Competition and Consumer (Consumer Data) Rules 2019

The Australian Competition and Consumer Commission makes the following rules.

Dated

EXPOSURE DRAFT

29 MARCH 2019

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) Rules 2019*.

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	1 July 2019	1 July 2019

Note: This table relates only to the provisions of this instrument as originally made.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

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 can be used by that person as they see fit.

Consumer data requests made by CDR consumers

A CDR consumer 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. The data can be used by the CDR consumer as they see fit.

Consumer data requests made on behalf of CDR consumers

A CDR consumer 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 is 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 under a CDR contract with the 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 2 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 definitions of terms that are used in these rules. The other provisions of these rules should be read together with these definitions. 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.

(4) Part 4 of these rules deals with consumer data requests that are made by accredited persons on behalf of 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 privacy safeguards. The rules set out in this Part should be read in conjunction with Division 5 of Part IVD of the Act.

(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.

(10) Schedule 1 to these rules sets out detailed steps for privacy safeguard 12 (subsection 56EO(1) of the Act and subrule 7.8(1) of these rules). These steps are

also relevant to outsourced service providers (see subrule 4.8(3)) and are an element of the ongoing obligations of persons accredited at the "unrestricted" level (see paragraph 5.11(b)).

(11) Other Schedules to these rules contain provisions that are relevant to particular designated sectors. Schedule 2 contains details that are relevant to the banking sector, and sets out the specific CDR data in respect of which requests under these rules may be made. Schedule 2 deals with the progressive application of these rules. 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;
- binding data standard;
- CDR consumer;
- CDR data;
- CDR participant;
- collects;
- 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:

Act means the *Competition and Consumer Act 2010*.

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

accredited person request service has the meaning given by subrule 1.12(3).

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 means the following:

(a) the number of CDR consumer complaints received;

(b) the number of CDR consumer complaints resolved through internal dispute resolution within 5 business days;

(c) the average number of days taken to resolve CDR consumer complaints through internal dispute resolution;

(d) the number of CDR consumer complaints notified to a recognised external dispute resolution scheme;

(e) the number of CDR consumer complaints resolved by external dispute resolution;

(f) the number of CDR consumer complaints that relate to privacy or confidentiality;

(g) the number of complaints made to a 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: Complaints covered by paragraph (g) are not "CDR consumer complaints".

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

(a) that relates to the CDR participant's obligations under or compliance with:

(i) Part IVD of the Act; or

(ii) these rules; or

(iii) binding data standards; and

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

CDR contract has the meaning given by rule 1.8.

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—see rule 1.13; and

(b) in relation to a data holder—see rule 1.14.

consumer data request:

(a) by a CDR consumer—means a request made under rule 3.3; and

(b) by an accredited person on behalf of a CDR consumer—means a request made under rule 4.4.

current:

(a) a consent to collect particular CDR data is ***current*** if it has not expired in accordance with rule 4.12; and

(b) a consent to use particular CDR data is ***current*** if it has not expired in accordance with rule 4.18; and

(c) an authorisation to disclose particular CDR data is ***current*** if it has not expired in accordance with rule 4.25.

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

(a) when making consumer data requests on behalf of a CDR consumer, the accredited person does not collect more CDR data than is reasonably needed in order to provide goods or services under a CDR contract; and

(b) when using CDR data that is collected under such requests, the accredited person does not use the CDR data beyond what is reasonably needed in order to provide goods or services under a CDR contract.

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

derived CDR data means information that is referred to in paragraph 56AI(1)(b) of the Act.

Note: "Derived CDR data" is information that is wholly or partly derived from information that is specified in a particular designation instrument made under section 56AC of the Act, but does not encompass the information that is specified in the instrument itself.

direct request service has the meaning given by subrule 1.12(2).

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 to the extent that they are relevant to the management of CDR data:

(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 5.1 of Schedule 2.

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.

outsourced service provider has the meaning given by rule 4.8.

PPF provider (short for purchased payment facility provider) means a class of ADIs that have obtained an authority under section 9 of the *Banking Act 1959* to conduct banking business as defined by regulation 3 of the *Banking Regulations 1966*.

Note: PPF providers are not authorised to conduct general banking business, but are permitted to undertake a specific type of banking activities.

primary CDR data means information that is referred to in paragraph 56AI(1)(a) of the Act.

Note: "Primary CDR data" is information that is specified in a particular designation instrument made under section 56AC of the Act, but does not encompass information that is wholly or partly derived from such information.

product data request means a request under rule 2.3.

product data request service has the meaning given by rule 1.11.

prohibited use or disclosure of CDR data for which there are CDR consumers, and which is disclosed pursuant to a consumer data request, means:

(a) selling the CDR data; or

(b) 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 person who:

(iv) is not the CDR consumer for that data; and

(v) did not make the consumer data request; or

(c) disclosing the CDR data other than to an outsourced service provider.

recognised external dispute resolution scheme means a dispute resolution scheme that is recognised under section 56DA 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 2.2 of Schedule 2.

required product data, in relation to the banking sector, has the meaning given by clause 2.1 of Schedule 2.

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

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

valid has the meaning given by subrule 3.3(4) or subrule 4.3(3) as appropriate.

(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) the CDR consumer for the particular CDR data that is dealt with in relation to the reference.
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.

(3) In these rules, a reference to a data holder is a reference to a data holder that would be required 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 clause 4.4 of Schedule 2.

1.8 Meaning of *CDR contract*

*Meaning of **CDR contract***

(1) For these rules, a contract between an accredited person and a CDR consumer is a ***CDR contract*** if the contract:
  (a) deals with the accredited person collecting and using CDR data in order to provide goods or services to the consumer or to another person; and
  (b) includes an option to terminate that satisfies subrule (3); and
  (c) does not include another clause that is inconsistent with, or that alters the effect of:
    (i) the right of the consumer to withdraw a consent to collect or to use CDR data under these rules; or
    (ii) the option to terminate.

(2) The contract is a ***CDR contract*** even if it deals with matters other than collection and use of CDR data in order to provide goods or services.

Option to terminate

(3) An option to terminate satisfies this subrule if it consists of a clause that has the effect that, if the consumer withdraws:

(a) all of the current consents to collect CDR data that have been given in relation to the CDR contract; and

(b) all of the current consents to use CDR data that have been given in relation to the CDR contract;

then:

(c) the consumer will have the option to terminate the CDR contract within a reasonable period, that is specified in the contract, after the withdrawals; and

(d) if the consumer exercises the option, then:

(i) the accredited person will no longer be obliged to provide any further goods or services to the consumer under the CDR contract; and

(ii) any right, obligation or liability of either party to the CDR contract that relates to goods or services that were provided under the contract prior to the exercise of the option will be unaffected by the exercise of the option; and

(iii) the consumer will have no further liability to pay any fees, charges or other amounts to the accredited person in relation to the contract (including in relation to the exercise of the option).

Note: If the termination option is exercised, any CDR data that has already been collected might then become "redundant data" within the meaning of subsection 56EO(2) of the Act. If it does, privacy safeguard 12 will be relevant: see subsection 56EO(2) of the Act and subrule 7.8(2) of these rules.

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 a determination under paragraph 52(1)(b) or any of paragraphs 52(1A)(a), (b), (c) or (d) of the *Privacy Act 1988*;

(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:

(i) an external dispute resolution scheme recognised under the *Privacy Act 1988*; or

(ii) a recognised external dispute resolution scheme;

that included a requirement to pay monetary compensation;

(g) any other relevant matter.

(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.

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

Subdivision 1.4.1—Preliminary

1.10 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.

Subdivision 1.4.2—Services for making requests under these rules

1.11 Product data request service

(1) A data holder must provide an online service that can be used to make product data requests.

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

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

(3) The service must:
  (a) enable requested data to be disclosed in machine-readable form; and
  (b) conform with the data standards.

1.12 Consumer data request service

(1) A data holder must provide:
  (a) an online service that can be used by CDR consumers to make consumer data requests directly to the data holder; and
  (b) an online service that can be used by accredited persons to make consumer data requests on behalf of CDR consumers to the data holder.

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.

(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) The data holder's direct request service must:
  (a) allow a request to be made in a manner that is no less timely, efficient and convenient than the online services that are ordinarily used by customers of the data holder to deal with the data holder; and
  (b) enable requested data to be disclosed in human-readable form; and
  (c) conform with the data standards.

(5) The data holder's accredited person request service must:
  (a) enable requested data to be disclosed in machine-readable form; and
  (b) conform with the data standards.

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

1.13 Consumer dashboard—accredited person

(1) An accredited person must provide an online service that can be used by each CDR consumer on whose behalf the accredited person makes a consumer data request to manage:
  (a) such requests; and
  (b) associated consents to collect CDR data and consents to use CDR data.

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

(3) The consumer dashboard for each such consumer must:
  (a) contain the following details of each consent to collect CDR data given by the consumer:
    (i) the specific CDR data to which the consent relates;
    (ii) when the CDR consumer gave the consent;
    (iii) whether the CDR consumer gave the consent for collection of CDR data:
      (A) on a single instance; or
      (B) over a period of time;
    (iv) if the CDR consumer gave the consent for collection of CDR data over a period of time:
      (A) what that period is; and
      (B) how often data has been, and is expected to be, collected over that period;
    (v) if the consent is current—when it is scheduled to expire;
    (vi) if the consent is not current—when it expired;
    (vii) information relating to CDR data that was collected pursuant to the consent (see rule 7.4); and
  (b) contain the following information relating to each consent to use CDR data given by the consumer:
    (i) the specific CDR data to which the consent relates;
    (ii) details of the specific use or uses for which the CDR consumer has given their consent;
    (iii) when the CDR consumer gave the consent;
    (iv) if the consent is current—when it is scheduled to expire;
    (v) if the consent is not current—when it expired; and
  (c) have functionality that allows for withdrawal, at any time, of:
    (i) consents to collect CDR data; and
    (ii) consents to use CDR data.

Note 1: For subparagraphs (a)(v) and (b)(iv), consents to collect and to use CDR data expire at the latest 12 months after they are given: see paragraphs 4.12(1)(c) and 4.18(1)(a).

Note 2: For subparagraph (b)(ii), for the specific uses that are possible, see the data minimisation principle: see rule 1.7.

(4) The withdrawal functionality must be:

(a) simple and straightforward to use; and
(b) no more complicated to use than the process for consenting to the collection or use; and
(c) clearly visibly displayed.

1.14 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 consumer to manage authorisations to disclose CDR data in response to the request.

(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 will also be provided with a consumer dashboard: see clause 3.4 of Schedule 2.

(3) The consumer dashboard must:
(a) contain the following details relating to each authorisation to disclose CDR data:
(i) the specific CDR data that has been authorised to be disclosed;
(ii) when the CDR consumer gave the authorisation;
(iii) the name of the accredited person who made the consumer data request;
(iv) the period for which the CDR consumer gave the authorisation;
(v) if the authorisation is current—when it is scheduled to expire;
(vi) if the authorisation is not current—when it expired;
(vii) information relating to CDR data that was disclosed pursuant to the authorisation (see rule 7.6); and
(b) have a functionality that allows for withdrawal of authorisations to disclose CDR data at any time.

Note: For subparagraph (a)(v), authorisations to disclose CDR data expire at the latest 12 months after they are given: see paragraph 4.25(c).

(4) The withdrawal functionality must be:
(a) simple and straightforward to use; and
(b) no more complicated to use than the process for giving the authorisation to disclose CDR data; and
(c) clearly visibly displayed.

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.

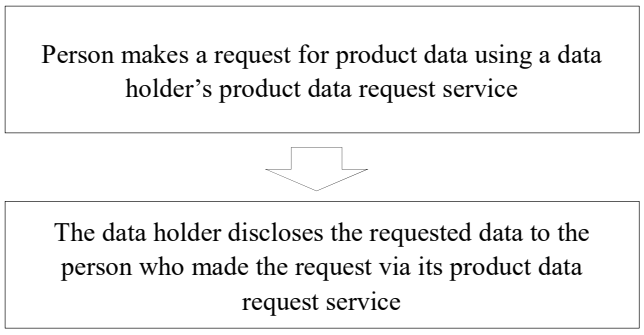
Subject to certain limitations, the requested data could be data about eligibility criteria, terms and conditions, price, and publicly available data about availability or performance of goods or services that the data holder offers.

Subject to an exception outlined in this Part, data holders must disclose such data when requested in accordance with this Part. The data is disclosed to the person who made the request, in machine-readable form, and can be used by the person as they see fit.

A fee cannot be charged for the disclosure.

2.2 Making product data requests—flowchart

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



2.3 Product data requests

(1) A person may request a data holder to disclose some or all of the CDR data:
  (a) that relates to one or more products that are offered by the data holder; and
  (b) that is required product data.

Note 1: For the definition of "required product data" in relation to the banking sector, see rule 1.7 and clause 2.1 of Schedule 2.

Note 2: 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 clause 4.4 of Schedule 2.

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

(3) A product data request may be made to a data holder only:
  (a) using the data holder's product data request service; and
  (b) in accordance with the data standards.

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

2.4 Disclosing required product data in response to product data request

(1) Subject to rule 2.5, if a data holder has received a product data request that has been made in accordance with rule 2.3, it must disclose the requested data to the person who made the request.

(2) The data must be disclosed:
  (a) using the data holder's product data request service; and
  (b) in accordance with the data standards.

Note: A fee cannot be charged for the disclosure.

2.5 Refusal to disclose in response to product data request

A data holder that has received a product data request that has been made in accordance with rule 2.3 may refuse to disclose CDR data in response to the request in circumstances (if any) set out in the data standards.

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.

Part 3—Consumer data requests made by 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 CDR consumers to data holders. Such requests are made using the data holder's direct request service.

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

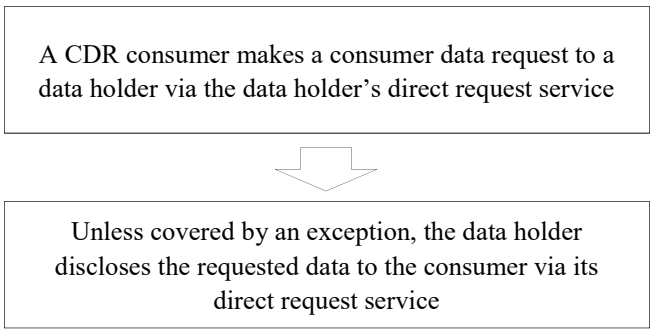
Subject to exceptions outlined in this Part, data holders are required to disclose CDR data when requested in accordance with this Part. The data is disclosed to the CDR consumer who made the request, in human-readable form, and can be used by the consumer as they see fit.

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

A fee cannot be charged for the disclosure.

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

The following is a flowchart for how a 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 request a data holder to disclose some or all of the CDR data:
   (a) for which the consumer is a CDR consumer; and
   (b) that is required consumer data for the consumer.

Note 1: See rule 1.7 for the definition of "required consumer data", and see clause 2.2 of Schedule 2 for the definition of "required consumer data" in relation to the banking sector.

Note 2: 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 clause 4.4 of Schedule 2.

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

(3) A CDR consumer may make a consumer data request to a data holder only by using the data holder's direct request service.

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

(4) A consumer data request made under this Part is ***valid*** if it is made in accordance with this rule.

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

(1) Subject to rule 3.5, if a data holder has received a valid consumer data request made under this Part, for disclosure of CDR data of which it is the data holder, it must disclose the requested data to the consumer.

Note: For the banking sector, for a request that relates to a joint account, see clause 3.3 of Schedule 2 for an additional circumstance in which data relating to the joint account might not be disclosed under these rules.

(2) The data must be disclosed:
   (a) using the data holder's direct request service; and
   (b) in accordance with the data standards.

Note: A fee cannot be charged for the disclosure.

3.5 Refusal to disclose in response to consumer data request

Refusal if disclosure would create risks of harm etc.

(1) A data holder that has received a valid consumer data request made under this Part may refuse to disclose CDR data in response to the request if it has reasonable grounds to believe that the disclosure would:
   (a) create a real risk of serious harm or abuse to an individual; or
   (b) adversely impact the security, integrity or stability of the information and communication technology systems the data holder uses to receive requests, and to disclose CDR data, under these rules.

(2) The data holder must, within 24 hours, inform the Commission of:

(a) such a refusal; and
(b) the reasons for the refusal;

in a form approved by the Commission for the purposes of this rule.

Refusal in circumstances provided for in the data standards

(3) A data holder that has received a valid consumer data request made under this Part may refuse to disclose CDR data in response to the request in circumstances (if any) set out in the data standards.

3.6 Use of data disclosed pursuant to consumer data request made under this Part

The consumer may use the data disclosed under this Part as they see fit.

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 and the accredited person need to be in a contractual relationship under which the accredited person provides goods or services to the CDR consumer, using the consumer's CDR data. Such a contract is called a CDR contract. There are special requirements for CDR contracts under these rules.

Before making a consumer data request on behalf of a CDR consumer relating to the contract, the consumer must first have consented to the accredited person:

(a) collecting specified CDR data from the data holder of that CDR data; and

(b) using the collected data in order to provide goods or services under the contract.

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 necessary in order to provide goods or services under the CDR contract; and

(b) may use the collected data only as consented to by the consumer, and only in order to provide goods or services under the CDR contract.

A data holder that receives a consumer data request under this Part from an accredited person must ask the CDR consumer to authorise disclosure of the requested data.

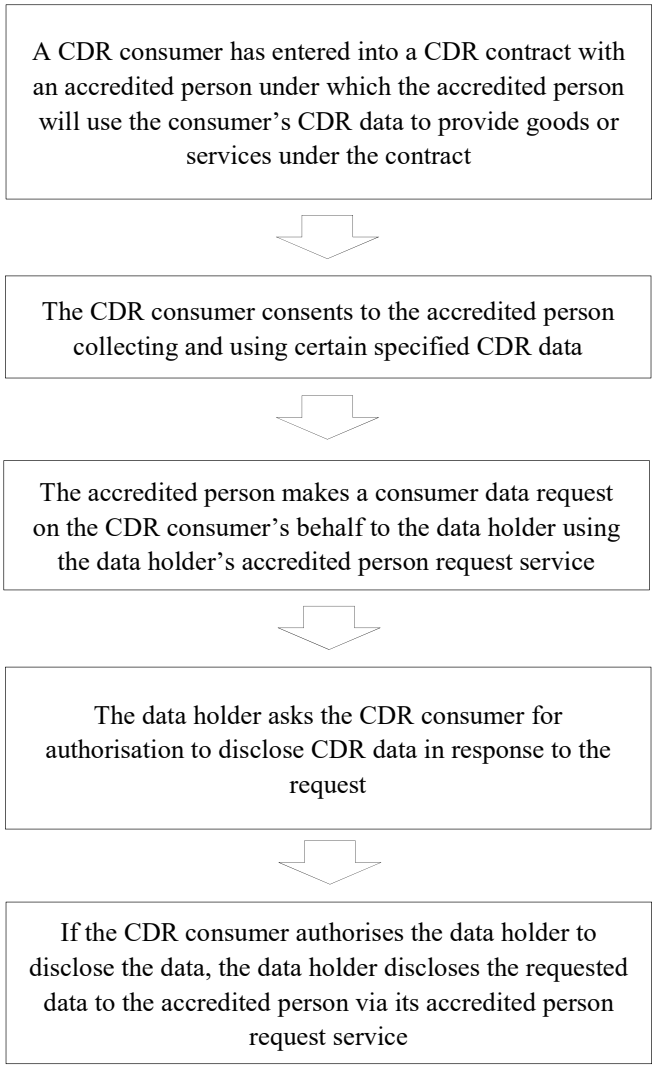
Subject to exceptions outlined in this Part, the data holder is then required to disclose the requested data to the accredited person. The accredited person is able to use the data in accordance with that person's current consent to use the CDR data, Part IVD of the Act (including the privacy safeguards) and these rules (including the data minimisation principle).

For the banking sector, special rules apply where there are joint account holders. These are set out in Part 3 of Schedule 2.

A fee cannot be charged for the disclosure.

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:



Division 4.2—Consumer data requests made by accredited persons

4.3 Request for accredited person to seek to collect CDR data

(1) An accredited person that enters into a CDR contract with a CDR consumer may ask the consumer to give their consent to the accredited person:

(a) collecting specified CDR data:

(i) for which the consumer is a CDR consumer; and

(ii) that is required consumer data for that consumer; and

(b) using that CDR data;

in order to provide goods or services under the contract.

(2) The accredited person may ask for:

(a) consents to collect CDR data only in accordance with Division 4.3; and

(b) consents to use CDR data only in accordance with Division 4.4.

Note 1: See rule 1.7 for the definition of "required consumer data", and see clause 2.2 of Schedule 2 for the definition of "required consumer data" in relation to the banking sector.

Note 2: In order to provide goods or services under the CDR contract, it might be necessary for the consumer to direct the accredited person to request CDR data from more than 1 data holder.

Note 3: The accredited person is able to collect and use CDR data only in accordance with the data minimisation principle: see rule 1.7 for the meaning of "data minimisation principle".

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

Note: See section 56EF of the Act (privacy safeguard 3).

(4) The request ceases to be ***valid*** if the CDR contract is terminated (see subrule 1.8(3)) or otherwise ceases to be in force.

4.4 Consumer data requests by accredited persons

(1) If:

(a) a CDR consumer has given an accredited person a valid request to seek to collect CDR data from a data holder; and

(b) the request has not ceased to be valid; and

(c) the consents referred to in rule 4.3 are current;

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

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

(e) it is able to collect in accordance with the data minimisation principle.

Note: See rule 1.7 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 goods or services under the CDR contract, 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 clause 4.4 of Schedule 2.

(3) A consumer data request made by an accredited person under this Part may be made only:

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

(b) in accordance with the data standards.

Note: A data holder cannot charge an accredited person a fee for making a consumer data request.

4.5 Data holder must ask CDR consumer to authorise disclosure as soon as practicable

Subject to rule 4.7, if:

(a) a data holder receives a consumer data request from an accredited person; and

(b) there is no current authorisation for the data holder to disclose the requested data to the accredited person;

the data holder must, as soon as practicable, ask the CDR consumer on whose behalf the request was made to authorise the disclosure of the data.

Note 1: For authorisations to disclose CDR data, see Division 4.5.

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 3.5 of Schedule 2.

4.6 Disclosing required consumer data in response to a consumer data request

(1) Subject to rule 4.7, 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;

the data holder must disclose, to the accredited person, the requested data that it is authorised to disclose.

Note: For the banking sector, for a request that relates to a joint account, see clause 3.5 of Schedule 2 for additional circumstances in which CDR data relating to the joint account might not be disclosed under these rules.

(2) The data must be disclosed:

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

(b) in accordance with the data standards.

Note 1: A fee cannot be charged for the disclosure.

Note 2: 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.

Note 3: Rule 7.6 (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.

4.7 Refusal to disclose in response to consumer data request

Refusal if disclosure would create risks of harm etc.

(1) A data holder that has received a consumer data request made under this Part may refuse to disclose CDR data in response to the request if it has reasonable grounds to believe that the disclosure would:
  (a) create a real risk of harm or abuse to an individual; or
  (b) adversely impact the security, integrity or stability of:
    (i) the Register of Accredited Persons; or
    (ii) the information and communication technology systems the data holder uses to receive requests, and to disclose CDR data, under these rules.

(2) The data holder must, within 24 hours, inform the Commission of:
  (a) such a refusal; and
  (b) the reasons for the refusal;
in a form approved by the Commission for the purposes of this rule.

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

Refusal in circumstances provided for in the data standards

(4) A data holder that has received a consumer data request made under this Part may refuse to disclose CDR data in response to the request in circumstances (if any) set out in the data standards.

4.8 Use and disclosure of data collected pursuant to consumer data requests under this Part

(1) The accredited data recipient may:
  (a) use the data collected under this Part to provide goods or services under the CDR contract, subject to:
    (i) Part IVD of the Act (including the privacy safeguards); and
    (ii) these rules (including current consents to use the CDR data and the data minimisation principle); and
  (b) use or disclose the collected data by providing it to an outsourced service provider, so that the outsourced service provider can use the data to provide goods or services to the accredited data recipient that will assist the accredited data recipient to provide the goods or services under the CDR contract.

Note: This rule is an authorisation for the purposes of paragraph 56EI(1)(b) of the Act (privacy safeguard 6).

(2) Despite subrule (1), the accredited data recipient must not use or disclose the collected data for a prohibited use or disclosure.

Note: See rule 1.7 for the meaning of "prohibited use or disclosure".

(3) For these rules, a person is an ***outsourced service provider*** of an accredited data recipient if:

(a) the accredited data recipient has entered into a contract with the person for the provision of goods or services; and

(b) under the contract, the outsourced service provider is required to take the steps outlined in Schedule 1, to the extent relevant having regard to the goods or services that the outsourced service provider provides to the accredited data recipient, as if the outsourced service provider were an accredited data recipient.

(4) The accredited data recipient must ensure that the outsourced service provider takes the steps referred to in paragraph (3)(b).

Division 4.3—Consents to collect CDR data

4.9 Purpose of Division

This Division deals with consents to collect CDR data, for the purposes of paragraph 4.3(1)(a).

4.10 Asking CDR consumer to give consent to collect CDR data

(1) A consent given by a CDR consumer to collect CDR data must be:
  (a) voluntary; and
  (b) express; and
  (c) informed; and
  (d) specific as to purpose; and
  (e) time limited; and
  (f) easily withdrawn.

(2) When asking a CDR consumer to give their consent for the purposes of paragraph 4.3(1)(a), an accredited person:
  (a) must seek to make the consent process as easy to understand as is practicable; and
  (b) may use visual or other aids to enhance comprehensibility; and
  (c) must not include other documents, or references to other documents, that reduce comprehensibility;
  (d) must do so in accordance with the data standards.

(3) The accredited person must:
  (a) identify the types of CDR data for which the consent is sought, having regard to the data minimisation principle; and
  (b) allow the CDR consumer to actively select or actively specify which types of CDR data they are consenting to the accredited person collecting; and
  (c) ask for the CDR consumer's express consent for the accredited person to collect the selected or specified data.

Example: For paragraph (b), 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: For paragraph (b), an accredited person cannot rely on, for example, pre-selected options to indicate the data that the consent relates to.

Note 2: For paragraph (c), an accredited person could not infer consent, or seek to rely on an implied consent.

(4) The accredited person must give the CDR consumer the following information:
  (a) the name and contact details of the accredited person;
  (b) whether the accredited person is asking the CDR consumer to give their consent for:
    (i) a single collection of CDR data; or
    (ii) collection of CDR data over a period of time of not more than 12 months;

(c) if the consumer is being asked to give a consent for collection over a period of time:
  (i) what that period is; and
  (ii) how often data is expected to be collected over that period;
(d) the period for which the accredited person would hold the CDR data that is the subject of the consent;
(e) a statement that at any time, the consent can be withdrawn;
(f) instructions for how the consent can be withdrawn.

Note: After the end of the period referred to in paragraph (d), the data would need to be dealt with in accordance with subsection 56EO(2) of the Act (privacy safeguard 12) and subrule 7.8(2).

4.11 Withdrawal of consent to collect CDR data and notification

(1) The CDR consumer who gave a consent to collect particular CDR data may withdraw the consent at any time:
  (a) by communicating the withdrawal to the accredited person in writing; or
  (b) by using the accredited person's consumer dashboard.

(2) If a consent to collect particular CDR data is withdrawn in accordance with this rule, the accredited person must, in accordance with the data standards, notify the data holder of the withdrawal.

Note: Upon notification, an authorisation to disclose the CDR data expires: see paragraph 4.25(1)(b).

4.12 Duration of consent to collect CDR data

(1) A consent to collect particular CDR data expires at the earliest of the following:
  (a) when the consent is withdrawn under rule 4.11;
  (b) when the accredited person is notified, under subrule 4.24(2), of the withdrawal of the authorisation to disclose that CDR data;
  (c) the end of the period of 12 months after the consent was given;
  (d) if the consent was for collection of that CDR data on a single occasion—after the CDR data has been collected;
  (e) if the consent was for collection of that CDR data over a specified period—the end of that period.

(2) If an accredited person's accreditation is revoked or surrendered in accordance with rule 5.14, all consents for the accredited person to collect CDR data expire when the revocation or surrender takes effect.

4.13 Updating consumer dashboard

If an accredited person receives, from a CDR consumer, a consent to collect CDR data, or if such a consent expires, the accredited person must update that CDR consumer's consumer dashboard as soon as practicable.

4.14 Ongoing notification requirement—consents to collect CDR data

While a consent to collect particular CDR data is current, the accredited person must notify the CDR consumer who gave the consent, each 90 days, that the consent is still current.

Division 4.4—Consents to use CDR data

4.15 Purpose of Division

This Division deals with consents to use CDR data, for the purposes of paragraph 4.3(1)(b).

4.16 Asking CDR consumer to give consent to use CDR data

(1) A consent given by a CDR consumer to use CDR data must be:
  (a) voluntary; and
  (b) express; and
  (c) informed; and
  (d) specific as to purpose; and
  (e) time limited; and
  (f) easily withdrawn.

(2) When asking a CDR consumer to give their consent for the purposes of paragraph 4.3(1)(b), an accredited person:
  (a) must seek to make the consent process as easy to understand as is practicable; and
  (b) may use visual or other aids to enhance comprehensibility; and
  (c) must not include other documents, or references to other documents, that reduce comprehensibility; and
  (d) must do so in accordance with the data standards.

(3) The accredited person must:
  (a) identify the specific uses of the CDR data from which the CDR consumer will be able to select or that the CDR consumer will be able to specify; and
  (b) allow the CDR consumer to actively select or actively specify those specific uses they are consenting to; and
  (c) ask for the CDR consumer's express consent for those uses.

Example: For paragraph (b), an accredited person could present the CDR consumer with a set of un-filled boxes corresponding to different types of uses, and permit the CDR consumer to select the boxes that correspond to the uses they consent to.

Note 1: For paragraph (b), an accredited person cannot rely on, for example, pre-selected options to indicate the uses the consent relates to.

Note 2: For paragraph (c), an accredited person could not infer consent, or seek to rely on an implied consent.

(4) The accredited person may ask the CDR consumer to consent only to uses of the collected CDR data that are allowable under the data minimisation principle.

Note: See rule 1.7 for the definition of "data minimisation principle".

(5) The accredited person must not ask a CDR consumer to give consent to use CDR data for a prohibited use or disclosure.

Note: See rule 1.7 for the meaning of "prohibited use or disclosure".

(6) The accredited person must give the CDR consumer the following information:
  (a) the name and contact details of the accredited person;

(b) the period of time, of not more than 12 months, for which the consumer is being asked to give their consent;
(c) 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;
(d) a statement that at any time, the consent can be withdrawn;
(e) instructions for how the consent can be withdrawn.

4.17 Withdrawal of consent to use CDR data

The CDR consumer who gave a consent to use particular CDR data may withdraw the consent at any time:
(a) by communicating the withdrawal to the accredited person in writing; or
(b) by using the accredited person's consumer dashboard.

4.18 Duration of consent to use CDR data

(1) A consent to use particular CDR data expires at the earlier of the following:
(a) the end of the period of 12 months after the consent was given;
(b) when the consent is withdrawn under rule 4.17.

Note: A consent to use CDR data could be current even after the corresponding consent to collect CDR data has expired.

(2) If an accredited person's accreditation is revoked or surrendered in accordance with rule 5.14, all consents for the accredited person to use CDR data expire when the revocation or surrender takes effect.

4.19 Updating consumer dashboard

If an accredited person receives a consent to use CDR data from a CDR consumer, or if such a consent expires, the accredited person must update the relevant consumer dashboard as soon as practicable.

4.20 Ongoing notification requirement—consents to use CDR data

While a consent to use particular CDR data is current, the accredited person must notify the CDR consumer who gave the consent, each 90 days, that the consent is still current.

Division 4.5—Authorisations to disclose CDR data

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 3.6 of Schedule 2.

4.22 Asking CDR consumer to authorise disclosure of CDR data

(1) When asking a CDR consumer to authorise the disclosure of CDR data for the purposes of rule 4.5, a data holder:
  (a) must seek to make the consent process as easy to understand as is practicable; and
  (b) may use visual or other aids to enhance comprehensibility; and
  (c) must not include other documents, or references to other documents, that reduce comprehensibility;
  (d) must do so in accordance with the data standards.

(2) The 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) a single disclosure of CDR data; 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:
    (i) what that period is; and
    (ii) how often data is expected to be disclosed over that period;
  (f) a statement that, at any time, the authorisation can be withdrawn;
  (g) instructions for how the authorisation can be withdrawn.

4.23 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:
  (a) add any requirements to the authorisation process beyond those specified in the data standards; or
  (b) request additional information during the authorisation process beyond that specified in the data standards; or
  (c) offer additional or alternative services as part of the authorisation process.

4.24 Withdrawal of authorisation to disclose CDR data and notification

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

(a) by communicating the withdrawal to the data holder in writing; or

(b) by using the data holder's consumer dashboard.

Note: For the banking sector, for a request that relates to a joint account, see subclause 3.7(1) of Schedule 2 for an additional circumstance in which an authorisation to disclose CDR data can be withdrawn.

(2) If an authorisation is withdrawn in accordance with this rule, the data holder must, in accordance with the data standards, notify the accredited person of the withdrawal.

Note: Upon notification, a consent to collect the CDR data to which the withdrawn authorisation relates expires: see paragraph 4.12(1)(b).

4.25 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) when the authorisation is withdrawn under rule 4.24;

(b) when the accredited person is notified, under subrule 4.11(2), of the withdrawal of a consent to collect that CDR data;

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

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

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

Note: In the case of the banking sector, for authorisations to disclose CDR data that relates to joint accounts, see also clause 3.7 of Schedule 2.

(2) If an accredited person's accreditation is revoked or surrendered in accordance with rule 5.14, 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 suspension.

4.26 Updating consumer dashboard

If a data holder receives, from a CDR consumer, an authorisation to disclose CDR data, or if such an authorisation expires, the data holder must update that CDR consumer's consumer dashboard as soon as practicable.

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 accredits 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
- continuing 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 the applicant intends offering to CDR consumers using CDR data 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 5.12(b) and (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) This rule applies if, in the view of the Data Recipient Accreditor, the Accreditor needs further information in order to assess an application to be an accredited person.

(2) The Data Recipient Accreditor may, by written notice given to the accreditation applicant, request that the applicant provide, within the period specified in the notice, the further information relating to the application that is specified in the notice.

Note: If the further information is not forthcoming, the Data Recipient Accreditor might not be in a position to be satisfied, under section 56CA of the Act, that the applicant satisfies 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 Other functions of Data Recipient Accreditor

For paragraph 56CH(1)(a) of the Act, the Data Recipient Accreditor's functions include interviewing an accreditation applicant when assessing an application under rule 5.2, if the Accreditor considers this appropriate.

5.6 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 would, if accredited, be able to comply with the obligations of a person who is accredited at that level (see rule 5.11).

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 5.2 of Schedule 2.

5.7 Accreditation decision—notifying Accreditation Registrar

(1) The Data Recipient Accreditor must notify the Accreditation Registrar, in writing, as soon as practicable after accrediting a person under subsection 56CA(1) of the Act.

(2) The notice must include the following:
  (a) that fact;
  (b) the accredited person's name;
  (c) the accredited person's addresses for service;
  (d) if the accredited person is a foreign entity—the name and addresses for service of the accredited person's local agent;
  (e) the level of accreditation;
  (f) either:
    (i) any conditions; or
    (ii) if the Accreditor considers it appropriate—a description of the effect of any conditions;

  that were imposed at the time of the accreditation.

Note 1: For paragraph (f), for conditions on accreditations, see rule 5.9.

Note 2: The Registrar must update the Register of Accredited Persons to reflect the accreditation and any notified conditions: see rule 5.23.

5.8 Accreditation decision—notifying accreditation applicant

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

(2) If the Accreditor accredited 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.

Note: For paragraph (c), for conditions on accreditations, see rule 5.9.

(3) If the Accreditor refused 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.

5.9 Conditions on accreditation

(1) The Data Recipient Accreditor may, in writing:
  (a) impose any 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 5.14.

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

(3) 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.

(4) 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.

5.10 Notification relating to conditions

Notice to accredited person

(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.

(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.

Notice to Accreditation Registrar

(3) The Data Recipient Accreditor must notify the Accreditation Registrar, in writing, as soon as practicable after the imposition, variation or removal of a condition on an accreditation.

(4) The notice must include the following:
   (a) the name of the accredited person;
   (b) either:
      (i) the conditions or the conditions as varied, or the condition that was removed; or
      (ii) if the Accreditor considers it appropriate—a description of the effect of the conditions or the conditions as varied or removed.

Note: The Registrar must amend the entry in the Register relating to the person to reflect the condition or the condition as varied: see rule 5.23.

Subdivision 5.2.3—Obligations of accredited person

5.11 Obligations of accredited person at the "unrestricted" level

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 manage CDR data; and

(b) take the steps outlined in Schedule 1 which relate to protecting the CDR data from:

(i) misuse, interference and loss; and

(ii) unauthorised access, modification or disclosure; and

(c) have internal dispute resolution processes that meet the requirements of Part 6; and

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

(e) 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 law relevant to the management of CDR data; and

(f) have addresses for service; and

(g) 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 5.2 of Schedule 2.

Note 3: For paragraph (b), the steps outlined in Schedule 1 relate to privacy safeguard 12 (see subsection 56EO(1) of the Act and subrule 7.8(1) of these rules).

Note 4: For paragraphs (f) and (g), see rule 1.7 for the meaning of "addresses for service".

5.12 Notification requirements

An accredited person must notify the Data Recipient Accreditor as soon as practicable of the following:

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

(b) any change to the person's addresses for service;

(c) if the person is a foreign entity—any change to:

(i) the person's local agent; or

(ii) the local agent's addresses for service;

(d) 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 manage CDR data.

Note: See rule 1.7 for the meaning of "addresses for service".

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

5.13 Transfer of accreditation

An accreditation cannot be transferred.

5.14 Revocation, suspension, or surrender of accreditation

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 an associated 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 person's accreditation, as appropriate.
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 (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.

	Grounds for revocation, suspension and surrender of accreditation as accredited person	
	If:	**the Data Recipient Accreditor:**
5	the following are satisfied: (a) the accredited person was, at the time of the accreditation, an ADI (including a PPF provider or a restricted 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; or (c) a condition (if any) of its accreditation;	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; or (c) a condition (if any) of its accreditation;	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 manage CDR data;	may, in writing: (a) suspend; or (b) revoke; the person's accreditation, as appropriate.

5.15 Revocation of accreditation—process

(1) Before revoking an accredited person's registration under rule 5.14, 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 5.14, 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).

5.16 Suspension of accreditation—duration

(1) Without limitation, the Data Recipient Accreditor, under rule 5.14:
  (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.

5.17 General process for suspension of accreditation or extension of suspension

(1) This rule applies subject to rule 5.18.

(2) Before suspending an accreditation under rule 5.14, 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 5.14, 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).

5.18 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) because of the urgency, it is not possible to comply with rule 5.17 prior to the suspension or extension.

(2) The Accreditor may suspend the accreditation, or extend the suspension, without first complying with rule 5.17.

(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.

5.19 When revocation or suspension takes effect

A revocation or suspension takes effect at the time specified by the Data Recipient Accreditor.

5.20 Notifying Accreditation Registrar of surrender, suspension or revocation

Notification of surrender, suspension or revocation

(1) The Data Recipient Accreditor must notify the Accreditation Registrar, in writing, of a surrender, suspension or an extension of a suspension, or a revocation, of an accreditation as soon as practicable.

Note: The Accreditation Registrar must amend the entry in the Register relating to the person to reflect the suspension, extension or revocation, as the case may be: see rule 5.23.

(2) The notice must include the following:
(a) the name of the accredited person;
(b) whether the accreditation has been surrendered, revoked or suspended, or whether a suspension has been extended;
(c) if the accreditation has been suspended or a suspension extended—the duration of the suspension or the suspension as extended, as appropriate.

Notification of revocation of decision to suspend or of suspension ceasing to have effect

(3) The Data Recipient Accreditor must notify the Accreditation Registrar, in writing, of a suspension ceasing to have effect, as soon as practicable.

Note: The Accreditation Registrar must amend the entry in the Register relating to the person to reflect suspension no longer having effect: see rule 5.23.

(4) The notice must include the following:
(a) the name of the accredited person;
(b) the fact that the suspension has ceased to have effect.

5.21 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.

Obligations of accredited person

(2) The person:
(a) is subject to:
(i) if their accreditation has been suspended—the obligations of an accredited person whose accreditation has not been suspended; and
(ii) if their accreditation has been surrendered or revoked—privacy safeguards 2, 6, 7 and 12; and

(b) must not, after the revocation or while the accreditation is suspended, seek to collect any, or any further, CDR data under these rules; and

(c) 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—that any consents to collect and to use CDR data may be withdrawn at any time.

(3) 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;

in addition, the person must destroy or de-identify that data by taking the steps specified in subrule 7.8(2).

Note: In addition:

- if an accreditation is revoked or surrendered:
  - any consents to collect CDR data expire: see subrule 4.12(2); and
  - any consents to use CDR data expire: see subrule 4.18(2); and
  - any authorisations to disclose CDR data expire: see subrule 4.25(2); and
- if an accreditation is suspended, the accredited person is not able to collect data while the suspension is in effect.

5.22 Consequences of surrender of accreditation

An accreditation that is surrendered in accordance with this Subdivision is taken to have been revoked on the day the surrender was requested.

Note: In addition, any consents to collect and use CDR data expire: see subrules 4.12(2), 4.18(2) and 4.25(2).

Division 5.3—Rules relating to Register of Accredited Persons

5.23 Inclusion of and updating entries in Register of Accredited Persons

As soon as practicable after receiving a notice under rule 5.7, 5.10 or 5.20 that relates to a particular accreditation, the Accreditation Registrar must update the Register of Accredited persons as appropriate by entering the following details or changes to the following details:

(a) the following details about the accredited person:
  (i) the accredited person's name;
  (ii) the accredited person's addresses for service;
  (iii) 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) any conditions on the accreditation that the Registrar has been notified of;
(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) any other information that the Registrar considers appropriate;

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

Note 2: For paragraphs (a) and (b), see paragraphs 5.7(2)(a) to (e).

Note 3: For paragraph (b), the only level of accreditation is the "unrestricted" level.

Note 4: For paragraph (c), see paragraphs 5.7(2)(f) and 5.10(4)(b).

Note 5: For paragraphs (d), (e) and (f), see rule 5.20.

5.24 Amendment and correction of entries in Register of Accredited Persons

The Accreditation Registrar:

(a) must, as soon as practicable, amend the Register of Accredited Persons as required by the Data Recipient Accreditor; and
(b) may make clerical amendments to entries in the Register as appropriate to ensure the accuracy of the Register.

5.25 Automated decision-making—Accreditation Registrar

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

Part 6—Rules relating to dispute resolution

6.1 Simplified outline of this Part

Certain data holders, and accredited persons, are required to have internal dispute resolution processes that comply with this Part. The corresponding requirement for accredited persons is contained in rule 5.11.

6.2 Interpretation

In this Part:

Regulatory Guide 165 means *Regulatory Guide 165 Licensing: Internal and external dispute resolution* published by the Australian Securities & Investments Commission in May 2018, as in force at the date of commencement of these rules.

Note: Regulatory Guide 165 could in 2019 be accessed from the Australian Securities & Investments Commission's website (https://asic.gov.au).

6.3 Obligation to have internal dispute resolution processes

A data holder must comply with Part B of Regulatory Guide 165 in relation to its internal dispute resolution processes, except to the extent that the provisions of Part B relate specifically to the regulatory activities of the Australian Securities & Investments Commission, as if:

(a) references to complaints or disputes were references to CDR consumer complaints; and

(b) references to financial service providers were references to CDR participants.

Note: An accredited person must also have internal dispute resolution processes that meet the requirements of this Part: see rule 5.11.

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 under Part IV of the Act. The privacy safeguards apply only to CDR data for which there are one or more CDR consumers (required consumer data); they do not apply to required 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.

Division 7.2—Rules relating to privacy safeguards

Subdivision 7.2.1—Rules relating to consideration of CDR data privacy

7.2 Rules 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.

Additional information for CDR policy

(2) 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 list of the outsourced service providers (whether based in Australia or based overseas, and whether or not any is an accredited person); and
   (b) 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
   (c) 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.

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

Note 2: For paragraph (c), 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.

(3) 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 lodged;
   (b) how a CDR consumer complaint can be lodged;
   (c) when a CDR consumer complaint can be lodged;
   (d) when acknowledgement of CDR consumer complaints 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 and externally.

Availability of policy

(4) For paragraph 56ED(7)(b) of the Act, a CDR participant must make its CDR policy readily available:
  (a) on its website; and
  (b) on an application for a mobile device.

(5) 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.

7.3 Rules relating to privacy safeguard 2—anonymity and pseudonymity

For subsection 56EE(3) of the Act, subsection 56EE(1) 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 Rules relating to privacy safeguard 5—notifying of the collection of CDR data

For paragraph 56EH(a) 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 subparagraph 1.13(3)(a)(vii).

Subdivision 7.2.3—Rules relating to dealing with CDR data

7.5 Rules relating to privacy safeguard 6—use or disclosure of CDR data by accredited data recipients

For paragraph 56EI(1)(b) of the Act, rule 4.8 authorise uses and disclosures of CDR data by an accredited data recipient.

Note: Rule 4.8 deals with use and disclosure of data collected pursuant to consumer data requests under this Part 4.

The ACCC is considering rules authorising the disclosure, with the consumer's consent, of a consumer's CDR data by an accredited person to another accredited person (for example an intermediary) or another person (for example a consumer's accountant, lawyer or financial counsellor).

7.6 Rules 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) a consumer data request; or

(b) a correction request;

must update each consumer dashboard that relates to the request to indicate:

(c) what CDR data was disclosed; and

(d) when the CDR data was disclosed; and

(e) 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 will need to be similarly updated: see clause 3.8 of Schedule 2.

Note 3: See subparagraph 1.14(3)(a)(vii).

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

7.7 Rules 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: For paragraph (d), see subsection 56EN(4) of the Act.

(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 24 hours;

after the CDR participant becomes aware of the matter referred to in paragraph 56EN(3)(b) of the Act.

7.8 Rules relating to privacy safeguard 12—security of CDR data held by accredited data recipients

(1) For subsection 56EO(1) of the Act, the steps are set out in Schedule 1.

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.

(2) For subsection 56EO(2) of the Act, the steps are, having regard to the DDM Framework, as soon as practicable, to:

(a) decide which of destruction or de-identification is appropriate in the circumstances; and

(b) destroy or de-identify the data, as appropriate; and

(c) make a record to evidence the destruction or de-identification (see paragraph 9.3(2)(g)).

(3) In this rule:

DDM Framework means *The De-Identification Decision-Making Framework* published by Data61, as in force from time to time.

Note: The *De-Identification Decision-Making Framework* could in 2019 be downloaded from Data61's website (https://www.data61.csiro.au/).

Subdivision 7.2.5—Rules relating to correction of CDR data

7.9 No fee for responding to or actioning correction request

A fee must not be charged for responding to or actioning a correction request.

7.10 Rules 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) add to, delete, alter, destroy or de-identify 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) 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) sets out the complaint mechanisms available to the requester.

Note: In relation to subparagraph (c)(ii), see Part 6.

Part 8—Rules relating to data standards

Division 8.1—Simplified outline

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 2 or more consumer or 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, 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 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 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.

(3) The Data Standards Chair:
   (a) must determine and publish a date by which submissions referred to in paragraph (2)(d) must be received by the Chair; and
   (b) may extend that date.

(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).

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 making product data requests and consumer data requests;

(b) the disclosure and security of CDR data, including:

(i) authentication of CDR consumers requiring multi-factor authentication or equivalent controls; and

(ii) seeking authorisations to disclose CDR data in response consumer data requests;

(c) the descriptions of the types of CDR data to be used by CDR participants in making and responding to requests;

(d) the formats in which CDR data is to be provided in response to requests;

(e) 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;

(f) the processes for CDR participants to notify other CDR participants of revocation of consent or revocation of authorisations by CDR consumers;

(g) 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.

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 audit; and
- civil penalty provisions, which are enforced under the enforcement provisions of the Act.

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 5.9 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 5.14 to:
  (i) suspend an accreditation; or
  (ii) extend a suspension; or
  (iii) revoke an accreditation.

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 of the following:
  (a) CDR complaint data;
  (b) consumer data requests received;
  (c) authorisations given by CDR consumers to disclose CDR data;
  (d) withdrawals of authorisations to disclose CDR data;
  (e) notifications of withdrawals of consents to collect CDR data;
  (f) disclosures of CDR data made in response to consumer data requests;
  (g) instances where CDR data has not been disclosed in reliance on an exemption from the obligation to disclose CDR data.

Records to be kept and maintained—accredited data recipient

(2) An accredited data recipient must keep and maintain records of the following:
  (a) CDR complaint data;
  (b) consents to collect and use CDR data provided by CDR consumers;
  (c) CDR data collected under these rules;
  (d) notifications of withdrawals of authorisations received from data holders;
  (e) withdrawals of consents by CDR consumers;
  (f) 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;
  (g) records that evidence any destruction or de-identification for the purposes of privacy safeguard 12 (see section 56EO of the Act and rule 7.8 of these rules); and
  (h) records of any matters that are required to be retained under Schedule 1 to these rules.

Period for retention of records

(3) Each record referred to in this rule must be kept for a period of 6 years beginning on the day the record was created.

9.4 Reporting requirements

Reports that must be prepared—data holder

(1) A data holder must prepare a report for each reporting period that summarises the CDR complaint data that relates to that reporting period.

Reports that must be prepared—accredited data recipient

(2) An accredited data recipient must prepare a report for each reporting period that:
   (a) summarises the CDR complaint data that relates to that reporting period; and
   (b) 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
   (c) describes any material changes that have been made to any goods or services offered by the accredited data recipient since the previous reporting period.

Form of reports

(3) Each report must be in the form approved by the Commission for the purposes of this rule.

Provision of reports

(4) Each report must be submitted to:
   (a) the Commission; and
   (b) the Information Commissioner.

(5) Each report must be submitted within 30 days after the end of each reporting period.

(6) 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).

(7) 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)(b), (c) 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)(b) and (d) 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:

(a) as soon as practicable; but

(b) no later than 10 business days;

after receiving the request.

(5) Copies of records must be provided in the form approved by the Commission for the purposes of this subrule.

(6) A fee may not be charged for making or responding to such a request.

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) The Commission, or the Information Commissioner, may give a CDR participant a written notice that requests the CDR participant to produce copies of records that:
   (a) are required, by this Division, to be kept; and
   (b) are specified in the notice;

   for the purposes of conducting the audit.

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 accreditation criteria;
   (b) any conditions imposed on their accreditation.

(2) The Data Recipient Accreditor may give an accredited data recipient a written notice that requests the accredited data recipient to produce copies of records that:
   (a) are required, by this Division, to be kept; and
   (b) are specified in the notice;

   for the purposes of conducting the audit.

(3) The Data Recipient Accreditor must provide a copy of any audit report to the Commission and the Information Commissioner.

Division 9.4—Civil penalty provisions

The ACCC is considering which rules will be made a civil penalty provision.

Schedule 1—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

(1) This Part sets out steps for the purpose of subsection 56EO(1) of the Act, which relate to privacy safeguard 12 (see subrule 7.8(1) and paragraph 5.11(b) of these rules).

(2) This Part is also relevant to:
   (a) obligations of outsourced service providers; and
   (b) obligations of accredited persons in relation to their outsourced service providers;

(see subrules 4.8(3) and (4) of these rules).

1.2 Interpretation

In this Schedule:

CDR data environment means the systems, technology and processes that relate to the management of CDR data, including CDR data disclosed to outsourced service providers.

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 (that is, the policies, processes, roles and responsibilities required to facilitate the oversight and management of information security) for managing information security risks relating to CDR data.

(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 (that is, 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 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) An accredited data recipient must have and maintain an information security capability commensurate with the extent and nature of threats to its CDR data environment.

(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.

(3) The accredited data recipient must design, implement and operate information security controls to protect CDR data, including the control requirements and minimum controls specified in Part 2 of this Schedule.

1.6 Step 4—Implement a formal controls assessment program

(1) An accredited data recipient must review and assess the effectiveness of its information security capability and controls relevant to its CDR data environment by establishing a formal controls testing program. The extent and frequency of this testing should be commensurate with:
   (a) the rate at which vulnerabilities and threats change; and

(b) material changes to the boundaries of its CDR data environment; and
(c) the likelihood of failure of controls having regard to the results of previous testing; and
(d) the risks associated with exposure to external environments where the accredited data recipient is or may be unable to enforce its information security policies.

(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 control requirements 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 in a timely manner.

(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*.

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 annually review and test its CDR data security response plans to ensure they remain resilient, effective and consistent with its obligations in relation to notifying CDR data security breaches.

Part 2—Minimum information security controls

2.1 Purpose of Part

This Part sets out the information security controls, for the purpose of subclause 1.5(3) 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	Multi-factor authentication is required for all access to CDR data.
		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. Note: In relation to retention, see paragraph 9.3(2)(h) of these rules.

Schedule 1—Steps for privacy safeguard 12—security of CDR data held by accredited data recipients

	Control requirements	Minimum controls	Description of minimum controls
		Access security	Processes, including automatic processes, have been 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 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)(h) of these rules.
		Password Authentication	Strong authentication mechanisms are enforced prior to allowing users to access systems within the CDR data environment, including, but not limited

Schedule 1—Steps for privacy safeguard 12—security of CDR data held by accredited data recipients

	Control requirements	Minimum controls	Description of minimum controls
			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 objective 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.

Schedule 1—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 export, screen scraping or download of CDR data presented in applications; and (b) blocking access to unapproved cloud computing services; and (c) logging and monitoring the recipient, file size and frequency of outbound emails; and (d) email filtering and blocking methods that block emails with CDR data in text and attachments; and (e) 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 ADR 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 subrule 7.8(2), destruction and de-identification.
4	An accredited data recipient must implement a formal vulnerability management program to identify, track and remediate vulnerabilities within the CDR	Security patching	A systematic program is implemented for identifying, testing and applying security patches to applications and operating systems in a timely manner. All “extreme risk” vulnerabilities are targeted for patching within 48 hours of identification.

Schedule 1—Steps for privacy safeguard 12—security of CDR data held by accredited data recipients

	Control requirements	Minimum controls	Description of minimum controls
	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.

Schedule 1—Steps for privacy safeguard 12—security of CDR data held by accredited data recipients

	Control requirements	Minimum controls	Description of minimum controls
6	An accredited data recipient must implement a formal information security training and awareness program for all personnel interacting with CDR data.	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.
		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 2—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, and these are defined in Part 1 of this Schedule.

Part 2 of this Schedule deals with CDR data that can be disclosed when product data requests and consumer data requests are made in relation to the banking sector.

Part 3 of this Schedule deals with joint accounts within the banking sector.

Part 4 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 5 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 4.1 of this Schedule.

any other relevant ADI has the meaning given by clause 4.1 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.

initial data holder has the meaning given by clause 4.1 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 3.2(3) of this Schedule.

phase 1 product has the meaning given by clause 4.3 of this Schedule.

phase 2 product has the meaning given by clause 4.3 of this Schedule.

phase 3 product has the meaning given by clause 4.3 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 4.1 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	means: (a) the person's name; and (b) the person's contact details, including their: (i) telephone number; and (ii) email address; and (iii) physical address; and (c) any information that: (i) the person provided at the time of acquiring a particular product; and (ii) relates to their eligibility to acquire that product; and (d) if the person operates a business—the following: (i) the person's business name; (ii) the person's ABN (within the meaning of the *A New Tax System (Australian Business Number) Act 1999*); (iii) the person's ACN (within the meaning of the *Corporations Act 2001*); (iv) the type of business; (v) the date the business was established; (vi) the registration date; (vii) the organisation type; (viii) the country of registration;

Schedule 2—Provisions relevant to the banking sector

Meaning of *customer data*, *account data*, *transaction data* and *product specific data*		
	Column 1	**Column 2**
		(ix) whether the business is a charitable or not-for-profit organisation; and (e) any other information that is specified in the data standards as being ***customer data*** in relation to a person. However, if the person is an individual, ***customer data*** in relation to the person does not include the person's date of birth.
2	***account data***, in relation to a particular account	means: (a) the account number; and (b) the account name; and (c) the opening and closing balances for the account, including a current balance and available funds; and (d) any authorisations on the account, including: (i) direct debit deductions, including, to the extent available: (A) identifying information for the merchant or party that has debited the account; and (B) the amount the merchant or party has debited on each occasion; and (C) the date the merchant or party has debited the account; and (ii) scheduled payments (for example, regular payments, payments to billers and international payments); and (iii) details of payees stored with the account, such as those entered by the customer in a payee address book; and (e) any other information that is specified in the data standards as being ***account data*** in relation to a particular account.
3	***transaction data***, in relation to a particular transaction	means: (a) the date on which the transaction occurred; and (b) any identifier for the counter-party to the transaction; and (c) if the counter-party is a merchant—any information that was provided by the merchant in relation to the transaction; and (d) the amount debited or credited pursuant to the transaction; and (e) any description of the transaction; and (f) the "simple categorisation" of the transaction (for example, whether the transaction is a debit, a credit, a fee or interest); and (g) any other information that is specified in the data standards as being ***transaction data*** in relation to a particular transaction.
4	***product specific data***, in relation to a particular product	means the following data about the product: (a) its type; (b) its name; (c) its price, including fees, charges and interest rates (however described);

Schedule 2—Provisions relevant to the banking sector

Meaning of *customer data*, *account data*, *transaction data* and *product specific data*	
Column 1	**Column 2**
	(d) associated features and benefits, including discounts and bundles; (e) associated terms and conditions; (f) customer eligibility requirements; (g) any other information that is specified in the data standards as being ***product specific data*** in relation to a particular product.

Part 2—CDR data that may be accessed under these rules—banking sector

2.1 Required product data—banking sector

For these rules, ***required product data***, in relation to the banking sector, means CDR data:

(a) that is primary CDR data; and

(b) for which there are no CDR consumers; and

(c) that is about the eligibility criteria, terms and conditions, price, availability or performance of a product; and

(d) in the case where the CDR data is about availability or performance—that is publicly available; and

(e) that is product specific data about particular products; and

(f) that is held in a digital form.

Note 1: See subsection 56AI(3) for the meaning of "CDR consumer".

Note 2: Paragraphs (b), (c) and (d) are based on subsection 56BF(1) of the Act.

2.2 Required consumer data—banking sector

(1) For these rules, subject to subrule (2), CDR data is ***required consumer data*** in relation to the banking sector for a consumer data request made by or on behalf of a particular CDR consumer at a particular time if:

(a) the data is primary CDR data; and

(b) the data is:

(i) customer data in relation to that consumer; or

(ii) account data in relation to an account held by that consumer:

(A) in their name alone; or

(B) if the person is an individual—jointly with 1 other individual; or

(iii) transaction data in relation to a transaction relating to such an account; or

(iv) product specific data in relation to a product that the consumer uses; and

(c) the data is held by the data holder in a digital form; and

(d) the consumer is, at that time, able to access products of the data holder online, for example, using an internet browser or a mobile phone application;

(e) the consumer has an account with the data holder that:

(i) is active when the request is made; or

(ii) is not active at that time, but was closed on or after 1 January 2017.

Note 1: "Required consumer data" does not include derived data.

Note 2: For subparagraph (b)(ii), consumer data requests cannot be made under these rules in relation to any other kinds of joint accounts.

Schedule 2—Provisions relevant to the banking sector

Note 3: For subparagraph (b)(iv), for a consumer data request, product specific data could include the following:

- any product prices that were negotiated individually with the 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 the consumer.

Note 3: So long as the CDR consumer has an account that satisfies paragraph (1)(e), 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 accounts that do not themselves satisfy that paragraph.

(2) Despite subclause (1):

(a) CDR data is not ***required consumer data*** at a particular time if the data is:

(i) customer data in relation to a consumer who is, at that time, less than 18 years of age; or

(ii) account data in relation to an account for which any of the joint account holders is less than 18 years of age at that time; or

(iii) transaction data in relation to a transaction on such an account; or

(iv) product specific data in relation to a product that the consumer uses; and

(b) for a particular joint account holder, customer data in relation to the other joint account holder is not ***required consumer data***.

Part 3—Joint accounts

Division 3.1—Preliminary

3.1 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.

3.2 Joint account management service

(1) A data holder must provide a service for joint accounts with the data holder that can be used by the joint account holders to:
  (a) 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) revoke, to the satisfaction of the data holder, such an election.

(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***.

Division 3.2—Consumer data requests made by CDR consumers—joint accounts

3.3 Refusal to disclose—request not made by authorised joint account holder

(1) This clause applies if:
  (a) a data holder receives a request under Part 3 of these rules from a CDR consumer for required consumer data that is:
    (i) account data in relation to a particular account held by the consumer jointly with another person; or
    (ii) customer data in relation to the consumer; or
    (iii) transaction data in relation to a transaction on the account; or
    (iv) product specific data in relation to a product relating to the account;

(whether or not the request is also for other CDR data); and

(b) in the case that the request was made by 1 of the joint account holders only—the election referred to in paragraph 3.2(1)(a) of this Schedule has not been made, or has been made and revoked; and

(c) in the case that the request was made by both of the joint account holders together (if offered by the data holder)—the election referred to in paragraph 3.2(2)(b) of this Schedule (if offered by the data holder) has not been made, or has been made and revoked.

(2) Despite subrule 3.4(1) of these rules, the data holder must refuse to disclose any of the requested data referred to in paragraph (1)(a).

Note 1: This clause does not prevent disclosure of any CDR data that is the subject of the request which does not relate to the joint account.

Note 2: This ground of refusal is in addition to other grounds on which the request could be refused: see rule 3.5 of these rules.

Division 3.3—Consumer data requests made by accredited persons—joint accounts

3.4 Consumer dashboard for joint accounts—data holder

If, for a particular joint account with a data holder:

(a) the election referred to in paragraph 3.2(1)(a) of this Schedule, or paragraph 3.2(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 1.14(1) of these rules;

the data holder must also provide a 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.

3.5 Refusal to disclose—election to share data on joint account not made

(1) This clause applies if:

(a) a data holder receives, from an accredited person, a consumer data request; and

(b) some or all of the data that is the subject of the request relates to one or more joint accounts (whether or not the data also relates to other accounts); and

(c) the election referred to in paragraph 3.2(1)(a) of this Schedule, or paragraph 3.2(2)(b) of this Schedule (if offered by the data holder), has not been made, or has been made and revoked.

Note: A request to which this clause applies would be made under Part 4 of these rules.

(2) The data holder must refuse to disclose any CDR data that relates to the joint account.

Note 1: This clause does not prevent disclosure of any CDR data that is the subject of the request which does not relate to the joint account.

Note 2: This ground of refusal is in addition to other grounds on which the request could be refused: see rule 4.7 of these rules.

3.6 Seeking authorisation to share CDR data—joint accounts

(1) This clause applies if:

(a) a data holder has received, from an accredited person, a consumer data request; and

(b) some or all of the data that is the subject of the request relates to a joint account (whether or not the request also relates to other accounts); and

(c) the request was made by the accredited person on behalf of 1 of the joint account holders only;

(d) the joint account holders have made the election referred to in paragraph 3.2(2)(b) of this Schedule (if offered by the data holder), but not the election referred to in paragraph 3.2(1)(a) of this Schedule.

Note: A request to which this clause applies would be made under Part 4 of these rules.

(2) Rule 4.5 and subrule 4.6(1) of these rules do not apply.

(3) Instead, subject to rule 4.7 of these rules:

(a) if either or both of the joint account holders have not given a current authorisation to disclose the requested data, to the extent that it relates to the joint account, the data holder must, in accordance with Division 4.5 of these rules, and as soon as practicable, ask the joint account holders who have not given such an authorisation to give such an authorisation; and

(b) the data holder must disclose, to the accredited person, the requested data that it is authorised to disclose.

Note: This clause does not prevent disclosure of any CDR data that is the subject of the request which does not relate to the joint account.

3.7 Withdrawing authorisations—joint accounts

(1) An authorisation to disclose the CDR referred to in subclause 3.6(3) of this Schedule may be withdrawn by either of the joint account holders individually.

(2) For the purposes of paragraph 4.25(1)(a) of these rules, a withdrawal under this clause is taken to be under rule 4.24 of these rules.

3.8 Privacy safeguard 10—special rules for joint accounts

(1) For subsection 56EM(1) of the Act, this clause applies if a data holder discloses CDR data relating to a joint account to an accredited person as a result of a consumer data request.

(2) The data holder must update the consumer dashboard for both joint account holders whenever CDR data that relates to the joint account is disclosed pursuant to the request, as soon as practicable, to indicate the information referred to in

paragraphs 7.6(c), (d) and (e) of these rules insofar as it relates to the joint account.

Part 4—Staged application of these rules to the banking sector

4.1 Meaning of *initial data holder*, *voluntarily participating data holder*, *accredited data holder* and *any other data holder to which this Schedule applies*

For this Part, a term listed in column 1 of the table has the meaning given by column 2.

Meaning of *initial data holder*, *voluntarily participating data holder*, *accredited data holder* and *any other data holder to which this Schedule applies*

	Column 1	Column 2
1	***initial data holder***	Any of the following: (a) Australia and New Zealand Banking Group Limited; (b) Commonwealth Bank of Australia; (c) National Australian Bank Limited; (d) Westpac Banking Corporation. Note: Clause 4.4 of this Schedule deals with the staged application of these rules to a progressively wider range of data holders and in respect of a progressively wider range of products. For initial data holders, these rules initially apply only in relation to products that are branded with the name of the data holder, and progressively apply to products offered by the data holder that are branded differently: see clause 4.4 of this Schedule.
2	***accredited ADI***	An ADI that: (a) is an accredited person; and (b) is not: (i) an initial data holder; or (ii) a foreign bank branch licensed to conduct banking business in Australia through branches; or (iii) a foreign branch of a domestic bank.
3	***voluntarily participating ADI***	An ADI that: (a) has given the Commission a notification in accordance with clause 4.2 of this Schedule; and (b) is not an accredited ADI.
4	***any other relevant ADI***	An ADI that is not: (a) an initial data holder; or (b) a voluntarily participating ADI; or

Meaning of *initial data holder*, *voluntarily participating data holder*, *accredited data holder* and *any other data holder to which this Schedule applies*	
Column 1	**Column 2**
	(c) an accredited ADI; or (d) a foreign bank branch licensed to conduct banking business in Australia through branches; or (e) a foreign bank branch of a domestic bank.

4.2 Election to voluntarily participate in CDR scheme early

(1) An ADI that:

(a) is a data holder; and

(b) is not an initial data holder;

may notify the Commission, in writing, that it is electing to be treated as a voluntarily participating ADI from 1 July 2019.

Note 1: Such an ADI is a "voluntarily participating ADI": see clause 4.4 of this Schedule for how the rules apply in relation to such an ADI.

Note 2: 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) The Commission must publish, on its website, a list of ADIs that have given a notification under this clause.

4.3 Meaning of *phase 1 product*, *phase 2 product* and *phase 3 product*

For this Part, the table has effect:

Meaning of *phase 1 product*, *phase 2 product* and *phase 3 product*		
	The following term:	**means a product that is offered to the general public 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 credit and charge card (personal) account; (k) a credit and charge card (business) account.
2	***phase 2 product***	(a) a residential mortgage; (b) an investment mortgage;

Schedule 2—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 offered to the general public and is generally known as being of any of the following types:**
		(c) a mortgage offset account.
3	***phase 3 product***	(a) business finance; (b) a personal loan; (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 leases.

4.4 Staged application of these rules to the banking sector

During the period referred to in column 1 of the table to this rule, requests may be made to a person referred to in column 2 for disclosure of data that is of a kind referred to in column 3.

	Column 1	**Column 2**	**Column 3**	**Column 4**
	During the period:	**the following:**	**may be made to:**	**for disclosure of CDR data relating to:**
1	between: (a) 1 July 2019; and (b) 31 January 2020;	a product data request;	an initial data holder;	a phase 1 product that is branded with the name of the bank.
		a product data request;	a voluntarily participating ADI;	a phase 1 product.

Schedule 2—Provisions relevant to the banking sector

	Column 1 During the period:	Column 2 the following:	Column 3 may be made to:	Column 4 for disclosure of CDR data relating to:
2	between: (a) 1 February 2020; and (b) 30 June 2020;	a product data request or a consumer data request;	an initial data holder;	any of the following: (a) a phase 1 product that is branded with the name of the bank; (b) a phase 2 product that is branded with the name of the bank.
		a product data request or a consumer data request;	an accredited ADI;	any of the following: (a) a phase 1 product; (b) a phase 2 product.
		a product data request;	a voluntarily participating ADI;	any of the following: (a) a phase 1 product; (b) a phase 2 product.
3	between: (a) 1 July 2020; and (b) 31 January 2021;	a product data request or a consumer data request;	an initial data holder;	any of the following: (a) a phase 1 product; (b) a phase 2 product that is branded with the name of the bank; (c) a phase 3 product that is branded with the name of the bank.
		a product data request or a consumer data request;	an accredited ADI;	any of the following: (a) a phase 1 product; (b) a phase 2 product; (c) a phase 3 product.
		a product data request or a consumer data request;	a voluntarily participating ADI;	any of the following: (a) a phase 1 product; (b) a phase 2 product; (c) a phase 3 product.
		a product data request or a consumer data request;	any other relevant ADI;	a phase 1 product.

Schedule 2—Provisions relevant to the banking sector

	Column 1 During the period:	Column 2 the following:	Column 3 may be made to:	Column 4 for disclosure of CDR data relating to:
4	between: (a) 1 February 2021; and (b) 30 June 2021;	a product data request or a consumer data request;	an initial data holder;	any of the following: (a) a phase 1 product; (b) a phase 2 product; (c) a phase 3 product that is branded with the name of the bank.
		a product data request or a consumer data request;	an accredited ADI;	any of the following: (a) a phase 1 product; (b) a phase 2 product; (c) a phase 3 product.
		a product data request or a consumer data request;	a voluntarily participating ADI;	any of the following: (a) a phase 1 product; (b) a phase 2 product; (c) a phase 3 product.
		a product data request or a consumer data request;	any other relevant ADI:	any of the following: (a) a phase 1 product; (b) a phase 2 product.
5	on or after 1 July 2021;	a product data request or a consumer data request;	(a) an ADI; or (b) a data holder that is an accredited person; other than: (c) a foreign bank branch licensed to conduct banking business in Australia through branches; or (d) a foreign bank branch of a domestic bank.	any of the following: (a) a phase 1 product; (b) a phase 2 product; (c) a phase 3 product.

Part 5—Other modifications of these rules for the banking sector

5.1 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.

5.2 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 rules 5.6 and 5.11 of these rules.

(2) An accredited person that is an ADI or a PPF provider need not comply with paragraph 5.11(e) of these rules.