance with subsection 56EO(2) of the Act (privacy safeguard 12) and rules 7.12 and 7.13.

(2) The accredited person must not present pre-selected options to the CDR consumer for the purposes of subrule (1).

Information presented to CDR consumer when asking for consent

(3) When asking for the consent, the accredited person must give the CDR consumer the following information:

(a) its name;

(b) its accreditation number;

(c) how the collection and use of CDR data indicated in accordance with subrule (1) complies with the data minimisation principle, including how:

(i) that collection of CDR data is reasonably needed, and relates to no longer a time period than is reasonably needed; and

(ii) that use of CDR data would not go beyond what is reasonably needed;

in order to provide the requested goods or services to the CDR consumer;

(d) if the following apply:

(i) the request covers voluntary consumer data;

(ii) the data holder charges a fee for disclosure;

(iii) the accredited person is intending to pass that fee onto the CDR consumer;

the following information:

(iv) that fact;
(v) the amount of the fee;
(vi) the consequences if the CDR consumer does not consent to the collection of that data;

(e) if the accredited person is asking for the CDR consumer's consent to de-identify some or all of the collected CDR data for the purpose of disclosing (including by selling) the de-identified data—the additional information relating to de-identification specified in rule 4.15;

(f) if the CDR data may be disclosed to an outsourced service provider (including one that is based overseas):
(i) a statement of that fact; and
(ii) a link to the accredited person's CDR policy; and
(iii) a statement that the consumer can obtain further information about such disclosures from the policy if desired;

(g) the following information about withdrawal of consents:
(i) a statement that, at any time, the consent can be withdrawn;
(ii) instructions for how the consent can be withdrawn;
(iii) a statement indicating the consequences (if any) to the CDR consumer if they withdraw the consent;

(h) the following information about redundant data:
(i) a statement, in accordance with rule 4.17, regarding the accredited person's intended treatment of redundant data;
(ii) a statement outlining the CDR consumer's right to elect that their redundant data be deleted;
(iii) instructions for how the election can be made.

Note: For paragraph (c), if the accredited person is seeking the CDR consumer's consent to de-identification as referred to in paragraph (e), the accredited person would need to indicate how that would comply with the data minimisation principle.

4.12 Restrictions on seeking consent

(1) An accredited person must not specify a period of time for the purposes of paragraph 4.11(1)(b) that is more than 12 months.

(2) An accredited person must not ask the CDR consumer to consent to collection or use of their CDR data unless the accredited data recipient would comply with the data minimisation principle in respect of that collection or those uses.

Note: See rule 1.8 for the definition of "data minimisation principle".

(3) An accredited person must not ask a CDR consumer to give consent to use or disclose their CDR data for any of the following uses or disclosures:
(a) selling the CDR data (unless de-identified in accordance with the CDR data de-identification process);

(b) subject to subrule (4), using the CDR data, including by aggregating the data, for the purpose of:
  (i) identifying; or
  (ii) compiling insights in relation to; or
  (iii) building a profile in relation to;
  any identifiable person who is not the CDR consumer who made the consumer data request.

(4) Paragraph (3)(b) does not apply in relation to a person whose identity is readily apparent from the CDR data, if the accredited person is seeking consent to:
  (a) derive, from that CDR data, CDR data about that person's interactions with the CDR consumer; and
  (b) use that derived CDR data in order to provide the requested goods or services.

4.13 Withdrawal of consent to collect and use CDR data and notification

(1) The CDR consumer who gave a consent to collect and use particular CDR data may withdraw the consent at any time:
  (a) by using the accredited person's consumer dashboard; or
  (b) by using an alternative method of communication made available by the accredited person for that purpose.

(2) The accredited person must:
  (a) if the withdrawal was in accordance with paragraph (1)(a)—give effect to the withdrawal as soon as practicable, and in any case within 2 business days after receiving the communication; and
  (b) in any case—notify the data holder of the withdrawal in accordance with the data standards.

Note 1: Upon notification, an authorisation to disclose the CDR data expires: see paragraph 4.26(1)(b).

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

(3) Withdrawal of a consent does not affect an election under rule 4.16 that the CDR consumer's collected CDR data be deleted once it becomes redundant.

4.14 Duration of consent to collect and use CDR data

(1) A consent to collect and use particular CDR data expires at the earliest of the following:
  (a) if the consent was withdrawn in accordance with paragraph 4.13(1)(a)—the earlier of the following:
    (i) when the accredited person gave effect to the withdrawal;
    (ii) 2 business days after the accredited person received the written communication;

(b) if the consent was withdrawn in accordance with paragraph 4.13(1)(b)—when the consent was withdrawn;

(c) if the accredited person was notified, under paragraph 4.25(2)(b), of the withdrawal of the authorisation to disclose that CDR data—when the accredited person received that notification;

(d) the end of the period of 12 months after the consent was given;

(e) at the end of the period the CDR consumer consented to in accordance with rule 4.11;

(f) if the consent expires as a result of the operation of another provision of these rules that references this paragraph.

Note: Clause 7.2 of Schedule 3 is an example of a provision referencing paragraph (f). This relates to when an accredited data recipient of CDR data becomes instead a data holder of that CDR data.

(2) If an accredited person's accreditation is revoked or surrendered in accordance with rule 5.17, all consents for the accredited person to collect and use CDR data expire when the revocation or surrender takes effect.

Subdivision 4.3.3—Information relating to de-identification of CDR data

4.15 Additional information relating to de-identification of CDR data

For paragraph 4.11(3)(e), the additional information relating to de-identification is the following:

(a) what the CDR data de-identification process is;

(b) that it would disclose (by sale or otherwise) the de-identified data to one or more other persons;

(c) the classes of persons to which it would disclose that data;

(d) why it would so disclose that data;

(e) that the CDR consumer would not be able to elect, in accordance with rule 4.16, to have the de-identified data deleted once it becomes redundant data.

Subdivision 4.3.4—Election to delete redundant data

4.16 Election to delete redundant data

(1) The CDR consumer who gave a consent to collect and use particular CDR data may elect that the collected data, and any data derived from it, be deleted when it becomes redundant data:

(a) when giving consent to the collection and use of the data; or

(b) at any other time before the consent expires.

Note: See rule 7.12 for the effect of an election.

(2) The CDR consumer may make the election:

(a) by communicating it to the accredited person in writing; or

(b) by using the accredited person's consumer dashboard.

(3) This rule does not apply if, when seeking consent for collection and use of the CDR data, the accredited person informs the CDR consumer that they have a general policy of deleting CDR data when it becomes redundant data.

Note: See paragraph 4.17(1)(a).

(4) This rule does not require the deletion of derived CDR data that was de-identified in accordance with the CDR data de-identification process before the collected data from which it was derived became redundant.

4.17 Information relating to redundant data

(1) For subparagraph 4.11(3)(h), the accredited person must state whether they have a general policy, when collected CDR data becomes redundant data, of:

(a) deleting the redundant data; or

(b) de-identifying the redundant data; or

(c) deciding, when the CDR data becomes redundant data, whether to delete it or de-identify it.

(2) An accredited person that gives the statement referred to in paragraph (1)(b) or (c) must also state:

(a) that, if it de-identifies the redundant data:

(i) it would apply the CDR data de-identification process; and

(ii) it would be able to use or, if applicable, disclose (by sale or otherwise) the de-identified redundant data without seeking further consent from the CDR consumer; and

(b) what de-identification of CDR data in accordance with the CDR data de-identification process means; and

(c) if applicable, examples of how it could use the redundant data once de-identified.

Note: For the CDR data de-identification process, see rule 1.17.

CONSULTATION DRAFT

Subdivision 4.3.5—Notification requirements

4.18 CDR receipts

(1) The accredited person must give the CDR consumer a notice that complies with this rule (a ***CDR receipt***) as soon as practicable after:

(a) the CDR consumer consents to the accredited person collecting and using CDR data in accordance with this Division; or

(b) the CDR consumer withdraws such a consent in accordance with rule 4.13.

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

(2) A CDR receipt given for the purposes of paragraph (1)(a) must set out:

(a) the details that relate to the consent that are listed in subparagraphs 1.14(3)(a) to (f); and

(b) the name of each data holder the CDR consumer has consented to the collection of CDR data from; and

(c) any other information the accredited person provided to the CDR consumer when obtaining the consent (see rule 4.11).

(3) A CDR receipt given for the purposes of paragraph (1)(b) must set out when the consent expired.

(4) A CDR receipt must be given in writing otherwise than through the CDR consumer's consumer dashboard.

(5) A copy of the CDR receipt may be included in the CDR consumer's consumer dashboard.

4.19 Updating consumer dashboard

An accredited person must update a CDR consumer's consumer dashboard as soon as practicable after the information required to be contained on the dashboard changes.

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

4.20 Ongoing notification requirement—consents to collect and use CDR data

(1) This rule applies in relation to a consent for an accredited person to collect and use CDR data that relates to a particular consumer data request under this Part if:

(a) the consent is current; and

(b) 90 days have elapsed since the latest of the following:

(i) the CDR consumer consented to the collection and use of the CDR data;

(ii) the CDR consumer last used their consumer dashboard;

(iii) the accredited person last sent the CDR consumer a notification in accordance with this rule.

(2) The accredited person must notify the CDR consumer in accordance with this rule that the consent is still current.

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

(3) The notification must be given in writing otherwise than through the CDR consumer's consumer dashboard.

(4) A copy of the notification may be included in the CDR consumer's consumer dashboard.

CONSULTATION DRAFT

Division 4.4—Authorisations to disclose CDR data

Note: Under rule 4.5, if a data holder is considering disclosing voluntary consumer data in response to a consumer data request, or if required consumer data was requested, the data holder must seek an authorisation from the CDR consumer to disclose the CDR data in accordance with (among other things) this Division, and in particular, rules 4.23, 4.24 and 4.25. A failure to do so could contravene one or more civil penalty provisions: see rule 4.5.

4.21 Purpose of Division

This Division deals with authorisations to disclose CDR data for the purposes of rule 4.5.

Note: This Division also deals with how to ask for authorisations to disclose CDR data that relates to joint accounts within the banking sector, for the purposes of clause 4.5 of Schedule 3.

4.22 Requirements relating to data holder's processes for seeking authorisation

A data holder's processes for asking a CDR consumer to give an authorisation must:

(a) accord with the data standards; and

(b) having regard to any consumer experience guidelines developed by the Data Standards Body, be as easy to understand as practicable, including by use of concise language and, where appropriate, visual aids.

4.23 Asking CDR consumer to give authorisation to disclose CDR data

When asking a CDR consumer to authorise the disclosure of CDR data, a data holder must give the CDR consumer the following information:

(a) the name of the accredited person that made the request;

(b) the period of time to which the CDR data that was the subject of the request relates;

(c) the types of CDR data for which the data holder is seeking an authorisation to disclose;

(d) whether the authorisation is being sought for:

(i) disclosure of CDR data on a single occasion; or

(ii) disclosure of CDR data over a period of time of not more than 12 months;

(e) if authorisation is being sought for disclosure over a period of time—what that period is;

(f) a statement that, at any time, the authorisation can be withdrawn;

(g) instructions for how the authorisation can be withdrawn.

4.24 Restrictions when asking CDR consumer to authorise disclosure of CDR data

When asking a CDR consumer to authorise the disclosure of CDR data, the data holder must not do any of the following:

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

(b) provide or request additional information during the authorisation process beyond that specified in the data standards and these rules;

(c) offer additional or alternative services as part of the authorisation process;

(d) include or refer to other documents.

4.25 Withdrawal of authorisation to disclose CDR data and notification

(1) The CDR consumer who gave, to a data holder, an authorisation to disclose particular CDR data to an accredited person may withdraw the authorisation at any time:

(a) by using the data holder's consumer dashboard; or

(b) by using an alternative method of communication made available by the data holder for that purpose.

(2) The data holder must:

(a) if the withdrawal was in accordance with paragraph (1)(a)—give effect to the withdrawal as soon as practicable, and in any case within 2 business days after receiving the communication; and

(b) in any case—notify the accredited person of the withdrawal in accordance with the data standards.

Note 1: Upon notification, an authorisation to disclose the CDR data expires: see paragraph 4.14(1)(b).

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

4.26 Duration of authorisation to disclose CDR data

(1) An authorisation to disclose particular CDR data to an accredited person expires at the earliest of the following:

(a) if the authorisation was withdrawn in accordance with paragraph 4.25(1)(a)—the earlier of the following:

(i) when the data holder gave effect to the withdrawal;

(ii) 2 business days after the data holder received the written communication;

(b) if the authorisation was withdrawn in accordance with paragraph 4.25(1)(b)—when the authorisation was withdrawn;

(c) if the CDR consumer ceases to be eligible in relation to the data holder;

(d) if the data holder was notified, under paragraph 4.13(2)(b), of the withdrawal of a consent to collect that CDR data—when the data holder received that notification;

(e) the end of the period of 12 months after the authorisation was given;

(f) if the authorisation was for disclosure of CDR data on a single occasion—after the CDR data has been disclosed;

(g) if the authorisation was for disclosure of CDR data over a specified period—the end of that period;

(h) if the authorisation expires as a result of the operation of a provision of these rules that references this paragraph.

Note: Clause 7.2 of Schedule 3 is an example of a provision satisfying paragraph (h). This relates to when an accredited data recipient of CDR data becomes instead a data holder of that CDR data.

(2) If an accredited person's accreditation is revoked or surrendered in accordance with rule 5.17, all authorisations for a data holder to disclose CDR data to that accredited person expire when the data holder is notified of the revocation or surrender.

4.27 Updating consumer dashboard

A data holder must update a CDR consumer's consumer dashboard as soon as practicable after the information required to be contained on the dashboard changes.

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

Part 5—Rules relating to accreditation etc.

Division 5.1—Preliminary

5.1 Simplified outline of this Part

A person may apply under this Part to be an accredited person. The Data Recipient Accreditor may accredit a person, under section 56CA of the Act, if satisfied that the person meets the criteria for accreditation specified in this Part. This Part also deals with:

- how applications are dealt with by the Data Recipient Accreditor; and
- obligations of accredited persons; and
- the transfer, suspension, surrender and revocation of accreditations; and
- related functions of the Data Recipient Accreditor.

This Part deals with how entries are added to the Register of Accredited Persons, and how that Register is updated, amended and corrected.

Division 5.2—Rules relating to accreditation process

Subdivision 5.2.1—Applying to be accredited person

5.2 Applying to be an accredited person

Note: There is currently only a single level of accreditation, the "unrestricted" level.

(1) A person may apply to the Data Recipient Accreditor to be an accredited person.

(2) The application must:

(a) be in the form approved, by the Data Recipient Accreditor, for the purposes of this paragraph (the ***approved form***); and

(b) include any documentation or other information required by the approved form; and

(c) state:

(i) the applicant's addresses for service; or

(ii) if the applicant is a foreign entity:

(A) the applicant's local agent; and

(B) the local agent's addresses for service; and

(d) describe the sorts of goods or services using CDR data that the applicant intends to offer to CDR consumers if they are accredited; and

(e) if the applicant is not a person who was specified in a designation instrument (see paragraph 56AC(2)(b) of the Act)—indicate whether it is or expects to be the data holder of any CDR data that is specified in a designation instrument.

Note 1: For paragraph (c), see rule 1.7 for the meaning of "addresses for service". The physical address for service could be a registered office (within the meaning of the *Corporations Act 2001*).

Note 2: For paragraph (c), changes to the addresses for service must be notified in accordance with paragraph 5.14(c). Documents may be served on an applicant in accordance with regulation 12 of the *Competition and Consumer Regulations 2010* by the Commission, or in accordance with section 28A of the *Acts Interpretation Act 1901* and section 9 of the *Electronic Transactions Act 1999*.

Subdivision 5.2.2—Consideration of application to be accredited person

5.3 Data Recipient Accreditor may request further information

(1) The Data Recipient Accreditor may request that the accreditation applicant provide further information to support the application.

(2) Without limiting subrule (1), the Data Recipient Accreditor may request the further information:
  (a) in writing; or
  (b) in an interview with the Data Recipient Accreditor; or
  (c) by phone, email, videoconferencing or any other form of electronic communication.

Note: If the accreditation applicant does not provide the further information as requested under this rule, the Data Recipient Accreditor might not be in a position to be satisfied, under section 56CA of the Act, that the applicant meets the criteria for accreditation.

5.4 Data Recipient Accreditor may consult

(1) When making a decision under this Part, the Data Recipient Accreditor may consult with:
  (a) other Commonwealth, State or Territory authorities as relevant, including, but not limited to:
    (i) the Information Commissioner; and
    (ii) the Australian Securities and Investments Commission; and
    (iii) the Australian Prudential Regulation Authority; and
    (iv) the Australian Financial Complaints Authority; and
  (b) similar authorities of foreign jurisdictions.

(2) The functions of the Australian Prudential Regulation Authority include providing the Data Recipient Accreditor with advice or assistance if consulted in accordance with this rule.

(3) The Australian Securities and Investments Commission may disclose information as reasonably necessary in order to provide the Data Recipient Accreditor with advice or assistance if consulted in accordance with this rule.

5.5 Criteria for accreditation—unrestricted level

Note: Under subsection 56CA(1) of the Act, the Data Recipient Accreditor may, in writing, accredit a person if the Data Recipient Accreditor is satisfied that the person meets the criteria for accreditation specified in the consumer data rules. This rule specifies those criteria for the "unrestricted" level of accreditation.

The criterion for accreditation at the "unrestricted" level is that the accreditation applicant:
  (a) would, if accredited, be able to comply with the obligations set out in rule 5.12; or

(b) where a Schedule to these rules sets out criteria for streamlined accreditation in relation to the relevant designated sector—meets those criteria.

Note 1: For paragraph (b), for the banking sector, see clause 7.3 of Schedule 3.

Note 2: See Schedules to these rules for other circumstances in which this provision might operate differently for different designated sectors.

Note 3: For the banking sector, see clause 7.3 of Schedule 3.

5.6 Accreditation decision—accreditation number

The Data Recipient Accreditor must, if it accredits an accreditation applicant, give the applicant a unique number by which it may be identified as an accredited person (their ***accreditation number***).

5.7 Accreditation decision—notifying accreditation applicant

(1) The Data Recipient Accreditor must notify an accreditation applicant, in writing, as soon as practicable after making a decision to accredit, or refuse to accredit, the applicant under subsection 56CA(1) of the Act.

(2) If the Accreditor decided to accredit the applicant, the notice must include the following:
   (a) that fact;
   (b) the level of accreditation;
   (c) any conditions that were imposed when the accreditation decision was made;
   (d) their accreditation number.

Note: For paragraph (c), for conditions on accreditations, see rule 5.10.

(3) If the Accreditor decided not to accredit the applicant, the notice must include the following:
   (a) that fact;
   (b) the applicant's rights to have the decision to refuse reviewed by the Administrative Appeals Tribunal.

5.8 When accreditation takes effect

An accreditation takes effect when the fact that the Data Recipient Accreditor has decided to accredit the person is included in the Register of Accredited Persons.

5.9 Default conditions on accreditation

An accreditation is subject to the conditions set out in Schedule 1.

5.10 Other conditions on accreditation

(1) The Data Recipient Accreditor may, in writing:
  (a) impose any other condition on an accreditation:
    (i) at the time of accreditation under subsection 56CA(1) of the Act; or
    (ii) at any time after accreditation; and
  (b) vary or remove any conditions imposed under this rule.

(2) Before imposing or varying a condition under this rule, the Accreditor must:
  (a) inform the accreditation applicant or accredited person, as appropriate, of the proposed imposition or variation; and
  (b) give the accreditation applicant or accredited person, as appropriate, a reasonable opportunity to be heard in relation to the proposal.

Note 1: Contravention of a condition could lead to suspension or revocation of accreditation: see items 6 and 7 of the table to rule 5.17.

Note 2: Applications may be made to the Administrative Appeals Tribunal to review a decision under this rule: see paragraph 9.2(a).

(3) If the reasons for imposing or varying a condition on an existing accreditation are such that, in the opinion of the Data Recipient Accreditor, complying with subrule (2) would create a real risk of:
  (a) harm or abuse to an individual; or
  (b) adversely impacting the security, integrity or stability of:
    (i) the Register of Accredited Persons; or
    (ii) information and communication technology systems that are used by CDR participants to disclose or collect CDR data;

the Accreditor may impose or vary the condition without complying with that subrule, but must, as soon as practicable, give the accredited person a reasonable opportunity to be heard in relation to the imposition or variation.

(4) A condition imposed under this rule, or a variation of such a condition, must include the time or date on which it takes effect.

Example: A condition could take effect from when the accredited person receives notice of it.

(5) The Accreditor:
  (a) may, but need not, give public notice of a condition or variation imposed or removed under this rule; and
  (b) may do so in any way that the Accreditor thinks fit.

Example: The Accreditor could give public notice of a description of the effect of the conditions, rather than of the conditions themselves.

5.11 Notification to accredited person relating to conditions

(1) The Data Recipient Accreditor must notify the accredited person, in writing, as soon as practicable after the imposition, variation or removal of a condition on an accreditation under rule 5.10.

(2) The notice must include the following:

(a) if a condition is imposed or varied:

(i) the condition or the condition as varied;

(ii) if applicable—the applicant's rights to have the decision reviewed by the Administrative Appeals Tribunal; and

(b) if a condition is removed—that fact.

CONSULTATION DRAFT

Subdivision 5.2.3—Obligations of accredited person

5.12 Obligations of accredited person at the "unrestricted" level

(1) A person who is accredited at the "unrestricted" level must:

(a) take the steps outlined in Schedule 2 which relate to protecting CDR data from:

(i) misuse, interference and loss; and

(ii) unauthorised access, modification or disclosure; and

(b) have internal dispute resolution processes that meet the internal dispute resolution requirements in relation to one or more designated sectors; and

(c) be a member of a recognised external dispute resolution scheme in relation to CDR consumer complaints; and

(d) have addresses for service; and

(e) if the applicant is a foreign entity—have a local agent that has addresses for service.

Note 1: See Schedules to these rules for how this provision might operate differently for different designated sectors.

Note 2: For the banking sector, see clause 7.4 of Schedule 3.

Note 3: For paragraph (a), the steps outlined in Schedule 2 relate to privacy safeguard 12 (see subsection 56EO(1) of the Act and rule 7.11 of these rules).

Note 4: For paragraph (b), see the definition of "meets the internal dispute resolution requirements" in relation to the banking sector in subrule 1.7(1), and see clause 5.1 of Schedule 3.

Note 5: For paragraphs (d) and (e), see rule 1.7 for the meaning of "addresses for service".

Note 6: This subrule is a civil penalty provision (see rule 9.8).

(2) A person who is accredited at the "unrestricted" level must:

(a) be, having regard to the fit and proper person criteria, a fit and proper person to be accredited at that level; and

(b) have adequate insurance, or a comparable guarantee, in light of the risk of CDR consumers not being properly compensated for any loss that might reasonably be expected to arise from a breach of obligations under any of the following to the extent that they are relevant to the management of CDR data:

(i) the Act;

(ii) any regulation made for the purposes of the Act;

(iii) these rules.

5.13 Accredited person must comply with conditions

An accredited person must comply with the conditions of their accreditation.

Note 1: This rule applies to the default conditions set out in Schedule 1 and any conditions imposed or varied under rule 5.10.

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

5.14 Notification requirements

An accredited person must notify the Data Recipient Accreditor within 5 business days if any of the following occurs:

(a) any material change in its circumstances that might affect its ability to comply with its obligations under this Subdivision;

(b) any matter that could be relevant to a decision as to whether the person is, having regard to the fit and proper person criteria, a fit and proper person to be accredited at the person's level of accreditation;

(c) there is a change to, or the accredited person becomes aware of an error in, any of the information provided to the Accreditor to be entered on the Register under rule 5.24.

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

5.15 Provision of information to the Accreditation Registrar

The Data Recipient Accreditor must:

(a) notify the Accreditation Registrar, in writing, as soon as practicable after:

(i) an accreditation; or

(ii) the imposition, variation or removal of a condition on an accreditation; or

(iii) a surrender, suspension or an extension of a suspension; or

(iv) a suspension ceasing to have effect; or

(v) a revocation of an accreditation; or

(vi) a notification under paragraph 5.14(c); and

(b) include in the notice:

(i) any information the Registrar is required to enter into the Register of Accredited Persons; and

(ii) any information the Registrar requires in order to amend an entry in the Register.

Subdivision 5.2.4—Transfer, suspension, surrender and revocation of accreditation

5.16 Transfer of accreditation

An accreditation cannot be transferred.

5.17 Revocation, suspension, or surrender of accreditation

(1) The table has effect:

	Grounds for revocation, suspension and surrender of accreditation as accredited person	
	If:	**the Data Recipient Accreditor:**
1	an accredited person applies to the Data Recipient Accreditor, in writing, to surrender their accreditation;	must, in writing, accept that surrender.
2	the Data Recipient Accreditor is satisfied that an accredited person's accreditation was granted as the result of statements or other information, by the accreditation applicant or by any other person, that were false or misleading in a material particular;	may, in writing: (a) suspend; or (b) revoke; the person's accreditation, as appropriate.
3	subject to items 6 and 7, the Data Recipient Accreditor is satisfied that that the accredited person or an associated person of the accredited person has been found to have contravened a law relevant to the management of CDR data; Note: See rule 1.7 for the meaning of "associated person" and "law relevant to the management of CDR data".	may, in writing: (a) suspend; or (b) revoke; the accredited person's accreditation, as appropriate.

	Grounds for revocation, suspension and surrender of accreditation as accredited person	
	If:	**the Data Recipient Accreditor:**
4	the Data Recipient Accreditor reasonably believes that revocation or suspension is necessary in order to: (a) protect consumers; or (b) protect the security, integrity and stability of: (i) the Register of Accredited Persons or the associated database; or (ii) information and communication technology systems that are used by CDR participants to disclose or collect CDR data; Note: See rule 1.7 for the meaning of "law relevant to the management of CDR data".	may, in writing: (a) suspend; or (b) revoke; the person's accreditation, as appropriate.
5	the following are satisfied: (a) the accredited person was, at the time of the accreditation, an ADI; (b) the accredited person is no longer an ADI for the reason that its authority to carry on banking business is no longer in force;	may, in writing: (a) suspend; or (b) revoke; the person's accreditation, as appropriate.
6	the Data Recipient Accreditor reasonably believes that the accredited person has or may have contravened: (a) an offence provision of the Act or a civil penalty provision of the Act or these rules; or (b) one or more data standards;	may, in writing, suspend the person's accreditation.
7	the accredited person has been found to have contravened: (a) an offence provision of the Act or a civil penalty provision of the Act or these rules; or (b) one or more data standards;	may, in writing: (a) suspend; or (b) revoke; the person's accreditation, as appropriate.
8	the Data Recipient Accreditor is no longer satisfied that the accredited person is, having regard to the fit and proper person criteria, a fit and proper person to be accredited at the person's level of accreditation;	may, in writing: (a) suspend; or (b) revoke; the person's accreditation, as appropriate.

	Grounds for revocation, suspension and surrender of accreditation as accredited person	
	If:	**the Data Recipient Accreditor:**
9	a relevant contract between the accredited person and a CDR consumer has been found to have a term that is unfair;	may, in writing: (a) suspend; or (b) revoke; the person's accreditation, as appropriate.
10	the Data Recipient Accreditor reasonably believes that a relevant contract between the accredited person and a CDR consumer has a term that is unfair;	may, in writing, suspend the person's accreditation.

(2) For items 9 and 10:

(a) ***relevant contract*** means a standard form contract that is a consumer contract or a small business contract within the meaning of section 23 of the Australian Consumer Law that arises from a request by a CDR consumer under subrule 4.3(1); and

(b) ***unfair*** has the meaning given by section 24 of the Australian Consumer Law; and

(c) ***Australian Consumer Law*** has the meaning given by section 130 of the Act.

5.18 Revocation of accreditation—process

(1) Before revoking an accredited person's registration under rule 5.17, the Data Recipient Accreditor must:

(a) inform the accredited person of:

(i) the proposed revocation; and

(ii) when it is proposed to take effect; and

(b) give the accredited person a reasonable opportunity to be heard in relation to the proposed revocation.

(2) If the Accreditor revokes an accredited person's accreditation under rule 5.17, the Accreditor must notify the person, in writing, of the revocation.

Note: The decision to revoke an accredited person's accreditation can be reviewed by the Administrative Appeals Tribunal: see paragraph 9.2(b).

5.19 Suspension of accreditation—duration

(1) Without limitation, the Data Recipient Accreditor, under rule 5.17:
  (a) may suspend an accreditation:
    (i) for a period of time that ends at a specified date; or
    (ii) for a period of time that ends with the occurrence of a specified event; and
  (b) may, subject to the same conditions on which an accreditation was suspended, extend the suspension.

(2) The Data Recipient Accreditor may, in writing, at any time, remove a suspension.

5.20 General process for suspension of accreditation or extension of suspension

(1) This rule applies subject to rule 5.21.

(2) Before suspending an accreditation under rule 5.17, or extending a suspension, the Data Recipient Accreditor must:
  (a) inform the accredited person of:
    (i) the proposed suspension or extension (including the proposed duration); and
    (ii) in the case of a suspension—when it is proposed to take effect; and
  (b) give the accredited person a reasonable opportunity to be heard in relation to the proposed suspension or extension.

(3) If the Accreditor suspends an accredited person's accreditation under rule 5.17, the Accreditor must notify the person, in writing, of the suspension and the period of the suspension.

Note: The decision to suspend an accredited person's accreditation can be reviewed by the Administrative Appeals Tribunal: see paragraph 9.2(b).

(4) If the Accreditor extends a suspension, the Accreditor must notify the person, in writing, of the extension and the period of the suspension as extended.

Note: The decision to extend a suspension can be reviewed by the Administrative Appeals Tribunal: see paragraph 9.2(b).

5.21 Process for urgent suspensions or extensions

(1) This rule applies if:
  (a) the Data Recipient Accreditor proposes to suspend an accreditation, or extend a suspension, on urgent grounds; and
  (b) in the opinion of the Data Recipient Accreditor, because of the urgency, it is not possible to comply with rule 5.20 prior to the suspension or extension.

(2) The Accreditor may suspend the accreditation, or extend the suspension, without first complying with rule 5.20.

(3) However, as soon as practicable after suspending the accreditation or extending the suspension, the Accreditor must:
   (a) inform the accredited person of the suspension or extension; and
   (b) give the accredited person a reasonable opportunity to be heard in relation to whether the suspension should be removed.

5.22 When surrender, revocation or suspension takes effect

A surrender, revocation or suspension takes effect when the fact that the accreditation has been surrendered, revoked or suspended is included in the Register of Accredited Persons.

5.23 Consequences of surrender, suspension or revocation of accreditation

Application of rule

(1) This rule applies if an accredited person's accreditation is surrendered, suspended or revoked.

Ongoing obligations following surrender, suspension or revocation of an accreditation

(2) If the person's accreditation has been surrendered or revoked, the person must comply with the following provisions as if the person still were an accredited data recipient:
   (a) section 56EI of the Act (privacy safeguard 6);
   (b) section 56EJ of the Act (privacy safeguard 7);
   (c) section 56EO of the Act (privacy safeguard 12).

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

(3) The person:
   (a) must not, after the revocation or surrender, or while the accreditation is suspended, seek to collect any, or any further, CDR data under these rules; and
   (b) if the person has collected any CDR data under these rules—must notify each person who has consented to the accredited person collecting CDR data for which they are a CDR consumer:
      (i) that their accreditation has been surrendered, suspended or revoked, as the case may be; and
      (ii) in the case of a suspension—of the following:
         (A) that any consents to collect and to use CDR data may be withdrawn at any time; and

(B) the effect of any such withdrawal.

Note 1: If an accredited person's accreditation is suspended, they remain an accredited person, and continue to be subject to the obligations of an accredited person whose accreditation has not been suspended.

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

(4) If:

(a) the person's accreditation has been surrendered or revoked; and

(b) the person has collected CDR data under these rules; and

(c) the person is not required to retain that CDR data by or under an Australian law or a court/tribunal order; and

(d) the CDR data does not relate to any current or anticipated:

(i) legal proceedings; or

(ii) dispute resolution proceedings;

to which the person is a party; and

(e) where there is a CDR consumer for the CDR data, the CDR data does not relate to any current or anticipated:

(i) legal proceedings; or

(ii) dispute resolution proceedings;

to which the CDR consumer is a party;

the person must delete or de-identify that data by taking the steps specified in rule 7.12 or 7.13, as appropriate.

Note 1: In addition:

- if an accreditation is revoked or surrendered:
  - any consents to collect and use CDR data expire: see subrule 4.14(2); and
  - any authorisations to disclose CDR data expire: see subrule 4.26(2); and
- if an accreditation is suspended, the accredited person is not able to collect data while the suspension is in effect.

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

(5) For the purposes of paragraph (4)(e), if paragraphs (4)(a) to (d) apply in relation to the CDR data of the CDR consumer, the person may:

(a) request the CDR consumer to state whether or not such proceedings are current or anticipated; and

(b) rely on that statement.

Division 5.3—Rules relating to Register of Accredited Persons

5.24 Maintaining the Register of Accredited Persons

The Accreditation Registrar must enter the following details on the Register of Accredited Persons:

(a) the following details about the accredited person:
  (i) the accredited person's name;
  (ii) the accredited person's accreditation number;
  (iii) the accredited person's addresses for service;
  (iv) if the accredited person is a foreign entity—the name and addresses for service of the accredited person's local agent;
(b) the level of the person's accreditation;
(c) either:
  (i) any conditions on the accreditation; or
  (ii) if the Data Recipient Accreditor so directs—a description of the effect of any such conditions;
(d) if the accreditation has been revoked—that fact and the date of the revocation;
(e) if the accreditation has been suspended—that fact and the period of the suspension;
(f) if a decision to suspend an accreditation has been revoked, or the suspension otherwise is no longer in effect:
  (i) that fact; and
  (ii) the date from which the accreditation is once more in effect;
(g) if the accreditation is surrendered—that fact and the date of the surrender;
(h) each brand name under which the accredited person provides goods or services where, in order to provide the good or service, the accredited person needs to access a CDR consumer's CDR data;
(i) a hyperlink to each of the following:
  (i) the relevant web site address of the accredited person;
  (ii) the accredited person's CDR policy;
  (iii) if the accredited person has a CDR policy for a brand name under which the accredited person provides goods or services where, in order to provide the good or service, the accredited person needs to access a CDR consumer's CDR data—that policy.

Note 1: For paragraphs (a), see rule 1.7 for the meaning of "addresses for service".

Note 2: For paragraph (b), the only level of accreditation is the "unrestricted" level.

Note 3: For paragraphs (a) to (g), see rule 5.15.

5.25 Other information to be kept in association with Register of Accredited Persons

(1) The Accreditation Registrar must create and maintain, in association with the Register of Accredited Persons, a database that includes:

(a) a list of data holders; and

(b) for each data holder:

(i) each brand name under which the data holder offers products in relation to which consumer data requests may be made under these rules; and

(ii) a hyperlink to:

(A) the relevant web site address of the data holder; and

(B) the data holder's CDR policy; and

(C) if the data holder has a CDR policy for a brand name under which the data holder offers products in relation which consumer data requests may be made under these rules—that policy; and

(iii) the universal resource identifier for the data holder's product data request service; and

(c) such other information relating to each data holder and each accredited person as the Accreditation Registrar considers is required in order for requests under these rules to be processed in accordance with these rules and the data standards.

Note 1: For subparagraph (b)(i), for the banking sector, see Part 6 of Schedule 3 for the staged application of these rules.

Note 2: For the banking sector, see subclause 6.3(2) of Schedule 3 for additional information to be included.

Accreditation Registrar may request further information

(2) The Accreditation Registrar may:

(a) request a data holder or accredited person to provide the information referred to in subrule (1), or updates to that information; and

(b) specify the form in which the information or updates are to be provided.

(3) The data holder or accredited person must comply with a request under subrule (2).

Civil penalty:

(a) for an individual—$50,000; and

(b) for a body corporate—$250,000.

Obligation to inform Accreditation Registrar to keep information up-to-date

(4) Subrule (5) applies if a data holder or an accredited person:

(a) has provided information to the Accreditation Registrar in accordance with this rule; and

(b) becomes aware that the information:

(i) is out of date; or

(ii) needs to be amended in order for product data requests and consumer data requests made under these rules to be processed in accordance with these rules and the data standards.

(5) The data holder or accredited person, as appropriate, must inform the Accreditation Registrar of the amendment that should be made to the database in the form approved by the Registrar for the purposes of this subrule and as soon as practicable after the data holder or accredited person becomes aware of either of the matters mentioned in paragraph (4)(b).

Civil penalty:

(a) for an individual—$50,000; and

(b) for a body corporate—$250,000.

5.26 Amendment and correction of entries in Register of Accredited Persons and database

The Accreditation Registrar:

(a) must, as soon as practicable after receiving information from the Data Recipient Accreditor that must be entered on the Register, enter that information on the Register; and

(b) must, as soon as practicable after receiving information from the Data Recipient Accreditor that requires the Registrar to update information on the Register, update the Register; and

(c) may, to the extent the Accreditation Registrar considers necessary, amend the database referred to in subrule 5.25(1) to reflect any amendment the Registrar has been informed of in accordance with rule 5.25; and

(d) may make clerical amendments to entries in the Register or database as appropriate to ensure the accuracy of the Register or database.

5.27 Publication or availability of specified information in the Register of Accredited Persons

For paragraph 56CE(4)(c) of the Act, the Accreditation Registrar must, in the manner the Registrar thinks fit, make the following information publicly available:

(a) the information referred to in rule 5.24;

(b) the information referred to in paragraphs 5.25(1)(a) and (b).

Note: For the banking sector, see subclause 6.3(3) of Schedule 3 for other information the Accreditation Registrar must make publicly available.

5.28 Making information available to the Commission, the Information Commissioner and the Data Recipient Accreditor

The Accreditation Registrar must make available to the Commission, the Information Commissioner and the Data Recipient Accreditor, on request:

(a) all or part of the Register of Accredited Persons or the associated database; or

(b) specified information in the Register or the associated database; or

(c) any information held by the Registrar in relation to the Register or the associated database.

5.29 Publication of specified information by the Commission

The Commission may publish information made available to it by the Accreditation Registrar relating to the performance and availability of systems to respond to requests under these rules.

5.30 Other functions of Accreditation Registrar

For paragraph 56CL(1)(b) of the Act, the other functions of the Accreditation Registrar include the following:

(a) enabling information included in the Register of Accredited Persons and associated database to be communicated to data holders and accredited persons to facilitate the making and processing of requests under these rules in accordance with these rules and the data standards;

(b) maintaining the security, integrity and stability of the Register and associated database, including undertaking or facilitating any testing by CDR participants for that purpose;

(c) requesting a data holder or an accredited person to do specified things where that is necessary or convenient in order for the Accreditation Registrar to perform its functions or exercise its powers;

Example: The Accreditation Registrar could request data holders or accredited persons to undertake and complete testing where it is necessary or convenient for the Registrar to perform its functions under paragraph (b).

(d) informing the Data Recipient Accreditor of any failure of an accredited person to comply with a condition of its accreditation or to do things requested by the Registrar in the performance of its functions or the exercise of its powers.

Note: The Accreditation Registrar has the power to do all things necessary or convenient to be done for or in connection with the performance of its functions. See subsection 56CL(2) of the Act.

5.31 Obligation to comply with Accreditation Registrar's request

(1) The Accreditation Registrar may request a data holder or an accredited person to do a specified thing in order to ensure the security, integrity and stability of the Register of Accredited Persons or associated database.

(2) The data holder or accredited person must comply with such a request.

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

5.32 Automated decision-making—Accreditation Registrar

The Accreditation Registrar may automate processes (including decision-making) under these rules.

5.33 Temporary restriction on use of the Register in relation to data holder

(1) The Accreditation Registrar may 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 in order to ensure the security, integrity and stability of the Register or associated database.

(2) The steps taken by the Registrar may include amending the information in the associated database relating to a data holder that is used to facilitate the making and processing of requests.

(3) Before, or as soon as practicable after, taking steps under subrule (1), the Accreditation Registrar must:

(a) inform the data holder of the steps to be taken, or that have been taken; and

(b) give the data holder a reasonable opportunity to be heard in relation to the matter.

(4) Despite anything else in these rules, a data holder is not required to:

(a) ask a CDR consumer to authorise disclosure of CDR data; or

(b) disclose CDR data;

in response to a request, where responding to the request would require the data holder to use 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 steps taken under this rule.

5.34 Temporary direction to refrain from processing consumer data requests

(1) The Accreditation Registrar may, by written notice:

(a) direct an accredited person not to make consumer data requests; or

(b) direct a data holder not to respond to any consumer data requests;

for a period of up to 10 days, if the Accreditation Registrar reasonably believes it is necessary to do so in order to ensure the security, integrity and stability of the Register or associated database.

(2) The notice must specify the period of application.

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

(4) Despite anything else in these rules:

(a) an accredited person must not make a consumer data request contrary to a direction it has received under this rule; and

(b) a data holder must not disclose CDR data in response to a consumer data request contrary to a direction it has received under this rule.

Civil penalty:

(a) for an individual—$50,000; and

(b) for a body corporate—$250,000.

(5) If a data holder is prevented by this rule from disclosing CDR data in response to a consumer data request made under Part 4, the data holder is not required to ask a CDR consumer to authorise the disclosure in accordance with subrule 4.5(3).

Part 6—Rules relating to dispute resolution

6.1 Requirement for data holders—internal dispute resolution

A data holder in relation to a particular designated sector must have internal dispute resolution processes that meet the internal dispute resolution requirements in relation to that sector.

Note 1: See the definition of "meets the internal dispute resolution requirements" in relation to the banking sector in subrule 1.7(1), see and clause 5.1 of Schedule 3.

Note 2: An accredited person must also have internal dispute resolution processes that meet those internal dispute resolution requirements: see paragraph 5.12(1)(b).

Note 3: This rule is a civil penalty provision (see rule 9.8).

6.2 Requirement for data holders—external dispute resolution

A data holder must be a member of a recognised external dispute resolution scheme in relation to CDR consumer complaints.

Note 1: See the definition of "recognised external dispute resolution scheme" in subrule 1.7(1), and see subrule 1.7(3) for the interpretation of references to "data holder".

Note 2: An accredited person must also be a member of such a recognised external dispute resolution scheme: see paragraph 5.12(1)(c).

Note 3: This rule is a civil penalty provision (see rule 9.8).

Part 7—Rules relating to privacy safeguards

Division 7.1—Preliminary

7.1 Simplified outline of this Part

The privacy safeguards are an additional protection given to CDR data under Part IV of the Act. The privacy safeguards apply only to CDR data for which there are one or more CDR consumers (such as required consumer data and voluntary consumer data); they do not apply to CDR data for which there are no CDR consumers (such as required product data and voluntary product data).

Several of the privacy safeguards depend on matters specified in these rules for their operation. This Part sets out the rules that relate to the privacy safeguards.

This Part also sets out some additional civil penalty provisions that protect the privacy or confidentiality of CDR consumers' CDR data.

Division 7.2—Rules relating to privacy safeguards

Subdivision 7.2.1—Rules relating to consideration of CDR data privacy

7.2 Rule relating to privacy safeguard 1—open and transparent management of CDR data

Policy about the management of CDR data

(1) For paragraph 56ED(3)(b) of the Act, the Information Commissioner may approve a form for a CDR policy.

(2) For paragraph 56ED(3)(b) of the Act, a CDR entity's CDR policy must be in the form of a document that is distinct from any of the CDR entity's privacy policies.

Additional information for CDR policy

(3) In addition to the information referred to in subsection 56ED(4) of the Act, a data holder's CDR policy must indicate:
  (a) whether it accepts requests for:
    (i) voluntary product data; or
    (ii) voluntary consumer data; and
  (b) if so:
    (i) whether it charges fees for disclosure of such data; and
    (ii) if it does—how information about those fees can be obtained.

(4) In addition to the information referred to in subsection 56ED(5) of the Act, an accredited data recipient's CDR policy must:
  (a) include a statement indicating the consequences to the CDR consumer if they withdraw a consent to collect and use CDR data; and
  (b) include a list of the outsourced service providers (whether based in Australia or based overseas, and whether or not any is an accredited person); and
  (c) for each such service provider—include:
    (i) the nature of the services it provides; and
    (ii) the CDR data or classes of CDR data that may be disclosed to it; and
  (d) if the accredited data recipient is likely to disclose CDR data of a kind referred to in subsection 56ED(5) of the Act to such a service provider that:
    (i) is based overseas; and
    (ii) is not an accredited person;
  include the countries in which such persons are likely to be based if it is practicable to specify those countries in the policy; and
  (e) if applicable—include the following information about de-identification of CDR data that is not redundant data:

(i) how the accredited person uses CDR data that has been de-identified in accordance with the CDR data de-identification process to provide goods or services to CDR consumers;

(ii) the further information specified in subrule (5); and

(f) include the following information about deletion of redundant CDR data:

(i) when it deletes redundant data;

(ii) how a CDR consumer may elect for this to happen;

(iii) how it deletes redundant data; and

(g) if applicable—include the following information about de-identification of redundant CDR data:

(i) if the de-identified data is used by the accredited data recipient—examples of how the accredited data recipient ordinarily uses de-identified data; and

(ii) the further information specified in subrule (5); and

(h) include the following information about the CDR consumer's election to delete their CDR data:

(i) information about how the election operates and its effect;

(ii) information about how CDR consumers can exercise the election.

Note 1: The specified service providers are the accredited data recipient's "outsourced service providers".

Note 2: For paragraph (d), if the service provider is an accredited person who is based overseas, paragraph 56ED(5)(f) of the Act requires similar information to be contained in the accredited data recipient's CDR policy.

Note 3: This subrule is a civil penalty provision (see rule 9.8).

(5) For subparagraphs (4)(e)(ii) and (g)(ii), the further information is:

(a) how the accredited person de-identifies CDR data, including a description of techniques that it uses to de-identify data; and

(b) if the accredited person ordinarily discloses (by sale or otherwise) de-identified data to one or more other persons:

(i) that fact; and

(ii) to what classes of person it ordinarily discloses such data; and

(iii) why it so discloses such data.

(6) In addition to the information referred to in paragraphs 56ED(4)(b) and (5)(d) of the Act, a CDR participant's CDR policy must include the following information in relation to the participant's internal dispute resolution processes:

(a) where a CDR consumer complaint can be made;

(b) how a CDR consumer complaint can be made;

(c) when a CDR consumer complaint can be made;

(d) when acknowledgement of a CDR consumer complaint can be expected;

(e) what information is required to be provided by the complainant;

(f) the participant's process for handling CDR consumer complaints;

(g) time periods associated with various stages in the CDR consumer complaint process;
(h) options for redress;
(i) options for review, both internally (if available) and externally.

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

(7) If an accredited data recipient proposes to store CDR data other than in Australia or an external territory, its CDR policy must specify any country in which they propose to store CDR data.

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

Availability of policy

(8) For paragraph 56ED(7)(b) of the Act, a CDR participant must make its CDR policy readily available through each online service by means of which the CDR participant ordinarily deals with CDR consumers.

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

(9) For subsection 56ED(8) of the Act, if a copy of a the CDR participant's policy is requested by a CDR consumer, the participant must give the CDR consumer a copy:
(a) electronically; or
(b) in hard copy;
as directed by the consumer.

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

7.3 Rule relating to privacy safeguard 2—anonymity and pseudonymity

For subsection 56EE(3) of the Act, subsection 56EE(1) of the Act does not apply if:
(a) the accredited data recipient is required or authorised by law or by a court/tribunal order to deal with an identified CDR consumer in relation to particular CDR data; or
(b) in relation to particular CDR data, it is impracticable for the accredited data recipient to deal with a CDR consumer that has not been identified.

Subdivision 7.2.2—Rules relating to collecting CDR data

7.4 Rule relating to privacy safeguard 5—notifying of the collection of CDR data

For section 56EH of the Act, an accredited person that collects CDR data in accordance with section 56EF of the Act as a result of a consent from a CDR consumer to collect CDR data must update the person's consumer dashboard as soon as practicable to indicate:

(a) what CDR data was collected; and

(b) when the CDR data was collected; and

(c) the data holder of the CDR data.

Note: See paragraph 1.14(3)(h).

Subdivision 7.2.3—Rules relating to dealing with CDR data

7.5 Meaning of *permitted use or disclosure* and *relates to direct marketing*

***Permitted uses or disclosures** that do not relate to direct marketing*

(1) For this Subdivision, for an accredited data recipient that has collected CDR data under a consumer data request under Part 4 on behalf of a CDR consumer, each of the following is a ***permitted use or disclosure***:

(a) using the CDR consumer's CDR data to provide goods or services requested by the CDR consumer (the ***existing goods or services***):

(i) in compliance with the data minimisation principle; and

(ii) in accordance with a current consent from the CDR consumer, other than a direct marketing consent;

(b) directly or indirectly deriving CDR data from the collected CDR data in order to use the data in accordance with paragraph (a);

(c) for the purpose of providing the existing goods or services, disclosing, to the CDR consumer, any of their CDR data;

(d) disclosing the CDR consumer's CDR data to an outsourced service provider:

(i) for the purpose of doing the things referred to in paragraphs (a) to (c); and

(ii) to the extent reasonably needed to do those things;

(e) disclosing (by sale or otherwise), to any person, CDR data that has been de-identified in accordance with the CDR data de-identification process.

(2) However, none of the uses or disclosures of CDR data referred to in subrule 4.12(3) is a ***permitted use or disclosure***.

Permitted uses or disclosures** that **relate to direct marketing

(3) For this Subdivision, a use or disclosure of the CDR consumer's CDR data that is not itself a permitted use or disclosure under subrule (1) is nevertheless a ***permitted use or disclosure*** that ***relates to direct marketing*** if it consists of one of the following:

(a) in accordance with a direct marketing consent from the CDR consumer—sending to the CDR consumer:

(i) information about upgraded or alternative goods or services to existing goods or services; or

(ii) an offer to renew existing goods or services when they expire; or

(iii) information about the benefits of existing goods or services;

(b) using the CDR data in a way and to the extent that is reasonably needed in order to send to the CDR consumer something permitted under paragraph (a) (including by analysing the CDR data to identify the appropriate information to send);

(c) disclosing the CDR consumer's CDR data to an outsourced service provider:

(i) for the purpose of doing the things referred to in paragraphs (a) or (b); and

(ii) to the extent reasonably needed to do those things.

*Meaning of **direct marketing consent***

(4) In this rule:

direct marketing consent means a consent requested in accordance with subparagraph 4.11(1)(c)(iii).

7.6 Use or disclosure of CDR data by accredited data recipients, outsourced service providers and others

(1) Subject to the Act and these rules, an accredited data recipient that has collected CDR data under a consumer data request under Part 4 made on behalf of a CDR consumer must not use or disclose it, or CDR data directly or indirectly derived from it, other than for a permitted use or disclosure (whether or not one that relates to direct marketing).

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

(2) For the purposes of subrule (1), if CDR data collected by an accredited person, or CDR data directly or indirectly derived from it, is disclosed to another person (the ***recipient***) in accordance with a CDR outsourcing arrangement, any use or disclosure of that CDR data by the recipient (whether or not in accordance with the arrangement) is taken to have been by the accredited person.

(3) For subrule (2), it is irrelevant whether the CDR data was disclosed to the recipient directly by the accredited data recipient, or indirectly through one or more further CDR outsourcing arrangements.

7.7 Rule relating to privacy safeguard 6—use or disclosure of CDR data by accredited data recipients

Note: Paragraph 56EI(1)(b) of the Act provides that an accredited data recipient of CDR data must not use or disclose it unless the use or disclosure is otherwise required, or authorised, under the consumer data rules. This rule provides an authorisation for that paragraph.

Section 56EI of the Act applies only in relation to CDR data for which there are one or more CDR consumers: subsection 56EB(1) of the Act.

For paragraph 56EI(1)(b) of the Act, the use or disclosure of CDR data for which there is a CDR consumer by an accredited data recipient of the CDR data is authorised under these rules if it is a permitted use or disclosure, other than one that relates to direct marketing.

7.8 Rule relating to privacy safeguard 7—use or disclosure of CDR data for direct marketing by accredited data recipients

Note: Paragraph 56EJ(1)(b) of the Act provides that an accredited data recipient of CDR data must not use or disclose it for direct marketing unless the use or disclosure is authorised under the consumer data rules in accordance with a valid consent of a CDR consumer for the CDR data. This rule provides an authorisation for that paragraph.

Section 56EJ of the Act applies only in relation to CDR data for which there are one or more CDR consumers: subsection 56EB(1) of the Act.

For paragraph 56EJ(1)(b) of the Act, the use or disclosure of CDR data for which there is a CDR consumer by an accredited data recipient of the CDR data for direct marketing is authorised under these rules if it is a permitted use or disclosure that relates to direct marketing.

7.9 Rule relating to privacy safeguard 10—notifying of the disclosure of CDR data

For subsection 56EM(1) of the Act, a data holder that discloses CDR data to an accredited person as a result of a consumer data request 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 accredited data recipient.

Note 1: For correction requests, see section 56EP of the Act (privacy safeguard 13) and Subdivision 7.2.5 of these rules.

Note 2: For the banking sector, 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 4.6 of Schedule 3.

Note 3: See paragraph 1.15(3)(f).

Subdivision 7.2.4—Rules relating to integrity and security of CDR data

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

(1) If a data holder makes a disclosure of a kind referred to in paragraphs 56EN(3)(a) and (b) of the Act to an accredited person, the data holder must provide the CDR consumer on whose behalf the disclosure was made, by electronic means, with a written notice that:

(a) identifies the accredited person to whom the CDR data was disclosed; and

(b) states the date of the disclosure; and

(c) identifies the CDR data that was incorrect in the sense referred to in paragraph 56EN(3)(b) of the Act; and

(d) states that:

(i) the CDR consumer can request the data holder to disclose the corrected CDR data to the accredited person; and

(ii) if such a request is made, the corrected CDR data will be so disclosed.

Note 1: For paragraph (d), see subsection 56EN(4) of the Act.

Note 2: The written notice could be given through the data holder's consumer dashboard (see rule 1.15).

(2) A single notice may deal with one or more such disclosures.

(3) The notice must be provided:

(a) as soon as practicable; and

(b) in any event—within 5 business days;

after the CDR participant becomes aware of the matter referred to in paragraph 56EN(3)(b) of the Act.

7.11 Rule relating to privacy safeguard 12—security of CDR data

For subsection 56EO(1) of the Act, the steps are set out in Schedule 2.

Note: Broadly speaking, the steps are for an accredited data recipient of CDR data to:

- define and implement security governance in relation to CDR data; and
- define the boundaries of the CDR data environment; and
- have and maintain an information security capability; and
- implement a formal controls assessment program; and
- manage and report security incidents.

7.12 Rule relating to privacy safeguard 12—de-identification of redundant data

(1) For subsection 56EO(2) of the Act, this rule applies if:

(a) the accredited data recipient, when it asked for consent to collect and use the CDR data, gave the CDR consumer the statement referred to in paragraph 4.17(1)(b) or (c); and

(b) the CDR consumer has not elected, in accordance with rule 4.16, that their redundant data should be deleted; and

(c) in the case of a statement referred to in paragraph 4.17(1)(c)—the accredited person thinks it appropriate in the circumstances to de-identify rather than delete the redundant data.

Note 1: The CDR data de-identification process is set out in rule 1.17.

Note 2: If this rule does not apply, rule 7.13 applies: see subrule 7.13(1).

(2) The steps are:

(a) to apply the CDR data de-identification process to the redundant data; and

(b) direct any outsourced service provider that had been provided with a copy of the redundant data:

(i) either to:

(A) return the redundant data to the accredited data recipient; or

(B) delete the redundant data, as well as any CDR data that has been directly or indirectly derived from it, and notify the accredited data recipient of the deletion; and

(ii) if the outsourced service provider has provided any such data to another person—to:

(A) direct the person to take either of the steps referred to in subparagraph (i) in relation to that data; and

(B) cause similar directions to be made to any person to whom such data has been further disclosed.

Note: If the redundant data cannot be de-identified in accordance with the CDR data de-identification process, it must be deleted in accordance with the CDR data deletion process: see subrule 1.17(4).

7.13 Rule relating to privacy safeguard 12—deletion of redundant data

(1) For subsection 56EO(2) of the Act, this rule applies if rule 7.12 does not apply.

(2) The step is to apply the CDR data deletion process to the redundant data.

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

Subdivision 7.2.5—Rules relating to correction of CDR data

7.14 No fee for responding to or actioning correction request

(1) A data holder must not charge a fee for responding to or actioning a request under subsection 56EP(1) of the Act.

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

(2) An accredited data recipient must not charge a fee for responding to or actioning a request under subsection 56EP(2) of the Act.

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

7.15 Rule relating to privacy safeguard 13—steps to be taken when responding to correction request

The recipient of a request under subsection 56EP(1) or (2) of the Act must:

(a) acknowledge receipt of the request as soon as practicable; and

(b) within 10 business days after receipt of the request, and to the extent that the recipient considers appropriate in relation to the CDR data that was the subject of the request:

(i) correct the data; or

(ii) do both of the following:

(A) include a statement with the data to ensure that, having regard to the purpose for which it is held, the data is accurate, up to date, complete and not misleading;

(B) where practicable, attach an electronic link to a digital record of the data in such a way that the statement will be apparent to any users of the data; and

(c) give the requester a written notice, by electronic means, that:

(i) indicates what the recipient did in response to the request; and

(ii) if the recipient did not think it appropriate to do either of the things referred to in subparagraphs (b)(i) or (ii)—states why a correction or statement is unnecessary or inappropriate; and

(iii) sets out the complaint mechanisms available to the requester.

Note 1: In relation to subparagraph (c)(iii), see Part 6.

Note 2: The written notice could be given through the accredited person's or the data holder's consumer dashboard (see rules 1.14 and 1.15).

Part 8—Rules relating to data standards

Division 8.1—Preliminary

8.1 Simplified outline of this Part

Product data requests and consumer data requests under these rules are made in accordance with data standards, which are made under Division 6 of Part IVD of the Act.

This Part of these rules sets out rules relating to data standards.

The Data Standards Chair is established by the Act and is responsible for making data standards. The Data Standards Chair is required to establish a Data Standards Advisory Committee to advise the Chair about data standards.

This Part also sets out procedural requirements for making, amending and reviewing data standards, and specifies data standards that the Data Standards Chair is required to make. These are all binding data standards.

Division 8.2—Data Standards Advisory Committee

8.2 Establishment of Data Standards Advisory Committee

The Data Standards Chair must, by written instrument, establish and maintain a committee to advise the Chair about data standards (the ***Data Standards Advisory Committee***).

Note: For variation and revocation, see subsection 33(3) of the *Acts Interpretation Act 1901* and paragraph 13(1)(a) of the *Legislation Act 2003*.

8.3 Functions of Data Standards Advisory Committee

The function of the Data Standards Advisory Committee is to advise the Data Standards Chair about:

(a) any matters identified in the instrument establishing the Committee; and

(b) any other matter referred to the Committee by the Chair.

8.4 Appointment to Data Standards Advisory Committee

(1) The Data Standards Chair:

(a) must appoint to the Data Standards Advisory Committee:

(i) 1 or more consumer representatives; and

(ii) 1 or more privacy representatives; and

(b) may appoint others to the Committee as the Chair sees fit.

(2) An appointment must be in writing.

(3) The Chair may determine the terms and conditions of an appointment in writing.

Note: An appointee may be reappointed: see section 33AA of the *Act Interpretation Act 1901* and paragraph 13(1)(a) of the *Legislation Act 2003*.

8.5 Termination of appointment and resignation

(1) The Data Standards Chair may, by writing, terminate an appointment to the Data Standards Advisory Committee at any time.

(2) An appointee to the Committee may resign his or her appointment by giving the Chair a written resignation.

(3) The resignation takes effect on the day it is received by the Chair or, if a later day is specified in the resignation, on that later day.

8.6 Procedural directions

The Data Standards Chair may give the Data Standards Advisory Committee written directions as to:

(a) the way in which the Committee is to carry out its functions; and
(b) procedures to be followed in relation to meetings.

Note: For variation and revocation, see subsection 33(3) of the *Acts Interpretation Act 1901* and paragraph 13(1)(a) of the *Legislation Act 2003*.

8.7 Observers

(1) Any of the following:
(a) the Commission;
(b) the Information Commissioner;
(c) the Department of the Treasury;
may elect to be an observer on the Data Standards Advisory Committee.

(2) The Data Standards Chair may invite any other person to act as an observer on the Committee.

Division 8.3—Reviewing, developing and amending data standards

8.8 Notification when developing or amending data standards

(1) Subject to subrule (2), the Data Standards Chair must notify the Commission and the Information Commissioner, in writing, of a proposal to make or amend a data standard.

(2) If the standard or amendment is urgent, the Chair may instead notify the Commission and the Information Commissioner after it has been made.

(3) A failure to comply with this rule does not affect the validity or enforceability of a data standard or an amendment to a data standard.

8.9 Consultation when developing or amending data standards

(1) This rule does not apply in relation to:
   (a) a data standard or an amendment to a data standard that is made before 1 August 2020; or
   (b) an amendment to a data standard that is, in the opinion of the Data Standards Chair, minor or urgent.

(2) Before making or amending a data standard, the Data Standards Chair must:
   (a) prepare a draft of the proposed standard or amendment (the ***consultation draft***); and
   (b) consult with:
      (i) the Data Standards Advisory Committee; and
      (ii) the Commission; and
      (iii) the Information Commissioner;
      on the consultation draft; and
   (c) cause the consultation draft to be published on the website of the Data Standards Body; and
   (d) invite submissions in relation to the consultation draft from interested members of the public to be made by a specified date that is no earlier than 28 days after the draft is published.

(3) The Data Standards Chair may extend the date for consultation.

(4) A failure to comply with this rule does not affect the validity or enforceability of a data standard or an amendment to a data standard.

8.10 Matters to have regard to when making or amending data standards

When making or amending a data standard, the Data Standards Chair must have regard to the following:
   (a) the advice or submissions (if any) received from:

(i) the Data Standards Advisory Committee; or

(ii) the Commission; or

(iii) the Information Commissioner;

on a draft of the proposed standard or amendment (the ***consultation draft***);

(b) submissions (if any) received during the public consultation (if any) that was undertaken in relation to the consultation draft in accordance with rule 8.9;

(c) any advice from any other relevant committee, advisory panel or consultative group that has been established by the Chair (see paragraph 56FH(2)(a) of the Act).

CONSULTATION DRAFT

Division 8.4—Data standards that must be made

8.11 Data standards that must be made

(1) The Data Standards Chair must make one or more data standards about each of the following:

(a) the processes for:

(i) making and responding to product data requests and consumer data requests; and

(ii) obtaining authorisations and consents, and withdrawal of authorisations and consents;

(b) the collection and use of CDR data, including requirements to be met by CDR participants in relation to seeking consent from CDR consumers;

(c) the disclosure and security of CDR data, including:

(i) authentication of CDR consumers to a standard which meets, in the opinion of the Chair, best practice security requirements; and

(ii) seeking authorisations to disclose CDR data in response to consumer data requests;

(d) the types of CDR data and descriptions of those types, to be used by CDR participants in making and responding to requests;

(e) the formats in which CDR data is to be provided in response to requests;

(f) requirements to be met by CDR participants in relation to:

(i) performance and availability of systems to respond to requests; and

(ii) public reporting of information relating to compliance with those requirements;

(g) the processes for CDR participants to notify other CDR participants of withdrawal of consent or authorisations by CDR consumers;

(h) the provision of administrative or ancillary services by CDR participants to facilitate the management and receipt of communications between CDR participants.

(2) Each such standard must indicate that it is binding and must specify the date on which it commences and the date by which it must be fully complied with.

Note: See sections 56FD and 56FE of the Act for the legal effect of a binding data standard.

(3) The data standards must be subject to such consumer testing as the Data Standards Chair considers appropriate.

Part 9—Other matters

Division 9.1—Preliminary

9.1 Simplified outline of this Part

This Part deals with a range of miscellaneous matters, including:

- decisions that can be reviewed by the Administrative Appeals Tribunal; and
- rules relating to reporting, record-keeping and auditing; and
- civil penalty provisions of the consumer data rules, which are enforced under the enforcement provisions of the Act.

CONSULTATION DRAFT

Division 9.2—Review of decisions

9.2 Review of decisions by the Administrative Appeals Tribunal

Applications may be made to the Administrative Appeals Tribunal to review any of the following decisions:

(a) a decision of the Data Recipient Accreditor under rule 5.10 to:
  (i) impose a condition on an accreditation; or
  (ii) vary a condition that has been imposed;

(b) a decision of the Data Recipient Accreditor under rule 5.17 to:
  (i) suspend an accreditation; or
  (ii) extend a suspension; or
  (iii) revoke an accreditation.

CONSULTATION DRAFT

Division 9.3—Reporting, record keeping and audit

Subdivision 9.3.1—Reporting and record keeping

9.3 Records to be kept and maintained

Records to be kept and maintained—data holder

(1) A data holder must keep and maintain records that record and explain the following:
   (a) authorisations given by CDR consumers to disclose CDR data;
   (b) withdrawals of authorisations to disclose CDR data;
   (c) notifications of withdrawals of consents to collect CDR data;
   (d) disclosures of CDR data made in response to consumer data requests;
   (e) instances where CDR data has not been disclosed in reliance on an exemption from the obligation to disclose CDR data;
   (f) CDR complaint data.

Civil penalty:
   (a) for an individual—$50,000; and
   (b) for a body corporate—$250,000.

Records to be kept and maintained—accredited data recipient

(2) An accredited data recipient must keep and maintain records that record and explain the following:
   (a) consents to collect and use CDR data provided by CDR consumers, including, if applicable, the uses of the CDR data that the CDR consumer has consented to;
   (b) withdrawals of consents by CDR consumers;
   (c) notifications of withdrawals of authorisations received from data holders;
   (d) CDR complaint data;
   (e) collections of CDR data under these rules;
   (f) elections to delete and withdrawals of those elections;
   (g) the use of CDR data by the accredited data recipient;
   (h) the process by which the accredited data recipient asks CDR consumers for their consent, including a video of that process;
   (i) if applicable:
      (i) arrangements that may result in sharing CDR data with outsourced service providers, including copies of agreements with outsourced service providers; and
      (ii) the use and management of CDR data by those providers;
   (j) if CDR data was de-identified in accordance with a consent referred to in paragraph 4.11(3)(e):
      (i) how the data was de-identified; and

(ii) how the accredited data recipient used the de-identified data; and

(iii) if the accredited data recipient disclosed (by sale or otherwise) the de-identified data to another person as referred to in paragraph 4.15(b):

(A) to whom the data was so disclosed; and

(B) why the data was so disclosed;

(k) records that are required to be made for the purposes of the CDR data de-identification process when applied as part of privacy safeguard 12;

(l) records of any matters that are required to be retained under Schedule 2 to these rules;

(m) any terms and conditions on which the accredited data recipient offers goods or services where the accredited data recipient collects or uses CDR data in order to provide the good or service.

Note: For paragraph (k), see section 56EO of the Act and rule 7.12.

Civil penalty:

(a) for an individual—$50,000; and

(b) for a body corporate—$250,000.

Specificity of records

(3) Each record referred to in this rule must include the date and time when the record was made and, if applicable, the date and time when the event described by the record occurred.

Translation of records

(4) Where a record referred to in this rule is kept in a language other than English, an English translation of the record must be made available within a reasonable time to a person who:

(a) is entitled to inspect the records under Subdivision 9.3.2; and

(b) asks for the English translation.

Period for retention of records

(5) Each record referred to in this rule must be kept for a period of 6 years beginning on the day the record was created.

Civil penalty:

(a) for an individual—$50,000; and

(b) for a body corporate—$250,000.

9.4 Reporting requirements

Reports that must be prepared—data holder

(1) A data holder must prepare a report for each reporting period that:

(a) is in the form approved by the Commission for the purposes of this rule; and

(b) summarises the CDR complaint data that relates to that reporting period; and

(c) sets out the number (if any) of:

(i) product data requests; and

(ii) consumer data requests made by eligible CDR consumers; and

(iii) consumer data requests made by accredited persons on behalf of eligible CDR consumers;

received by the data holder during the reporting period; and

(d) sets out:

(i) the number of times the data holder has refused to disclose CDR data; and

(ii) the rule or data standard relied upon to refuse to disclose that data.

Note: For the meaning of ***product data request*** see rule 2.3. For the meaning of ***consumer data request*** see rules 3.3 (requests made by CDR consumers) and 4.4 (requests by accredited persons).

Civil penalty:

(a) for an individual—$50,000; and

(b) for a body corporate—$250,000.

Reports that must be prepared—accredited data recipient

(2) An accredited data recipient must prepare a report for each reporting period that:

(a) is in the form approved by the Commission for the purposes of this rule; and

(b) summarises the CDR complaint data that relates to that reporting period; and

(c) describes any goods or services that they offer to CDR consumers using CDR data that were not:

(i) described in the relevant application to be an accredited person; or

(ii) previously included in a report prepared under this rule; and

(d) in relation to any good or service that is required to be described under paragraph (c):

(i) describes the CDR data that is needed in order to offer the good or service to CDR consumers; and

(ii) explains why that data is needed in order to offer the good or service to CDR consumers; and

(e) describes any material changes that have been made to any goods or services offered by the accredited data recipient since the previous reporting period, including any changes to the matters referred to in paragraph (c); and

(f) sets out the number of consumer data requests made by the accredited data recipient during the reporting period; and

(g) sets out the proportion of CDR consumers who, at the date of the report, had exercised the election to delete, by reference to each brand of the accredited person.

Civil penalty:

(a) for an individual—$50,000; and

(b) for a body corporate—$250,000.

Provision of reports

(3) Each report must be submitted to:

(a) the Commission; and

(b) the Information Commissioner;

within 30 days after the end of each reporting period.

Civil penalty:

(a) for an individual—$50,000; and

(b) for a body corporate—$250,000.

(4) Either the Commission or the Information Commissioner may:

(a) publish any report received under this rule; or

(b) require an accredited data recipient to publish, on its website, a report that it has prepared under subrule (2).

(5) For this rule, the ***reporting periods*** are:

(a) 1 January to 30 June of each year; and

(b) 1 July to 31 December of each year.

9.5 Requests from CDR consumers for copies of records

Requests to data holders of CDR data

(1) A CDR consumer may request a data holder for copies of records relating to the information referred to in paragraphs 9.3(1)(a), (d) and (f) that relates to the CDR consumer.

Requests to accredited data recipients

(2) A CDR consumer may request an accredited data recipient for copies of records relating to the information referred to in paragraphs 9.3(2)(a) and (c) that relates to the CDR consumer.

Form for requests

(3) A request under this rule must be in the form (if any) approved by the Commission for the purposes of this subrule.

Dealing with requests under this rule

(4) A person who receives a request under this rule must provide the requested copies, in the form (if any) approved by the Commission for the purposes of this rule, as soon as practicable, but no later than 10 business days, after receiving the request.

Civil penalty:
(a) for an individual—$50,000; and
(b) for a body corporate—$250,000.

(5) A data holder must not charge a fee for making or responding to a request under subrule (1).

Civil penalty:
(a) for an individual—$50,000; and
(b) for a body corporate—$250,000.

(6) An accredited data recipient must not charge a fee for making or responding to a request under subrule (2).

Civil penalty:
(a) for an individual—$50,000; and
(b) for a body corporate—$250,000.

Subdivision 9.3.2—Audits

9.6 Audits by the Commission and the Information Commissioner

(1) The Commission may, at any time, audit the compliance of any CDR participant with any or all of the following:
   (a) Part IVD of the Act, including Division 5 of Part IVD to the extent that it relates to these rules;
   (b) these rules;
   (c) the data standards.

(2) The Information Commissioner may, at any time, audit the compliance of any CDR participant with any or all of the following:
   (a) the privacy safeguards (Division 5 of Part IVD of the Act);
   (b) these rules to the extent that they relate to:
      (i) the privacy safeguards (see in particular Part 7 of these rules); or
      (ii) the privacy and confidentiality of CDR data.

(3) For the purposes of conducting an audit or otherwise monitoring the compliance of the CDR participant with the provisions mentioned in subrules (1) and (2), the Commission, or the Information Commissioner, may give a CDR participant a written notice that requests the CDR participant to produce, within the time specified in the notice:
   (a) copies of records that are required by this Division to be kept; or
   (b) information from such records.

(4) The CDR participant must comply with a request under subrule (3).

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

9.7 Audits by the Data Recipient Accreditor

(1) The Data Recipient Accreditor may, at any time, audit the compliance of an accredited data recipient with any or all of the following:
   (a) the obligations under rule 5.12;
   (b) any conditions imposed on their accreditation.

(2) For the purposes of conducting an audit or otherwise monitoring the compliance of the CDR participant with the criteria and conditions mentioned in subrule (1), the Data Recipient Accreditor may give an accredited data recipient a written notice that requests the accredited data recipient to produce:
   (a) copies of records that are required by this Division to be kept; or
   (b) information from such records.

(3) The accredited data recipient must comply a request under subrule (2).

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

(4) The Data Recipient Accreditor must provide a copy of any audit report to the Commission and the Information Commissioner.

CONSULTATION DRAFT

Division 9.4—Civil penalty provisions

9.8 Civil penalty provisions

For section 56BL of the Act, the following provisions of these rules are civil penalty provisions (within the meaning of the Regulatory Powers Act):

(a) subrule 1.12(1);
(b) subrule 1.13(1);
(c) subrule 1.14(1);
(d) subrule 1.15(1);
(e) rule 1.16;
(f) subrule 2.4(3);
(g) rule 2.6;
(h) subrule 3.4(3);
(i) subrule 4.3(5);
(j) subrule 4.4(3);
(k) subrule 4.5(2);
(l) subrule 4.5(3);
(m) subrule 4.6(3);
(n) subrule 4.6(4);
(o) subrule 4.13(2);
(p) subrule 4.18(1);
(q) rule 4.19;
(r) subrule 4.20(2);
(s) subrule 4.25(2);
(t) rule 4.27;
(u) subrule 5.12(1);
(v) rule 5.13;
(w) rule 5.14;
(x) subrule 5.23(2);
(y) subrule 5.23(3);
(z) subrule 5.23(4);
(aa) subrule 5.31(2);
(bb) rule 6.1;
(cc) rule 6.2;
(dd) subrule 7.2(4);
(ee) subrule 7.2(6);
(ff) subrule 7.2(7);
(gg) subrule 7.2(8);
(hh) subrule 7.2(9);
(ii) subrule 7.6(1);
(jj) subrule 7.14(1);

(kk) subrule 7.14(2);
(ll) subrule 9.6(4);
(mm) subrule 9.7(3);
(nn) subclause 4.2(1) of Schedule 3;
(oo) subclause 4.2(4) of Schedule 3;
(pp) subclause 4.3(2) of Schedule 3;
(qq) subclause 4.3(3) of Schedule 3;
(rr) clause 4.4 of Schedule 3.

Note: Subrules 2.5(2), 3.5(2), 4.7(3), 5.25(3), 5.25(5), 5.34(4), 9.3(1), 9.3(2), 9.3(5), 9.4(1), 9.4(2), 9.4(3), 9.5(4), 9.5(5) and 9.5(6) are also civil penalty provisions within the meaning of the Regulatory Powers Act.

Schedule 1—Default conditions on accreditations

Part 1—Preliminary

1.1 Purpose of Schedule

This Schedule sets out the default conditions on accreditations, for rule 5.9 of these rules.

Part 2—Default conditions on accreditations

2.1 Ongoing reporting obligation on accredited persons

(1) In this clause:

ASAE followed by a number means the standard with that number issued by the Auditing and Assurance Standards Board of the Australian Government (AUASB).

assurance report means a report on the design, implementation and operating effectiveness of controls over a period of time that:

(a) is made in accordance with ASAE 3150; and

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

attestation statement means a statement in the form of a responsible party's statement on controls and system description that is made in accordance with ASAE 3150.

initial reporting period means:

(a) if the accreditation decision takes effect within 3 months before the end of the financial year—the period starting on the day the accreditation takes effect and ending on the last day of the following financial year;

(b) if the accreditation decision takes effect more than 3 months before the end of the financial year—the period starting on the day the accreditation decision takes effect and ending on the last day of that financial year.

Example 1: For paragraph (a) if an accreditation decision takes effect on 30 May 2020, the initial reporting period starts on 30 May 2020 ends on 30 June 2021.

Example 2: For paragraph (b) if an accreditation decision takes effect on 1 January 2021, the initial reporting period starts on 1 January 2021 and ends on 30 June 2021.

reporting period means any of the initial reporting period and each period of 12 months starting on the day after the end of the previous reporting period.

Attestation statements

(2) The accredited person must provide an attestation statement to the Data Recipient Accreditor within 3 months after the end of:

(a) the initial reporting period; and

(b) every second reporting period thereafter;

that covers the reporting period.

Assurance reports

(3) The accredited person must provide an assurance report to the Data Recipient Accreditor within 3 months after the end of:

(a) the reporting period after the initial reporting period; and

(b) every second reporting period thereafter;

that covers the reporting period.

CONSULTATION DRAFT

Schedule 2—Steps for privacy safeguard 12—security of CDR data held by accredited data recipients

Part 1—Steps for privacy safeguard 12

1.1 Purpose of Part

This Part sets out steps for the purpose of subsection 56EO(1) of the Act, which relate to privacy safeguard 12 (see rule 7.11 and paragraph 5.12(1)(a) of these rules).

Note: An accredited data recipient must take the steps set out in this Schedule to protect CDR data from misuse, interference and loss, and unauthorised access, modification or disclosure, under subsection 56EO(1) of the Act. Subsection 56EO(1) is a civil penalty provision (see section 56EU of the Act).

1.2 Interpretation

In this Schedule:

CDR data environment means the information technology systems used for, and processes that relate to, the management of CDR data.

information security capability, of an accredited data recipient:

(a) means the accredited data recipient's ability to manage the security of its CDR data environment in practice through the implementation and operation of processes and controls; and

(b) includes the accredited data recipient being able to allocate adequate budget and resources, and provide for management oversight.

senior management, of an accredited data recipient that is a body corporate, means:

(a) the accredited data recipient's directors; and

(b) any person who is an associated person, within the meaning of paragraph (a) of the definition of that term, of the accredited data recipient.

1.3 Step 1—Define and implement security governance in relation to CDR data

(1) An accredited data recipient of CDR data must establish a formal governance framework for managing information security risks relating to CDR data setting out the policies, processes, roles and responsibilities required to facilitate the oversight and management of information security.

(2) The accredited data recipient must clearly document its practices and procedures relating to information security and management of CDR data, including the specific responsibilities of senior management.

(3) The accredited data recipient must have and maintain an information security policy that details:
   (a) its information security risk posture setting out the exposure and potential for harm to the accredited data recipient's information assets, including CDR data that it holds, from security threats; and
   (b) how its information security practices and procedures, and its information security controls, are designed, implemented and operated to mitigate those risks.

(4) The accredited data recipient must review and update the framework for appropriateness:
   (a) in response to material changes to both the extent and nature of threats to its CDR data environment and its operating environment; or
   (b) where no such material changes occur—at least annually.

1.4 Step 2—Define the boundaries of the CDR data environment

(1) An accredited data recipient must assess, define and document the boundaries of its CDR data environment.

(2) The accredited data recipient must review the boundaries of its CDR data environment for completeness and accuracy:
   (a) as soon as practicable when it becomes aware of material changes to the extent and nature of threats to its CDR data environment; or
   (b) where no such material changes occur—at least annually.

1.5 Step 3—Have and maintain an information security capability

(1) The accredited data recipient must have and maintain an information security capability that:
   (a) complies with the information security controls specified in Part 2 of this Schedule; and
   (b) is appropriate and adapted to respond to risks to information security, having regard to:
      (i) the extent and nature of threats to CDR data that it holds; and
      (ii) the extent and nature of CDR data that it holds; and
      (iii) the potential loss or damage to one or more CDR consumers if all or part of the consumer's data were to be:
         (A) misused, interfered with or lost; or
         (B) accessed, modified or disclosed without authorisation.

(2) The accredited data recipient must review and adjust its information security capability:

(a) in response to material changes to both the nature and extent of threats and its CDR data environment; or

(b) where no such material changes occur—at least annually.

1.6 Step 4—Implement a formal controls assessment program

(1) An accredited data recipient must establish and implement a testing program to review and assess the effectiveness of its information security capability which:

(a) is appropriate having regard to the factors set out in paragraph 1.5(1)(b); and

(b) requires testing at a frequency, and to an extent, that is appropriate having regard to:

(i) the rate at which vulnerabilities and threats change; and

(ii) material changes to the boundaries of its CDR data environment; and

(iii) the likelihood of failure of controls having regard to the results of previous testing.

(2) The accredited data recipient must monitor and evaluate the design, implementation and operating effectiveness of its security controls relating to the management of CDR data in accordance with its obligations under Part IVD of the Act and these rules, and having regard to the information security controls in Part 2 of this Schedule.

(3) The accredited data recipient must escalate and report to senior management the results of any testing that identifies design, implementation or operational deficiencies in information security controls relevant to its CDR data environment.

(4) The accredited data recipient must ensure that testing is conducted by appropriately skilled persons who are independent from the performance of controls over the CDR data environment.

(5) The accredited data recipient must review the sufficiency of its testing program referred to in subclause (1):

(a) when there is a material change to the nature and extent of threats to its CDR data environment or to the boundaries of its CDR data environment—as soon as practicable; or

(b) where no such material changes occur—at least annually.

1.7 Step 5—Manage and report security incidents

(1) An accredited data recipient must have procedures and practices in place to detect, record, and respond to information security incidents as soon as practicable.

(2) The accredited data recipient must create and maintain plans to respond to information security incidents that it considers could plausibly occur (***CDR data security response plans***).

(3) The accredited data recipient's CDR data security response plans must include procedures for:

(a) managing all relevant stages of an incident, from detection to post-incident review; and

(b) notifying CDR data security breaches to the Information Commissioner and to CDR consumers as required under Part IIIC of the *Privacy Act 1988*; and

(c) notifying information security incidents to the Australian Cyber Security Centre as soon as practicable and in any case no later than 30 days after the accredited data recipient becomes aware of the security incident.

Note: For paragraph (3)(b), see section 56ES of the Act for the extended application of Part IIIC of the *Privacy Act 1988*.

(4) The accredited data recipient must review and test its CDR data security response plans:

(a) when there is a material change to the nature and extent of threats to its CDR data environment or to the boundaries of its CDR data environment—as soon as practicable; and

(b) where no such material changes occur—at least annually.

(5) In this clause:

Australian Cyber Security Centre means the cyber security function within the Australian Signals Directorate.

Part 2—Minimum information security controls

2.1 Purpose of Part

This Part sets out the information security controls, for the purpose of paragraph 1.5(1)(a) of this Schedule.

2.2 Information security controls

The information security controls are set out in the following table:

	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.	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.
		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.
		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.

Schedule 2—Steps for privacy safeguard 12—security of CDR data held by accredited data recipients

	Control requirements	Minimum controls	Description of minimum controls
			Note: In relation to retention, see paragraph 9.3(2)(l) of these rules.
		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 (b) monitoring and review of the appropriateness of user access privileges on at least a quarterly basis.
		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.
		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.
		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.

Schedule 2—Steps for privacy safeguard 12—security of CDR data held by accredited data recipients

	Control requirements	Minimum controls	Description of minimum controls
		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.
2	An accredited data recipient of CDR data must take steps to secure their network and systems within the CDR data environment.	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.
		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.
		Server hardening	Processes are in place to harden servers running applications, databases and operating systems in accordance with accepted industry standards.
		End-user devices	End-user devices, including bring-your-own-device (BYOD) systems, are hardened in accordance with accepted industry standards.

CONSULTATION DRAFT

Schedule 2—Steps for privacy safeguard 12—security of CDR data held by accredited data recipients

	Control requirements	Minimum controls	Description of minimum controls
3	An accredited data recipient must securely manage information assets within the CDR data environment over their lifecycle.	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.
		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.
		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 management	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.

Schedule 2—Steps for privacy safeguard 12—security of CDR data held by accredited data recipients

	Control requirements	Minimum controls	Description of minimum controls
	program to identify, track and remediate vulnerabilities within the CDR data environment in a timely manner.	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.
		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.	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.
		Web and email content filtering	Solutions are implemented to identify, quarantine and block suspicious content arising from email and the web.
		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	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.

Schedule 2—Steps for privacy safeguard 12—security of CDR data held by accredited data recipients

	Control requirements	Minimum controls	Description of minimum controls
	information security training and awareness program for all personnel interacting with CDR data.		
		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.
		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.

Schedule 3—Provisions relevant to the banking sector

Part 1—Preliminary

1.1 Simplified outline of this Schedule

This Schedule deals with how these rules apply in relation to the banking sector.

Some defined terms apply only in relation to the banking sector. These are defined in Part 1 of this Schedule.

Part 2 of this Schedule deals with eligible CDR consumers in relation to the banking sector.

Part 3 of this Schedule deals with CDR data that can or must be disclosed when product data requests and consumer data requests are made in relation to the banking sector.

Part 4 of this Schedule deals with joint accounts within the banking sector.

Part 5 of this Schedule deals with internal dispute resolution requirements in relation to the banking sector.

Part 6 of these rules deals with the staged application of these rules to the banking sector. Over time, as set out in this Part, these rules will apply to a progressively broader range of data holders within the banking sector, and to a progressively broader range of banking products.

Part 7 deals with provisions of these rules that apply differently in relation to the banking sector.

1.2 Interpretation

In this Schedule:

account data has the meaning given by clause 1.3 of this Schedule.

accredited ADI has the meaning given by clause 6.2 of this Schedule.

any other relevant ADI has the meaning given by clause 6.2 of this Schedule.

associate has the meaning given by the banking sector designation instrument.

banking business has the meaning given by the banking sector designation instrument.

banking sector means the sector of the Australian economy that is designated by the banking sector designation instrument.

banking sector designation instrument means the *Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019* as in force from time to time.

customer data has the meaning given by clause 1.3 of this Schedule.

foreign ADI has the meaning given by the *Banking Act 1959*.

initial data holder has the meaning given by clause 6.2 of this Schedule.

joint account means a joint account with a data holder for which there are 2 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.

joint account management service has the meaning given by subclause 4.2(3) of this Schedule.

phase 1 product has the meaning given by clause 1.4 of this Schedule.

phase 2 product has the meaning given by clause 1.4 of this Schedule.

phase 3 product has the meaning given by clause 1.4 of this Schedule.

product has the meaning given by the banking sector designation instrument.

product specific data has the meaning given by clause 1.3 of this Schedule.

transaction data has the meaning given by clause 1.3 of this Schedule.

voluntarily participating ADI has the meaning given by clause 6.2 of this Schedule.

1.3 Meaning of *customer data, account data, transaction data* and *product specific data*

For this Schedule, a term listed in column 1 of the table has the meaning given by column 2.

Meaning of *customer data, account data, transaction data* and *product specific data*

	Column 1	Column 2
1	***customer data***, in relation to a particular person	(a) means information that identifies or is about the person; and (b) includes: (i) the person's name; and (ii) the person's contact details, including their: (A) telephone number; and

Schedule 3—Provisions relevant to the banking sector

Meaning of *customer data, account data, transaction data* and *product specific data*		
Column 1	**Column 2**	
		(B) email address; and (C) physical address; and (iii) any information that: (A) the person provided at the time of acquiring a particular product; and (B) relates to their eligibility to acquire that product; and (iv) if the person operates a business—the following: (A) the person's business name; (B) the person's ABN (within the meaning of the *A New Tax System (Australian Business Number) Act 1999*); (C) the person's ACN (within the meaning of the *Corporations Act 2001*); (D) the type of business; (E) the date the business was established; (F) the registration date; (G) the organisation type; (H) the country of registration; (I) whether the business is a charitable or not-for-profit organisation; and (c) if the person is an individual—does not include the person's date of birth.
2	***account data***, in relation to a particular account	(a) means information that identifies or is about the operation of the account; and (b) includes: (i) the account number, other than to the extent that an account number is masked (whether as required by law or in accordance with any applicable standard or industry practice); and (ii) the account name; and (iii) account balances; and (iv) any authorisations on the account, including: (A) direct debit deductions, including, to the extent available: (I) identifying information for the merchant or party that has debited the account; and (II) the amount the merchant or party has debited on the last occasion; and (III) the date the merchant or party has debited the account; and

Schedule 3—Provisions relevant to the banking sector

Meaning of *customer data, account data, transaction data* and *product specific data*			
	Column 1	**Column 2**	
			(B) scheduled payments (for example, regular payments, payments to billers and international payments); and (C) details of payees stored with the account, such as those entered by the customer in a payee address book.
3	***transaction data***, in relation to a particular transaction	(a)	means information that identifies or describes the characteristics of the transaction; and
		(b)	includes: (i) the date on which the transaction occurred; and (ii) any identifier for the counter-party to the transaction; and (iii) if the counter-party is a merchant—any information that was provided by the merchant in relation to the transaction; and (iv) the amount debited or credited pursuant to the transaction; and (v) any description of the transaction; and (vi) the "simple categorisation" of the transaction (for example, whether the transaction is a debit, a credit, a fee or interest).
4	***product specific data***, in relation to a particular product	(a)	means information that identifies or describes the characteristics of the product; and
		(b)	includes the following data about the product: (i) its type; (ii) its name; (iii) its price, including fees, charges and interest rates (however described); (iv) associated features and benefits, including discounts and bundles; (v) associated terms and conditions; (vi) customer eligibility requirements.

1.4 Meaning of *phase 1 product, phase 2 product* and *phase 3 product*

For this Schedule, the table has effect:

Schedule 3—Provisions relevant to the banking sector

Meaning of *phase 1 product, phase 2 product* and *phase 3 product*		
	The following term:	**means a product that is publicly offered and is generally known as being of any of the following types:**
1	***phase 1 product***	(a) a savings account; (b) a call account; (c) a term deposit; (d) a current account; (e) a cheque account; (f) a debit card account; (g) a transaction account; (h) a personal basic account; (i) a GST or tax account; (j) a personal credit or charge card account; (k) a business credit or charge card account.
2	***phase 2 product***	(a) a residential home loan; (b) a home loan for an investment property; (c) a mortgage offset account; (d) a personal loan.
3	***phase 3 product***	(a) business finance; (b) a loan for an investment; (c) a line of credit (personal); (d) a line of credit (business); (e) an overdraft (personal); (f) an overdraft (business); (g) asset finance (including leases); (h) a cash management account; (i) a farm management account; (j) a pensioner deeming account; (k) a retirement savings account; (l) a trust account; (m) a foreign currency account; (n) a consumer lease.

Part 2—Eligible CDR consumers—banking sector

2.1 Meaning of *eligible*—banking sector

(1) This clause is made for the purposes of the definition of ***eligible*** in subrule 1.7(1) of these rules.

(2) For the banking sector, in relation to a particular data holder at a particular time, a CDR consumer is ***eligible*** if, at that time the CDR consumer:

(a) is an individual who is 18 years of age or older; and

(b) is the account holder for an account with the data holder that:

(i) is open; and

(ii) is set up in such a way that it can be accessed online.

Part 3—CDR data that may be accessed under these rules—banking sector

3.1A Application of Part

This Part applies in relation to:

(a) phase 1 products; and

(b) phase 2 products; and

(c) phase 3 products.

Note: See Part 6 of this Schedule for the staged application of these rules to the banking sector. CDR data relating to different phase products will become available at different times, in accordance with that Part.

3.1 Meaning of *required product data* and *voluntary product data*—banking sector

(1) For these rules, ***required product data***, in relation to the banking sector, means CDR data for which there are no CDR consumers:

(a) that is within a class of information specified in the banking sector designation instrument; and

(b) that is about the eligibility criteria, terms and conditions, price, availability or performance of a product; and

(c) in the case where the CDR data is about availability or performance—that is publicly available; and

(d) that is product specific data about a product; and

(e) that is held in a digital form.

Note: Paragraphs (b) and (c) are based on subsection 56BF(1) of the Act.

(2) For these rules, ***voluntary product data***, in relation to the banking sector, means CDR data for which there are no CDR consumers:

(a) that is within a class of information specified in the banking sector designation instrument; and

(b) that is product specific data about a product; and

(c) that is not required product data.

3.2 Meaning of *required consumer data* and *voluntary consumer data*—banking sector

(1) For these rules, subject to this clause, ***required consumer data***, in relation to the banking sector, means CDR data for which there are one or more CDR consumers:

(a) that is within a class of information specified in the banking sector designation instrument; and

(b) that is:

(i) customer data in relation to a CDR consumer; or

(ii) account data in relation to an account (whether or not the account can be accessed online, and whether or not open) that:

(A) is held by a CDR consumer who is an individual:

(I) in their name alone; or

(II) jointly with 1 other individual; and

(B) is available through the data holder's primary retail banking channel in relation to the brand of the account; or

(iii) transaction data in relation to a transaction on any such account; or

(iv) product specific data in relation to a product that a CDR consumer uses; and

(c) that is held by the data holder in a digital form.

Note 1: For subparagraph (b)(ii), consumer data requests cannot be made under these rules in relation to any other kinds of joint accounts.

Note 2: For subparagraph (b)(iv), for a consumer data request, product specific data could include the following:

- any product prices that were negotiated individually with a CDR consumer;
- the interest rates that are current at the time of the request, as well as any other interest rates applicable to the product, and any terms and conditions associated with those interest rates;
- any features and benefits negotiated individually with a CDR consumer.

Note 3: So long as the CDR consumer is eligible to make a consumer data request in relation to a particular data holder, they will be able to make or cause to be made a consumer data request that relates to any account they have with the data holder, including closed or accounts that cannot be accessed online.

Note 4: A person is not a data holder of CDR data that was held by or on behalf of them before the earliest holding day (see paragraph 56AJ(1)(b) of the Act). Accordingly, such data cannot be requested under these rules.

(2) For these rules, subject to this clause, CDR data is ***voluntary consumer data*** in relation to the banking sector if:

(a) there is a CDR consumer for the CDR data; and

(b) the CDR data is not required consumer data.

(3) For this clause:

(a) CDR data is neither ***required consumer data*** nor ***voluntary consumer data*** at a particular time if the data is:

(i) account data in relation to an account that is neither of the following:

(A) an account held in the name of a single individual;

(B) a joint account; or

(ii) account data in relation to a joint account for which any of the joint account holders is less than 18 years of age at that time; or

(iv) transaction data in relation to a transaction on any such account; or

(v) product specific data in relation to a product relating to any such account; and

(b) for a particular joint account holder, customer data in relation to the other joint account holder is neither ***required consumer data*** nor ***voluntary consumer data***.

(4) Despite subclause (1), CDR data is not ***required consumer data*** at a particular time if the data is:

(a) transaction data in relation to a transaction:

(i) on an account that is open at that time; and

(ii) that occurred more than 7 years before that time; or

(b) transaction data in relation to a transaction on an account that:

(i) is closed at that time; and

(ii) was closed more than 24 months before that time; or

(c) transaction data in relation to a transaction:

(i) on an account that:

(A) is closed at that time; and

(B) was closed no more than 24 months before that time; and

(ii) that occurred more than 12 months before the account was closed; or

(d) account data that relates to an authorisation on an account for direct debit deductions, where:

(i) the account is open at that time; and

(ii) the direct debit deduction occurred more than 13 months before that time; or

(e) account data that relates to an authorisation on an account for direct debit deductions, where the account is closed at that time.

Part 4—Joint accounts

Division 4.1—Preliminary

4.1 Purpose of Part

These rules apply differently in relation to joint accounts within the banking sector. This Part sets out how the rules apply in relation to such accounts.

4.2 Joint account management service

(1) A data holder that could be required to disclose CDR data that relates to a joint account must provide a service for joint accounts with the data holder that can be used:

(a) by both of the joint account holders together to jointly elect, to the satisfaction of the data holder, that each joint account holder will individually be able to:

(i) make consumer data requests directly to the data holder for information that relates to the joint account; and

(ii) give authorisations to disclose CDR data in response to consumer data requests for information that relates to the joint account that are made by accredited persons; and

(iii) revoke such authorisations, whether given by themselves or by the other joint account holder; and

(b) by either of the joint holders individually to revoke, to the satisfaction of the data holder, such an election.

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

(2) The service may, but need not:

(a) be online; and

(b) include a functionality that permits the joint account holders to:

(i) elect, to the satisfaction of the data holder, that both joint account holders will be able to perform the tasks referred to in subparagraphs (1)(a)(i), (ii) and (iii) together; and

(ii) revoke, to the satisfaction of the data holder, such an election.

(3) Such a service is a ***joint account management service***.

Note: If no election is made on a particular joint account, it will not be possible to make consumer data requests for CDR data relating to the account under these rules.

(4) If an election is made on a joint account management service, the data holder must give effect to the election as soon as practicable.

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

Division 4.2—Operation of these rules in relation to joint accounts

4.3 Exception to the requirement to seek authorisation and to disclose

(1) This clause applies to required consumer data or voluntary consumer data that was requested under a consumer data request under Part 3 or Part 4 of these rules if:

(a) the data relates to a joint account; and

(b) either:

(i) at the time the request was made, there was no current election as described in clause 4.2 of this Schedule; or

(ii) there was a current election, but the request did not accord with the election.

Note: If there is no current election as described in clause 4.2 of this Schedule, consumer data requests cannot be made for CDR data relating to the joint account.

Example: For subparagraph (1)(b)(ii), if the joint account holders had elected that both together would be able to make consumer data requests directly to the data holder, and the request was made by one of the joint account holders on their own, the request would not accord with the election.

(2) The data holder must not disclose the data in relation to which this clause applies.

Note 1: This clause does not prevent a data holder from disclosing any other CDR data that might have been requested at the same time but to which this clause does not apply.

Note 2: This subclause is a civil penalty provision (see rule 9.8 of these rules).

(3) For a request under Part 4 of these rules, the data holder must not seek authorisations to disclose that data.

Note: This subclause is a civil penalty provision (see rule 9.8 of these rules).

4.4 Consumer dashboard for joint accounts—data holder

If, for a particular joint account with a data holder:

(a) the election referred to in paragraph 4.2(1)(a) of this Schedule, or paragraph 4.2(2)(b) of this Schedule (if offered by the data holder), has been made; and

(b) the data holder provides a joint account holder with a consumer dashboard in accordance with subrule 1.15(1) of these rules;

the data holder must also provide an equivalent consumer dashboard to the other joint account holder.

Note: A data holder is required to provide consumer dashboards only if a consumer data request is made by an accredited person. Such requests are made under Part 4 of these rules.

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

4.5 Seeking authorisation to share CDR data—joint accounts

(1) This clause applies to required consumer data or voluntary consumer data that was requested under a consumer data request under Part 4 of these rules if:

(a) the data relates to a joint account; and

(b) the request was pursuant to a current election under paragraph 4.2(2)(b) of this Schedule (if offered by the data holder); and

(c) there was no current election referred to in subparagraph 4.2(1)(a)(ii) of this Schedule.

(2) Subrules 4.5(2) and (3) of these rules apply as if the reference to "the CDR consumer on whose behalf the request was made" were a reference to each joint account holder in relation to which there is no current authorisation to disclose the data to which this clause applies.

4.6 Exception to rule 7.9—physical or financial harm or abuse

Rule 7.9 of these rules does not apply if:

(a) a data holder discloses CDR data to an accredited person as a result of a consumer data request that was made by a joint account holder of a joint account; and

(b) the data holder considers it necessary, in order to prevent physical or financial harm or abuse, not to update the consumer dashboard of the other joint account holder to indicate the matters referred to in paragraphs 7.9(a), (b) and (c).

Part 5—Internal dispute resolution—banking sector

Note: See the definition of "meets the internal dispute resolution requirements" in subrule 1.7(1) of these rules, paragraph 5.12(b) of these rules, and rule 6.1 of these rules.

5.1 Internal dispute resolution—banking sector

(1) For the banking sector, a CDR participant ***meets the internal dispute resolution requirements*** if its internal dispute resolution processes comply with provisions of Regulatory Guide 165 that deal with the following:

(a) guiding principles or standards that its internal dispute resolution procedures or processes must meet regarding the following:

(i) commitment and culture;

(ii) the enabling of complaints;

(iii) resourcing;

(iv) responsiveness;

(v) objectivity;

(vi) fairness;

(vii) complaint data collection or recording;

(viii) internal reporting and analysis of complaint data;

(b) outsourcing internal dispute resolution procedures;

(c) the manner in which, and timeframes within which, it should acknowledge, respond to and seek to resolve complaints;

(d) multi-tiered internal dispute resolution procedures;

(e) tailoring internal dispute resolution procedures to its business;

(f) documenting internal facing internal dispute resolution processes, policies and/or procedures;

(g) establishing appropriate links between internal dispute resolution and external dispute resolution;

as if references in Regulatory Guide 165 to:

(h) complaints or disputes were references to CDR consumer complaints; and

(i) financial firms and financial service providers were references to CDR participants.

(2) In this clause:

Regulatory Guide 165 means Regulatory Guide 165 published by the Australian Securities & Investments Commission, as in force from time to time.

Note: Regulatory Guide 165 could in 2020 be accessed from the Australian Securities & Investments Commission's website (https://asic.gov.au).

Part 6—Staged application of these rules to the banking sector

Division 6.1—Preliminary

6.1 Interpretation

In this Part:

commencement table has the meaning given by clause 6.6.

brand request to an initial data holder means a product data request or a consumer data request that relates to a product that is marketed under:

(a) the name of the initial data holder as given by item 1 of the table to clause 6.2; or

(b) the name in brackets next to that name; or

(c) a name similar to either of those names.

non-brand request to an initial data holder means a product data request or a consumer data request to an initial data holder that is not a brand request.

Phase 1 means phase 1 product.

Phase 2 means phase 2 product.

Phase 3 means phase 3 product.

6.2 Meaning of *initial data holder, accredited ADI, voluntarily participating ADI, any other relevant ADI* and *accredited non-ADI*

For this Part, a term listed in column 1 of the table has the meaning given by column 2.

Meaning of *initial data holder, accredited ADI, voluntarily participating ADI, any other relevant ADI* and *accredited non-ADI*

	Column 1	Column 2
1	***initial data holder***	Any of the following ADIs: (a) Australia and New Zealand Banking Group Limited (ANZ); (b) Commonwealth Bank of Australia (CBA); (c) National Australia Bank Limited (NAB); (d) Westpac Banking Corporation (Westpac).
2	***accredited ADI***	An ADI that: (a) is an accredited person; and

Schedule 3—Provisions relevant to the banking sector

Meaning of *initial data holder, accredited ADI, voluntarily participating ADI, any other relevant ADI* and *accredited non-ADI*

	Column 1	Column 2
		(b) is not: (i) an initial data holder; or (ii) a foreign ADI; or (iii) a foreign branch of a domestic bank. Note: A restricted ADI could be an "accredited ADI". However, a restricted ADI could not be an "initial data holder", a "voluntarily participating ADI" or "any other relevant ADI".
3	***voluntarily participating ADI***	An ADI, other than an accredited ADI: (a) that has given the Accreditation Registrar a notification in accordance with subclause 6.3(1) of this Schedule; and (b) whose entry in the Register of Accredited Persons has been updated in to indicate that it is a voluntarily participating ADI.

4	***any other relevant ADI***	An ADI that is not: (a) an initial data holder; or (b) a voluntarily participating ADI; or (c) an accredited ADI; or (d) a foreign ADI; or (e) a foreign bank branch of a domestic bank; or (f) a restricted ADI.
5	***accredited non-ADI***	An accredited person that is: (a) a data holder; but (b) not an ADI.

6.3 Election to voluntarily participate in CDR scheme early

(1) An ADI that:

(a) is a data holder; and

(b) is not:

(i) an initial data holder; or

(ii) a restricted ADI;

may notify the Accreditation Registrar, in writing, that it is electing to be treated as a voluntarily participating ADI.

Note 1: Such an ADI is a "voluntarily participating ADI": see Division 6.2 of this Schedule for how these rules apply in relation to such an ADI.

Note 2: Voluntarily participating ADIs are required to deal with consumer data requests under Part 3 and Part 4 of these rules earlier than they would otherwise have been required, in accordance with the commencement table: see clause 6.6.

They are not required to deal with product data requests made under Part 2 of these rules earlier than they would otherwise have been required. However, they are authorised to disclose product data in advance of being required to do so: see clause 6.5.

Note 3: If a "voluntarily participating ADI" is accredited under section 56CA of the Act, it will become an "accredited ADI", and will no longer be a "voluntarily participating ADI".

(2) For each ADI that makes such a notification, the Accreditation Registrar must include the notification on the Register of Accredited Persons, in association with the information referred to in paragraphs 5.25(1)(a) and (b) of these rules.

(3) For paragraph 56CE(4)(c) of the Act, the Accreditation Registrar must, in the manner the Registrar thinks fit, make the notification publicly available.

Note: See also rule 5.27 of these rules.

Division 6.2—Staged application of rules

6.4 Staged application of rules—requirement to disclose CDR data

(1) This clause applies if:

(a) a product data request or a consumer data request of a type referred to in column 1 of the commencement table is made to a data holder; and

(b) the request is made under a Part of these rules referred to in column 2 of the commencement table; and

(c) the request is made after the commencement of these rules and during a period referred to in any of columns 3 to 9 of the commencement table.

(2) Despite clause 3.1A of this Schedule, for the request, Part 3 of this Schedule applies in relation to the kinds of product referred to in the relevant cell of the commencement table.

(3) Where a table cell refers to this subclause, 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) joint accounts;

(ii) closed accounts;

(iii) direct debits;

(iv) scheduled payments;

(v) payees; or

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

6.5 Authorisation to disclose CDR data before required to do so

For these rules, at a particular time, a data holder is authorised to disclose any required CDR data or voluntary CDR data that it is not required, at that time, to disclose.

Note: The data holder might be subject to an obligation to comply with a request from the Accreditation Registrar under rule 5.31 in relation to disclosure of CDR data as authorised by this clause.

6.6 Commencement table

Note: This consultation draft does not include amendments relating to changes in the staged commencement process. These will be addressed separately by the Commission.

For this Part, the ***commencement table*** is:

Column 1	Column 2	Column 3	Column 4	Column 5	Column 6	Column 7	Column 8	Column 9
Type of request	**Part of these rules**	**1/2/20 to 30/6/20**	**1/7/20 to 31/10/20**	**1/11/20 to 31/1/21**	**1/2/21 to 30/6/22**	**1/7/21 to 31/1/22**	**1/2/22 to 30/6/22**	**from 20/6/22**
A brand request to an initial data holder	Part 2	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
	Part 3	–	–	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
	Part 4	–	Phase 1 (see sc 6.4(3))	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
A non-brand request to an initial data holder; or a request to any other relevant ADI	Part 2	–	Phase 1	Phase 1	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
	Part 3	–	–	–	–	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
	Part 4	–	–	–	Phase 1 (see sc 6.4(3))	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
A request to a voluntarily participating ADI	Part 2	–	Phase 1	Phase 1	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
	Part 3	–	–	–	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
	Part 4	–	–	Phase 1	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
A request to an accredited ADI;	Part 2	–	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3

Schedule 3—Provisions relevant to the banking sector

Column 1	Column 2	Column 3	Column 4	Column 5	Column 6	Column 7	Column 8	Column 9
Type of request	**Part of these rules**	**1/2/20 to 30/6/20**	**1/7/20 to 31/10/20**	**1/11/20 to 31/1/21**	**1/2/21 to 30/6/22**	**1/7/21 to 31/1/22**	**1/2/22 to 30/6/22**	**from 20/6/22**
or a request to an accredited non-ADI	Part 3	–	–	–	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
	Part 4	–	–	Phase 1	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3

Part 7—Other rules, and modifications of these rules, for the banking sector

7.1 Laws relevant to the management of CDR data—banking sector

For paragraph (f) of the definition of "law relevant to the management of CDR data" in rule 1.7 of these rules, the *Australian Securities and Investments Commission Act 2001* is a law relevant to the management of CDR data in relation to the banking sector.

7.2 Conditions for accredited person to be data holder

(1) For paragraph 56AJ(4)(c) of the Act, this clause sets out conditions for a person that has collected CDR data in accordance with a consumer data request under Part 4 of these rules to be a data holder (rather than an accredited data recipient) of that CDR data and any CDR data that it directly or indirectly derived from that CDR data (together, the ***relevant*** CDR data**)**.

(2) The conditions are that:
- (a) the person is an ADI; and
- (b) the CDR consumer has acquired a product from the person; and
- (c) the person:
  - (i) reasonably believes that the relevant CDR data is relevant to its provision of the product to the CDR consumer; and
  - (ii) has asked the CDR consumer to agree to the person being a data holder, rather than an accredited data recipient, of the relevant CDR data; and
  - (iii) has explained to the CDR consumer:
    - (A) that, as a result, the privacy safeguards, to the extent that they apply to an accredited data recipient of CDR data, would no longer apply to the person in relation to the relevant CDR data; and
    - (B) the manner in which it proposes to treat the relevant CDR data; and
    - (C) why it is entitled to provide the CDR consumer with this option; and
  - (iv) has outlined the consequences, to the CDR consumer, of not agreeing to this; and
- (d) the CDR consumer has agreed to the person being a data holder, rather than an accredited data recipient, of the relevant CDR data.

Related modifications of these rules

(3) If 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 this clause:
   (a) for paragraph 4.14(1)(f) of these rules, any consents to collect CDR data under the consumer data request expire; and
   (b) for paragraph 4.26(1)(h) of these rules, any authorisations to disclose CDR data in relation to the consumer data request expire; and
   (c) if the person's accreditation has been surrendered or revoked, the following do not apply to the person in relation to that CDR data:
      (i) subrule 5.23(2);
      (ii) paragraph 5.23(3)(b).

7.3 Streamlined accreditation—banking sector

For paragraph 5.5(b) of these rules, for the banking sector, the criteria for streamlined accreditation are that the accreditation applicant:
   (a) is an ADI; but
   (b) is not a restricted ADI.

7.4 Exemptions to accreditation criteria—banking sector

(1) This clause sets out how the accreditation criteria operate in relation to the banking sector, for the purposes of rule 5.12 of these rules.

(2) An accredited person that:
   (a) is an ADI; but
   (b) is not a restricted ADI;

need not comply with paragraph 5.12(2)(b) of these rules.