Explanatory Statement

Proposed Competition and Consumer (Consumer Data Right) Rules 2019 – August 2019

Prepared by the Australian Competition and Consumer Commission

Contents

Explanatory Statement – Competition and Consumer (Consumer Data Right) Rules 2019

Background

1.1. This explanatory statement accompanies the *Competition and Consumer (Consumer Data) Rules 2019* (**rules**).

1.2. The Consumer Data Right (**CDR**) is an economy-wide reform that will apply sector-by-sector, starting with the banking sector. The objective of the CDR is to provide consumers with the ability to efficiently and conveniently access specified data held about them by businesses (data holders), and to authorise the secure disclosure of that data to third parties (accredited data recipients) or to themselves. The CDR also requires businesses to provide public access to information on specified products that they offer. The right is designed to give consumers more control over their data, leading, for example, to more choice in where they take their business and more convenience in managing their services.

1.3. The CDR is a new regime that operates in addition to existing data sharing arrangements and practices. In the banking sector, the CDR operates in addition to the mechanisms by which banks currently provide information to their customers, such as through bank statements that are available online, for download. The CDR also does not prevent alternative data sharing arrangements that are used by consumers to access goods or services.

1.4. The CDR is regulated by both the Australian Competition and Consumer Commission (**ACCC**) and the Office of the Australian Information Commissioner (**OAIC**) as it concerns both competition and consumer matters as well as the privacy and confidentiality of consumer data. The ACCC leads on issues concerning the designation of new sectors of the economy to be subject to the CDR and the establishment of the CDR rules. The OAIC leads on matters relating to the protection of individual and small business consumer participants' privacy and confidentiality, and compliance with the CDR Privacy Safeguards (**Privacy Safeguards**).

1.5. A Data Standards Body assists the Data Standards Chair in making data standards for the CDR. The data standards prescribe the format and process by which CDR data is to be shared with consumers and accredited data recipients within the CDR system.

Authority and purpose for making the rules

1.6. The *Treasury Laws Amendment (Consumer Data Right) Act 2019* inserted a new Part IVD into the *Competition and Consumer Commission Act 2010* (the **Act**) to enact the CDR.

1.7. Under s 56BA(1) of the Act, the ACCC is empowered to make rules with the consent of the Minister (s 56BR). The ACCC must have regard to certain matters before making the rules, including the likely effect of the rules on the interests of consumers, the efficiency of relevant markets, the privacy and confidentiality of consumers' information, and the regulatory impact of the rules. The CDR rules may deal with all aspects of the CDR regime (as provided in Part IVD of the Act) including the accreditation process, the use and disclosure of CDR data, dispute resolution, and in relation to the privacy safeguards.

1.8. Initially, the CDR rules will apply only to certain products that are offered by certain data holders in the banking sector. It is intended that the rules will progressively apply to a broader range of data holders and products over time.

Statement of compatibility with human rights

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

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

Human right implications

1.11. The rules invoke the right to protection from unlawful or arbitrary interference with privacy under Art 17 of the International Covenant on Civil and Political Rights (the **ICCPR**) because they enable consumers to authorise data sharing and use in a regulated manner that is subject to Privacy Safeguards. They provide individuals and businesses with a right to access data relating to them, and to consent to secure access by accredited third parties.

1.12. The rules provide for important mechanisms for protecting consumers' privacy including by setting out requirements relevant to the Privacy Safeguards provided for under the Act. These are broadly similar to the Australian Privacy Principles in the *Privacy Act 1988* and seek to ensure the privacy and confidentiality of consumers' data, ensuring only authorised use and access. A further mechanism for protecting consumers' privacy is the requirements in the rules that a consumer has to expressly consent to any disclosure or use of their data, including requirements around transparency on who has requested access to the data and how it will be used.

1.13. Accreditation of third parties to enable them to collect and use CDR data is a key protection against arbitrary or unlawful interference with privacy. The rules specify the criteria for accreditation for the initial 'unrestricted' level of accreditation, are that the Data Recipient Accreditor is satisfied that an applicant for accreditation would be able to comply with the obligations of an accredited person. These obligations relevantly include that the person:

a. meets the requirements of being 'fit and proper' to manage CDR data

b. protects consumer data from misuse, interference and loss and unauthorised access, modification or disclosure as set out in Schedule 2 to the rules

c. have internal dispute resolution processes that meet the requirements in the rules

d. is a member of a recognised external dispute resolution scheme (which will be the Australian Financial Complaints authority for the banking sector) avenues available to the consumer.

1.14. In summary, the rules are consistent with Article 17 of the ICCPR, as they are proportional to the end sought and necessary in the circumstances.

1.15. The civil penalty provisions in the rules potentially invoke Articles 14 and 15 of the ICCPR. Although the Articles cover criminal process rights, in international human rights law, where a civil penalty is imposed, it must be determined whether it nevertheless amounts to a 'criminal' penalty. The civil penalty provisions should not be considered 'criminal' for this purpose. While they are intended to deter non-

compliance with CDR obligations, none of the provisions carry a penalty of imprisonment for non-payment of a penalty.

Conclusion

1.16. The rules are compatible with human rights and freedoms.

Consultation

1.17. In developing the rules, the ACCC consulted on a framework for the rules from 11 September 2018 to 12 October 2018, and published a document for public consultation titled *Consumer Data Right Rules Framework, September 2018* (Rules Framework). The Rules Framework provided stakeholders with the proposed structure and content of the rules, including a phased approach to implementation.

1.18. On 21 December 2018 the ACCC released the *Consumer Data Right Rules Outline, December 2018* (Rules Outline), setting out the ACCC's position on the rules and responding to stakeholder views on the Rules Framework.

1.19. An Exposure Draft of the rules was released on 29 March 2019 covering the key aspects of the rules required to implement the CDR in banking. The ACCC has considered and taken into account stakeholder feedback in finalising these rules.

1.20. Prior to this, the Australian Government consulted extensively on the *Treasury Laws Amendment (Consumer Data Right) Bill 2018* between 15 August and 7 September 2018, and again between 24 September and 12 October 2018.

Explanatory notes

Part 1 – Preliminary

Division 1.1 – Preliminary

Rules 1.1 to 1.3

1.21. The rules will commence the day after they are registered on the Federal Register of Legislation. The authority and purpose for making the rules is outlined at paragraphs 1.6 to 1.8 of this explanatory statement.

Division 1.2 – Simplified outline and overview of these rules

Rules 1.4 to 1.6

1.22. The three types of CDR data requests that can be made under the rules are:

a. product data requests made by any person

b. consumer data requests made by CDR consumers

c. consumer data requests made on behalf of CDR consumers by accredited data recipients.

1.23. Product data is data for which there are no CDR consumers while consumer data relates to an identifiable, or reasonably identifiable, CDR consumer.

1.24. The simplified outline in the rules broadly sets out what the rules are about, the other documents that should be read together with the rules, and an overview of the different parts of the rules and what they contain.

Division 1.3 – Interpretation

Rules 1.7 to 1.10

1.25. Rules 1.7 to 1.10 contain defined terms or expressions used in the rules.

1.26. Certain terms in the rules have the meaning as defined in the Act while other definitions are specific to the rules, or have their meaning affected by the rules. For example, the terms at rule 1.7(2) are to be interpreted differently according to the context in which they appear throughout the rules.

1.27. One example of a term that has its meaning affected by the rules is that of '***CDR consumer***'. CDR consumer is a term defined in the legislation, however, only 'eligible' CDR consumers are able to make consumer data requests under the rules. It is intended that the rules will progressively apply to a broader range of consumers over time. Schedule 3, clause 2.1 provides a CDR consumer for the banking sector is eligible if the consumer:

a. is 18 years or older; and

b. has an account with the data holder that is an open account and set up in such a way that it can be accessed online.

1.28. In this explanatory statement references to requests made by consumers are references to requests made by eligible CDR consumers, unless stated otherwise.

1.29. The rules contain references to both '***accredited persons***' and '***accredited data recipients***' in various places. An accredited person is accredited to receive data through the CDR once certain requirements set out in the Rules have been met. An accredited data recipient is an accredited person that has received CDR data. Many obligations apply from the point at which a person is accredited, whereas the privacy safeguards apply only to accredited data recipients. For the avoidance of doubt, all accredited data recipients are also accredited persons.

1.30. For ***outsourced service provider***, and ***CDR outsourcing arrangement***, see paragraph 1.42.

1.31. Two key concepts defined in Part 1 of the rules are the ***data minimisation principle*** and the ***fit and proper person criteria***.

a. The ***data minimisation principle***:

Under the CDR, accredited persons must not seek to collect and must not use data beyond what is reasonably needed to provide the good or service that a consumer has consented to, or for a longer time period than is reasonably required.

b. The ***fit and proper person criteria***:

One of the criteria to become accredited (and maintain accredited status) is that the Data Recipient Accreditor is satisfied that the applicant (and associated persons as defined in the rules) is a person that is a fit and proper person to manage CDR data. Rule 1.9 specifies the criteria to be taken into account by the Data Recipient Accreditor in deciding whether the fit and proper person test under the rules is satisfied. The fit and proper person criteria take into account a range of matters including whether a person has a criminal history and whether they have been found to have contravened a law relevant to the management of CDR data.

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

Subdivision 1.4.1 – Preliminary

Rule 1.11

1.32. The simplified outline sets out the general obligations of data holders for product data requests and consumer data requests, as well as the general obligations for data holders and accredited persons to provide CDR consumers with consumer dashboards.

Subdivision 1.4.2 – Services for making requests under these rules

Rules 1.12 and 1.13

1.33. Part 1 also deals with services that must be provided by data holders and accredited persons to facilitate the making and management of requests to disclose or use data.

1.34. Data holders must provide an online service that can be used by:

a. persons to make requests for product information (***product data request service***). The service must conform to the data standards and enable data to be disclosed in machine-readable form

b. consumers to make requests for their own data (***direct request service***). The service must be as timely, efficient and as convenient as other online services ordinarily used by customers of the data holder, enable data to be disclosed in human-readable form, and conform to the data standards

c. accredited persons to make consumer data requests on behalf of CDR consumers (***accredited person request service***). The service must conform to the data standards and enable data to be disclosed in machine-readable form.

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

Rules 1.14 to 1.15

1.35. Accredited persons are required to provide consumers with a consumer dashboard that will enable them to see and manage their consents for the collection and use of their CDR data. Data holders are required to provide consumers with a consumer dashboard that will enable consumers to see and manage their authorisations for the disclosure of CDR data.

1.36. The rules set out requirements for information that must be displayed on a dashboard. It is up to data holders and accredited persons as to how this information is presented to consumers, provided that the required information is made available on the dashboard.

1.37. The dashboards are required to be an online service and therefore they may be built in to online banking or mobile apps.

Accredited person dashboard

1.38. The dashboard must contain a functionality that allows a CDR consumer, at any time, to withdraw authorisations to disclose CDR data, and:

a. is simple and straightforward to use; and

b. is prominently displayed; and

c. is no more complicated than the process for giving the authorisation to disclose the CDR data; and

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

1.39. The accredited person's dashboard must also contain the details of each consent to collect and use CDR data given by the CDR consumer, including information about the data to which the consent relates and the uses to which the consent relates (see rule 1.14).

Data holder dashboard

1.40. The dashboard must contain a functionality that:

e. allows a CDR consumer, at any time, to:

i. withdraw consents to collect and use CDR data

ii. elect that redundant data be deleted and withdraw such an election; and

f. is simple and straightforward to use; and

g. is prominently displayed.

1.41. The data holder's dashboard must also contain the details of each authorisation to disclose CDR data given by the CDR consumer, including information about the data to which the authorisation relates and the name of the accredited person who made the consumer data request (see rules 1.15 and 7.9).

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

CDR outsourcing arrangements

Rule 1.16

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

1.43. Under rule 1.10, a CDR outsourcing arrangement involves a person (the discloser) disclosing CDR data to another person (the recipient) under a CDR outsourcing arrangement if it is done under a written contract between the discloser and the recipient, under which:

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

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

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

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

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

a. return to the discloser CDR data that the discloser disclosed to it;

b. delete CDR data that it holds in accordance with the CDR data deletion process;

c. provide, to the discloser, records of any deletion that are required to be made under the CDR data deletion process;

d. direct any other person to which it has disclosed CDR data to take corresponding steps; and

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

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

Example 1: B3 is an accredited data recipient. B3's service has been very popular and it no longer has the storage capacity to facilitate any growth. B3 contracts B4, a reputable storage provider, to help meet its storage requirements. B4 subcontracts B3's storage to Bat.

In order to comply with the rules, there must be a contract between B3 and B4, and a contract between B4 and Bat that require the outsourced service provider, and in turn each subcontractor, to comply with the outsourced service provider requirements contained in the rules. B3 must ensure that B4 complies with its requirements under the arrangement which in turn requires that B4 must ensure that Bat complies with its requirements.

Sub-division 1.4.5 – Deletion and de-identification of CDR data

Rules 1.17 and 1.18

CDR data de-identification process

1.44. The rules set out the process by which particular CDR data (the relevant data) must be de-identified:

a. for the purposes of Privacy Safeguard 12 (rule 7.11)

b. in accordance with a consumer's consent, where the de-identified data will be disclosed (by sale or otherwise) as a use of collected CDR data (rules 4.11(3)(e) and 4.12(3)(a)).

1.45. Before de-identifying the relevant data, an accredited data recipient must consider whether the data in question is able to be de-identified to the extent that no person would any longer be identifiable, or reasonably identifiable, from the relevant data and other information that would be held by any person (the required extent).

1.46. In making this assessment, an accredited data recipient must have regard to:

a. the OAIC and Data61's *De-identification Decision-Making Framework* (**DDF**)

b. the techniques that are available for the de-identification of data

c. the extent to which it would be technically possible for any person to be once more identifiable (re-identified), or reasonably identifiable, after applying such techniques to the data

d. the likelihood (if any) of a person being re-identified, or once more reasonably identifiable, from the data after it is de-identified.

1.47. Only CDR data that is de-identified to the required extent, having regard to the above factors:

a. meets the level of de-identification required for the purposes of Privacy Safeguard 12

b. subject to a consumer's consent, is able to disclosed (by sale or otherwise) to other persons during the consent period.

1.48. If it is not possible to de-identify the CDR data or data derived from that data to the required extent, the data must be deleted.

1.49. If, in making the assessment described in paragraph 1.3, an accredited data recipient decides that CDR data can be de-identified to the required extent, the accredited data recipient must apply the appropriate technique to achieve this outcome.

1.50. In applying the de-identification process, an accredited data recipient must delete, in accordance with the deletion process described below, any CDR data that must be deleted in order to ensure the remaining data is de-identified to the relevant extent.

1.51. An accredited data recipient must make certain records relating to the de-identification process. These are required to be kept, in accordance with the record keeping rules (see rule 9.3), to evidence:

a. the assessment made by the accredited data recipient that it is possible to de-identify the relevant data to the required extent

b. that the relevant data was de-identified to that extent

c. how the relevant data was de-identified, including the technique applied to the data

d. any persons to whom the de-identified data is disclosed.

1.52. The requirement to record persons to whom the de-identified data is disclosed is not a time-limited obligation – a record must be made every time the de-identified data is so disclosed.

1.53. The ACCC considers that a data standard for de-identification will be useful and expects that this may be required in a later version of the rules.

CDR data deletion process

1.54. If an accredited data recipient is required to delete CDR data, including to treat redundant data, the accredited data recipient must:

a. delete, to the extent reasonably practicable, the data and any copies of the data

b. make a record to evidence the deletion

c. direct any other person to which it has disclosed the CDR data to:

i. delete, to the extent reasonably practicable, any copies of the data (including any data derived from the disclosed data)

ii. make a record to evidence the steps taken to delete the CDR data

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

Part 2 – Product data requests

Rules 2.1 to 2.6

1.55. One of the objectives of the CDR is to enable the efficient and convenient access to information about products or services in a particular sector. The disclosure of product data in a standardised form is expected to make product comparisons easier for consumers through existing and new services, such as comparison services.

Example 2: A product comparison website makes a series of product data requests to a range of financial institutions. The data collected enables the comparison site to publish a report on the highest interest rates currently available for savings accounts.

1.56. Product data for the purposes of the CDR, is data that does not relate to any particular identifiable consumer. It includes information about terms and conditions, eligibility criteria, and the pricing and availability of products.

1.57. A product data request may be for required product data, voluntary product data or both. While a fee cannot be charged for the disclosure of required product data, a fee can be charged for disclosing voluntary product data.

1.58. Data holders are required to provide a product data request service that can be used to make product data requests by any person. The requester must make their request in accordance with the data standards (paragraph 2.3(1)(b)). The standards require the product data request service to be via an API.

1.59. Subrule 2.4(3) provides the data holder must disclose to the requester, in machine readable form and in accordance with the data standards, the product data the requester has sought. The required product data must include data that is contained on the data holder's website or in a product disclosure statement that relates to the product. This is a qualitative rule intended to ensure that product data provided in accordance with the standards is commensurate to the product data made available publically by a data holder through its website or in product disclose statement relating to a relevant product.

1.60. A data holder must not impose conditions, restrictions or limitations of any kind on the use of the data, with the person who receives the data able to use the product data in any way they wish.

1.61. Rule 2.5 provides that in certain circumstances, a data holder may refuse to disclose required product data in response to the request as set out in the data standards. Where this occurs, the data holder must inform the requester of the refusal, in accordance with the data standards.

Part 3 – Consumer data requests made by eligible CDR consumers

Division 3.1 – Preliminary

Rules 3.1 and 3.2

1.62. The CDR facilitates consumers receiving their own CDR data directly, in human-readable form, from a data holder. This data is required to be shared in human-readable form, rather than machine-readable, as it is not practical for most consumers to receive their data through APIs and due to the added security risks in relation to a machine-readable approach. The obligation to share CDR data directly with consumers will commence at different times for different classes of data holder, see from paragraph 1.276. The rules require a standard to be made by the Data Standards Chair; this will be developed for implementation by July 2020.

Division 3.2 – Consumer data requests made by CDR consumers

Rules 3.3 to 3.5

1.63. If a data holder holds CDR data that relates to a CDR consumer, the consumer may request the data holder to provide them with all or part of that data. A data holder cannot charge a consumer for making a consumer data request in respect of required

consumer data and must not place any restrictions on what a consumer chooses to do with the disclosed information.

1.64. To facilitate consumer data requests, data holders are required to provide a 'direct request service'. The service must be as easy for consumers to access and use as existing online services ordinarily used by consumers to deal with the data holder.

Example 3: A consumer data request service could form part of a consumer's online banking website or mobile banking app.

1.65. The data holder may disclose any requested voluntary consumer data to the CDR consumer. The data holder must (subject to rule 3.5, see below), disclose any requested required consumer data to the CDR consumer who made the request through the direct request service and in accordance with the data standards.

1.66. In certain circumstances, a data holder may refuse to disclose required consumer data where the data holder considers this necessary to prevent physical or financial harm or abuse, or in accordance with the data standards. Where this occurs, the data holder must inform the CDR consumer of such a refusal in accordance with the data standards (which will require the request to be responded to with an error code as defined in the standards).

1.67. For consumer data requests made by consumers with a joint account, see from paragraph 1.259.

Part 4 – Consumer data requests made by accredited persons

Division 4.1 – Preliminary

Rules 4.1 and 4.2

1.68. To receive CDR data for the purpose of providing goods or services to an eligible CDR consumer, an accredited person must obtain the consumer's consent and make a consumer data request to the data holder to disclose the data.

1.69. If the accredited person makes a valid request to the data holder, the data holder must seek authorisation from the consumer to disclose the data. If the consumer authorises the data holder to disclose their data to the accredited person, the data holder must disclose the data requested to the accredited person.

1.70. The consumer data requests will be facilitated via APIs, as defined in the data standards. The rules and data standards outline the format for the provision of the data and how these processes must occur as well as circumstances in which a data holder can refuse to comply with a request.

Division 4.2 – Consumer data requests made by accredited persons

Rules 4.3 and 4.4

Requests to collect CDR data

1.71. If a consumer requests an accredited person to provide them, or another person, with goods or services that require the use of their CDR data, the accredited person may make a request to the data holder of the CDR data. The consumer must consent to the accredited person collecting and using their data to provide the specified goods or services, in order for the request to be valid.

1.72. An accredited person may request a data holder disclose, to the accredited person, CDR data that is subject to a valid and current consent to collect and use. An accredited person must only request the data holder disclose CDR data that it is able to collect and use in compliance with a current consent and the data minimisation principle.

1.73. An accredited person must make all valid requests through the data holder's accredited person request service and in accordance with the data standards. A data holder cannot charge an accredited person a fee for making a consumer data request where their request relates to required consumer data.

1.74. The accredited person may request the relevant data holder to disclose, to the accredited person, some or all of the CDR data.

Rules 4.5 to 4.7

Authorisations to disclose CDR data

1.75. A data holder must seek authorisation from a consumer to disclose CDR data to an accredited person. A data holder must seek authorisation from a consumer if:

a. it receives a consumer data request;

b. there is no current authorisation to disclose the requested data to the person who made the request; and

c. it reasonably believes that the request was made by an accredited person on behalf of an eligible consumer.

1.76. A data holder must ask the relevant consumer to authorise the disclosure of required consumer data. The authorisation request must be made in accordance with these rules and the data standards.

1.77. A data holder may ask the relevant consumer to authorise the disclosure of voluntary consumer data in accordance with these rules and the data standards.

1.78. If the voluntary consumer data or required consumer data relates to joint accounts, further steps may be required, as outlined in Part 4 of Schedule 3.

1.79. If a data holder receives authorisation from the relevant consumer, it may disclose any of the voluntary consumer data requested to the accredited person, through its accredited person request service and in accordance with the data standards.

1.80. If a data holder receives authorisation from the relevant consumer, it must disclose the required consumer data to the accredited person through its accredited person request service and in accordance with the data standards.

1.81. Under rule 4.7, a data holder may refuse to seek authorisation for CDR data, or refuse to disclose required CDR data if:

a. it considers it necessary in order to prevent physical or financial harm or abuse; or

b. it has reasonable grounds to believe that disclosure of some or all of the data would adversely impact the security, integrity or stability of the Register of Accredited Persons or the data holder's information and communication technology systems.

1.82. A data holder may also refuses to disclose data in response to a valid request in the circumstances provided in the standards and it must inform the accredited person of the refusal in accordance with the standards (this would involve responding to the request with an error code as defined in the standards).

Division 4.3 – Consents to collect and use CDR data

Sub-division 4.3.1 – Preliminary

Rules 4.8 and 4.9

1.83. Consent is one of the underlying concepts of the CDR system. While the CDR places a high threshold on consent, it is not intended to make consent so complex as to discourage participation in the CDR regime. The focus of consents to collect and use should be on transparency and ensuring consumers understand the potential consequences of what they are agreeing to. The objective of Division 4.3 is to ensure that consent given by a consumer to collect and use CDR data is:

a. voluntary;

b. express;

c. informed;

d. specific as to purpose;

e. time limited; and

f. easily withdrawn.

Sub-division 4.3.2 – Consents and their duration and withdrawal

Seeking consent

Rules 4.10 and 4.11

1.84. The accredited person's process for seeking consent (consent process) must be in line with the data standards, concise, and easy to understand. It is expected that at a minimum, accredited persons will be guided by the language and processes of guidelines produced by the Data Standards Body. The design of an accredited person's product or service should include consumer experience testing to ensure consumers' comprehension of the consent process.

1.85. Visual aids should be used where they are likely to improve consumer comprehension. For example, to visually demonstrate relationships, processes, concepts or results. Visual aids should be clear and concise and be of an appropriate size and quality.

1.86. The consent process must not include or refer to other documents if doing so would reduce the consumer's understanding of what they are agreeing to. The consumer should be able to understand the key elements of what data will be collected and how it will be used, without having to refer to other documents or sources.

1.87. Consent should be separated out, and never be bundled with other directions, permissions, consents or agreements.

1.88. The consumer must be able to actively select or clearly indicate their consent for:

a. the types of data to be collected (referred to as 'data clusters' in the data standards)

b. the specific uses for that data

c. a period over which CDR data will be collected and used, up to a maximum of 12 months, including whether CDR data may be:

    a. collected on a single occasion and used over a specified period of time; or

    b. collected and used over a specified period of time.

1.89. A consumer must also be asked their express consent for the accredited person to collect those types of CDR data over that period of time and for those uses of the collected CDR data. A consumer must also provide express consent to any direct marketing the accredited data recipient intends to undertake.

1.90. If the requested data includes voluntary consumer data, the accredited person must clearly distinguish between the required consumer data and the voluntary consumer data. If the data holder charges a fee for disclosure of voluntary consumer data which will be passed onto the consumer by the accredited person, the consumer must be able to actively select or otherwise clearly indicate whether they consent to the collection of that data, in line with the requirement for all CDR data.

1.91. A consumer must also be able to make an election in relation to deletion of redundant data.

1.92. The accredited person must not present pre-selected options to the consumer when requesting consent to collect and use data (subrule 4.11(2)).

Example 4: Light Years seeks consent to collect and use consumers' account information relating to their home loans. In order to provide its service, Light Years requires access to home loan transaction information dating back to the last six months, and makes these options the default by pre-selecting the options during the consent process. Light Years has not complied with the rules.

Example 5: Whey Bank allows consumers to select boxes that correspond to the data they consent to Whey Bank collecting and using in order to receive its service. Whey Bank complies with the requirement to allow consumers to actively select or otherwise clearly indicate their consent.

1.93. The consumer must also be presented with:

a. the accredited person's name

b. the accredited person's accreditation number

c. reasons why the accredited person must collect and use data over that period of time to provide the requested goods or services

d. if the request covers voluntary data that the data holder charges a fee for disclosure and the accredited person is intending to pass that fee on to the consumer:

    a. that fact

    b. the amount of the fee

c. the consequences if the consumer does not consent to the collection of that data.

e. if the accredited person is asking for consent to de-identify CDR data for the purpose of disclosing, including selling, the de-identified data

f. if the CDR data may be disclosed to an outsourced service provider, a statement of that fact, a link to the accredited person's CDR policy and a statement that the consumer can obtain further information about such disclosures from the policy if desired

g. a statement that consent may be withdrawn at any time during the consent period, instructions for how consent may be withdrawn, and a statement indicating any consequences for the consumer if they withdraw their consent, including any contractual consequences

h. statements regarding: the accredited person's intended treatment of redundant data, the consumer's right to elect that their redundant data be deleted and instructions for how the election may be made.

Example 6: GA is a company that offers support services to people that identify as having gambling problems. As part of its support service it encourages clients to access its Accountability app, which flags with GA any spending or withdrawals that may be related to gambling. In order to ensure GA's clients understand the types of data the Accountability app needs to offer this service, the Accountability app outlines to consumers:

Your name – this allows us to make sure we talk to you about your activities, not the activities of someone else

Transaction information – this allows us to provide you with our service.

GA has not sufficiently outlined to the consumer the reasons it must collect and use the consumer's transaction information to provide the requested service.

Restrictions on seeking consent

Rule 4.12

1.94. When asking a consumer to provide consent to the accredited person collecting and using their data, an accredited person must not ask a consumer for consent, or allow the consumer to elect to provide consent, for a period that exceeds 12 months.

1.95. To comply with the data minimisation principle, an accredited person must ensure that it is seeking only data that is directly required for the requested good or service, and must not seek consent for access to data in excess of what is required to deliver the requested good or service.

1.96. An accredited person must not ask consumers to give consent to use or disclose their data for any of the following uses or disclosures:

a. selling the CDR data, unless de-identified in accordance with the CDR data de-identification process

b. using the CDR data, including by aggregating the data, for the purpose of:

a. identifying;

b. compiling insights in relation to;

c. building a profile in relation to;

any identifiable person who is not the consumer who made the consumer data request.

Example 7: Shoe String Travel offers a service that tracks consumer spending while travelling. It breaks spending down into categories and creates budgets for each category, creates savings goals, as well as charting 'real spending' against 'budgeted spend'. During the consent process, Shoe String Travel asks consumers to consent to it providing their data to local accommodation business to see if the business can provide accommodation to the consumer for a price within their accommodation budget. Shoe String Travel has not complied with the rules, as it asks consumers to consent to it disclosing CDR data in a way prohibited by the rules, that is, by disclosing it to another party.

1.97. The requirement to not aggregate the data for the purpose of identifying, compiling insights in relation to, or building a profile in relation to any identifiable person who is not the consumer who made the consumer data request does not apply in relation to a person whose identity is readily apparent from the CDR data, if the accredited person is seeking consent to:

a. derive, from the CDR data, CDR data about the person's interactions with the CDR consumer; and

b. use that derived CDR data in order to provide the requested goods or services.

Example 8: Olivia uses a budgeting service that requires her CDR data. Olivia also owns a rental property, which is currently tenanted by Fabian. Fabian pays rent to Olivia on a monthly basis and also transfers Olivia money for the water bill quarterly. Sometimes Fabian will organise and pay to have maintenance work done on the property and Olivia will transfer Fabian the money for those services once completed. In Olivia's transaction data, Fabian is someone whose identity is readily apparent. Olivia's CDR budgeting service may consider Fabian's behaviour only in so far as it is relevant to Olivia's spending and saving habits for the purpose of providing Olivia with the budgeting service.

Withdrawal of consent

Rule 4.13

1.98. The withdrawal process under the rules will allow consumers to withdraw consent for an accredited person to collect and use data at any time. Consumers must, at a minimum, be able to withdraw consent by communicating the withdrawal to the accredited person in writing or using the process provided for on the accredited person's consumer dashboard. As above, consumers must be notified of the consequences for the consumer if they withdraw their consent, including any contractual consequences.

1.99. An accredited person must give effect to a withdrawal of consent it receives in writing as soon as practicable, and in any case within two business days after receiving the written request.

1.100. If a consent to collect and use data is withdrawn by a consumer, the accredited person must notify the data holder of the withdrawal in accordance with the data standards.

1.101. Withdrawal of consent does not impact a consumer's election to have their data destroyed, and in most cases may bring forward the date of destruction.

> **Example 9**: Octavia was recently gifted a mobile phone, but otherwise does not consider herself to be very technologically savvy. Octavia recently signed up for a service that uses her CDR data. Octavia now wants to withdraw consent from that service. Octavia calls the accredited person's customer helpline and they step her through how to withdraw her consent on the consumer dashboard.

Duration of consent

Rule 4.14

1.102. Consent to collect and use CDR data expires at the earliest of the following:

a. if the consumer withdraws consent by communicating the withdrawal to the accredited person in writing, the earliest of:

   i. when the accredited person gave effect to the withdrawal

   ii. two business days after the accredited person received the written communication

b. if the consent was withdrawn by using the accredited person's consumer dashboard, when the consent was withdrawn

c. if the accredited person was notified of the withdrawal of the authorisation to disclose that data, when the accredited person received that notification

d. at the end of 12 months after the consent was given

e. at the end of the period the consumer consents to the accredited person collecting and using their data.

1.103. If an accredited person's accreditation is revoked or surrendered, all consents for the accredited person to collect and use data expires at the time revocation or surrender takes effect (subrule 4.14(2)).

Subdivision 4.3.3 – De-identification of CDR data for the purpose of providing goods or services to a CDR consumer

Rule 4.15

1.104. If an accredited person asks a CDR consumer for their consent to de-identify some or all of their collected CDR data for the purpose of disclosing (including by selling) the de-identified data under rule 4.11(3)(e), the accredited person must also provide the consumer with the following information:

a. what the CDR data de-identification process is

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

c. the classes of persons to which it would disclose that data

d. why it would so disclose that data

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

1.105. The purpose of this rule is to ensure that a consumer makes an informed decision about whether or not to consent to a use that includes the de-identification of their data, and the disclosure of that data. For instance, an accredited person may ask for a consumer's consent to sell their de-identified data in order for the consumer to receive the good or service provided by the accredited person free of charge.

Subdivision 4.3.4 – Election to delete redundant data

Rule 4.16

Election to delete redundant data

1.106. A CDR consumer who gives consent to an accredited person to collect and use their CDR data may elect that their collected data, and any data derived from it, be deleted when it becomes redundant (rule 4.11(1)(e)).

1.107. A consumer is able to make this election when giving consent, or, if they do not make the election at that point, at any other time before the expiry of their consent (rule 4.16(1)). A consumer may make the election by communicating it to the accredited person in writing, or by using the accredited person's consumer dashboard.

1.108. An accredited person does not need to provide the consumer with the ability to elect for their redundant data to be deleted during the consent process if the accredited data recipient has a general policy of deleting redundant CDR data.

1.109. A consumer's election to delete redundant CDR data will not apply to CDR data that is de-identified in accordance with the CDR data de-identification process.

Rule 4.17

Information relating to redundant data

1.110. During the consent process, the accredited person must state whether they have a general policy when collected CDR data becomes redundant data, of:

a. deleting the redundant data

b. de-identifying the redundant data

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

1.111. An accredited person that has made such a statement to a consumer must delete the consumer's redundant CDR data, even if its general policy has since been updated.

1.112. An accredited person that makes a statement of the kind referred to in (b) or (c) above, must also state:

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

    a. it would apply the CDR data de-identification process to the data; and

    b. it would be able to use or disclose (by sale or otherwise) the de-identified redundant data without seeking further consent from the consumer; and

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

c. if applicable (that is, if the accredited person retains the de-identified data for it's own use), examples of how it could use the redundant data once de-identified.

Subdivision 4.3.5 – Notification requirements

Rules 4.18 to 4.20

1.113. An accredited person must provide consumers with a notice as soon as practicable after the consumer provides consent to the accredited person collecting and using their data (CDR receipt) or withdraws their consent for an accredited person to collect and use their data. It is expected that CDR receipts would be provided in near real-time.

1.114. The CDR receipt must set out all details relevant to the consent under the rules, and any other information the accredited person provided to the consumer when obtaining the consent, including any additional terms and conditions or fees.

1.115. The notification of withdrawal of a consumer's consent for an accredited person to collect and use their data must state when the consent expired.

1.116. All consent notifications must be in writing, and in a form other than the consumer's dashboard, although, an accredited data recipient may also include a copy on the dashboard if they wish. Consent notifications do not need to be provided to consumers in a particular manner.

Example 10: Rainy Day Savings provides a CDR receipt to users of its service by email. If a consumer withdraws consent to collect and use their data, consumers receive a text that notifies them of their withdrawal notification, and states the time and date when the consent expired. Rainy Day Savings complies with the notification requirements.

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

1.118. An accredited person must notify consumers that their consents are still current in writing and through a form of communication other than the consumer's dashboard, if:

a. the consumer's consent is current; and

b. 90 days have passed since the latest of the following:

i. the consumer consented to the collection and use of the data

ii. the consumer last used their consumer dashboard

iii. the accredited person last sent the consumer a notification in accordance with rule 4.20.

Division 4.4 – Authorisations to disclose CDR data

Rules 4.21 to 4.24

1.119. A data holder must allow CDR consumers to grant their authorisation to the data holder disclosing their CDR data to an accredited person in accordance with the data standards.

1.120. A data holder's authorisation process must, having regard to consumer experience guidelines developed by the Data Standards Body, be as easy to understand as

practicable. Concise language and the use of visual aids should be used as appropriate.

1.121. During the authorisation process, a consumer must be presented with:

a. the name of the accredited person that made the request to the data holder

b. the relevant time period the request relates to

c. the types of data the data holder is seeking authorisation to disclose to the accredited person

d. whether authorisation is sought for a disclosure of data on a single occasion or multiple disclosures of data over a period of time that does not exceed 12 months

e. if authorisation is sought for multiple disclosures of data over a period of time, what that time period is

f. a statement that authorisation may be withdrawn at any time

g. instructions for how authorisation can be withdrawn.

1.122. When asking a consumer to give their authorisation, a data holder must not:

a. include any requirements beyond those specified in the data standards and the rules

b. provide or request additional information beyond that which is specified in the standards and the rules

c. offer additional or alternative services as part of this process

d. include or refer to other documents.

Withdrawal of authorisation to disclose CDR data and notification

Rule 4.25

1.123. Consumers must be able to withdraw authorisation at any time while consent is current. Consumers must be able to withdraw authorisation by communicating the withdrawal to the data holder in writing or by using the data holder's consumer dashboard.

1.124. If a consumer has communicated to the data holder in writing, the data holder must give effect to the withdrawal as soon as practical, and in any case within two business days after receiving the communication.

1.125. If an authorisation is withdrawn, whether in writing or via the dashboard, the data holder must notify the accredited person of the withdrawal in accordance with the data standards.

Duration of authorisation to disclose CDR data

Rules 4.26 to 4.27

1.126. An authorisation to disclose data to an accredited person expires at the earliest of the following:

a. if the authorisation was withdrawn in writing, the earlier of the following:

   i. when the data holder gave effect to the withdrawal

   ii. two business days after the data holder received the written communication

b. if the authorisation was withdrawn by using the dashboard, when the authorisation was withdrawn.

c. if the consumer ceases to be eligible in relation to the data holder.

d. if the data holder was notified by the accredited person of the withdrawal of a consent to collect that data, when the data holder received that notification.

e. the end of the period of 12 months after the authorisation was given.

f. if the authorisation was for disclosure of data on a single occasion, after the data has been disclosed.

g. if the authorisation was for disclosure of data over a specified period of time, at the end of that period of time.

1.127. If an accredited person's accreditation is revoked or surrendered, all authorisations for a data holder to disclose data to that accredited person expire when the data holder is notified of the revocation or surrender.

1.128. If a data holder receives from a consumer an authorisation to disclose data, or if an authorisation expires, the data holder must update the relevant consumer's dashboard as soon as practicable. This is expected to occur in as close to real time as possible.

Part 5 – Rules relating to accreditation etc

Division 5.1 – Preliminary

Rule 5.1

1.129. In order to collect data under the CDR regime, a person must be accredited. A person may apply to the Data Recipient Accreditor to become accredited. The Data Recipient Accreditor may accredit a person if satisfied that the person meets the criteria for accreditation.

Division 5.2 – Rules relating to accreditation process

Subdivision 5.2.1 – Applying to be accredited person

Rule 5.2

1.130. A person may apply to the Data Recipient Accreditor to be an accredited person. There is one level of accreditation provided for in the rules – the 'unrestricted' level. It is expected that later versions of the rules will provide for more levels of accreditation as other sectors are designated and are subject to the CDR.

1.131. The application to be an accredited person must:

a. be in the form approved by the Data Recipient Accreditor; 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 foreign entity, the applicant's local agent and the local agent's addresses for service; and

d. describe the sorts of goods or services the applicant intends to offer to consumers using data if they become accredited; and

e. if the applicant is not a person who was specified in a designation instrument, indicate whether it is or expects to be the data holder of any data that is specified in a designation instrument. This is relevant to reciprocal data holder obligations that may apply, if accreditation is granted to a person who holds data that is specified for the banking sector in the designation instrument.

1.132. There are currently no fees to apply for accreditation.

Example 11: Pennies from Heaven is a non-bank lender offering personal loans and therefore not a person specified in the designation instrument for the banking sector. In making an application to become accredited, Pennies from Heaven must indicate that it holds data of the type specified in the designation instrument because it provides lending services

Subdivision 5.2.2 – Consideration of application to be accredited person

Rules 5.3 to 5.11

1.133. The Data Recipient Accreditor may ask an applicant to provide further information to support their application. The Data Recipient Accreditor may seek this information in any way, including, but not limited to: in writing, in an interview, by phone, email, videoconferencing or any other form of electronic communication.

1.134. The Data Recipient Accreditor is not required to make an accreditation decision until the requested information has been provided. However, in the absence of the requested information the Data Recipient Accreditor may still choose to make an accreditation decision.

1.135. The Data Recipient Accreditor may also consult with other government authorities in making their decision, including, but not limited to, the Information Commissioner, Australian Securities and Investments Commission, Australian Prudential Regulation Authority, Australian Financial Complaints Authority, or similar authorities of foreign jurisdictions.

1.136. The criterion for accreditation at the unrestricted level is that the applicant would, if accredited, be able to comply with the obligations for an accredited person at an unrestricted level at rule 5.12.

1.137. The criterion for streamlined accreditation is meeting the criteria for streamlined accreditation set out in the rules for the relevant designated sector.

1.138. If it accredits an applicant, the Data Recipient Accreditor must provide the applicant with a unique number that identifies them as an accredited person. This number is referred to as an accredited person's accreditation number.

1.139. The Data Recipient Accreditor must notify an accreditation applicant, in writing, as soon as practicable after making a decision to accredit, or refuse to accredit an accreditation applicant.

1.140. If the Data Recipient Accreditor decided to accredit the applicant, the notice to them must include all of the following:

a. that the Data Recipient Accreditor has made a decision to accredit them;

b. the level of accreditation they have received;

c. any conditions that were imposed when the accreditation decision was made;

d. their accreditation number.

1.141. If the Data Recipient Accreditor decided not to accredit the applicant, the notice must include all of the following:

a. that the Data Recipient Accreditor has made a decision not to accredit them;

b. the accreditation applicant's rights to have the decision to not accredit reviewed by the Administrative Appeals Tribunal.

1.142. Accreditation takes effect when the applicant is included on the Register of Accredited Persons.

1.143. Accreditation is subject to the default conditions set out in Schedule 1, and conditions imposed or varied under rule 5.11.

1.144. The Data Recipient Accreditor may, at any time and in writing, impose any other condition on accreditation, or vary or remove a condition of accreditation imposed under rule 5.10.

1.145. Before imposing or varying a condition under rule 5.10, the Data Recipient Accreditor must inform the person of the proposed imposition or variation, and give the person a reasonable opportunity to be heard in relation to the proposed imposition or variation.

1.146. The Data Recipient Accreditor may impose or vary a condition without notice, if notice would create a real risk of:

a. harm or abuse to an individual; or

b. adversely impacting the security, integrity or stability of:

i. the Register of Accredited Persons; or

ii. information and communication technology systems that are used by CDR participants to disclose or collect data.

1.147. If the Data Recipient Accreditor has imposed or varied a condition without notice it must, as soon as practicable, give the accredited person a reasonable opportunity to be heard in relation to the imposition or variation.

1.148. A condition or a variation of a condition under rule 5.10 must include the time or date on which it takes effect.

1.149. The Data Recipient Accreditor may, but need not, give public notice of a condition or variation imposed or removed under 5.10 in any way the Data Recipient Accreditor thinks fit. This will enable issues relating to security or confidentiality to be taken into account in notifying the condition.

1.150. 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 their accreditation under rule 5.10.

1.151. If a condition is imposed or varied, the notice must include the condition or the condition as varied, and if applicable, the notice must also include the accredited person's right to have the decision reviewed by the Administrative Appeals tribunal (paragraph 5.11(2)(a)).

1.152. If a condition is removed, the notice must outline that fact.

Subdivision 5.2.3 – Obligations of accredited person

Rules 5.12 to 5.15

1.153. A person who is accredited at the unrestricted level must:

a. take the steps outlined in Schedule 2 which relate to protecting the data from:

i. misuse, interference and loss; and

ii. unauthorised access, modification or disclosure; and

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

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

d. have address for service; and

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

1.154. A person who is accredited at the unrestricted level must:

a. be, having regard to the fit and proper person criteria at rule 1.9, a fit and proper person to manage data

b. have adequate insurance, or a comparable guarantee, in light of the risk of consumers not being properly compensated for any loss that might reasonably be expected to arise from a breach of obligations under the Act, any regulation made for the purpose of the Act, or rules, to the extent that they are relevant to the management of data. Further information to assist in complying with this obligation will be available in guidelines on the ACCC's website.

1.155. An accredited person must comply with the conditions of their accreditation, including any conditions imposed or varied under rule 5.10.

1.156. Under rule 5.14, an accredited person must notify the Data Recipient Accreditor within five business days if any of the following occurs:

a. any material change in its circumstances that might affect its ability to comply with its accreditation obligations

b. any matter that could be relevant to a decision as to whether the person is, having regard to the fit and proper person criteria, a fit and proper person to manage data

c. There is a change to, or the accredited person becomes aware of an error in, any information provided to the Data Recipient Accreditor to be entered on the Register of Accredited Persons under rule 5.24.

1.157. Information must be provided to the Accreditation Registrar, by the Data Recipient Accreditor, who must:

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

i. an accreditation; or

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

iii. a surrender, suspension or an extension of a suspension; or

iv. a suspension ceasing to have effect; or

v. a revocation of an accreditation; or

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

b. include in the notice:

i. any information the Registrar is required to enter into the Register of Accreditation Persons; and

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

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

Rules 5.16 to 5.23

Transfer of accreditation

1.158. Accreditation cannot be transferred.

Surrender of accreditation

1.159. An accredited person may surrender their accreditation at any time by applying to the Data Recipient Accreditor in writing to surrender their accreditation. If the accredited person writes to the Data Recipient Accreditor to surrender their accreditation, the Data Recipient Accreditor must, in writing, accept the surrender.

Suspension and revocation of accreditation

1.160. The Data Recipient Accreditor may, in writing, suspend or revoke an accredited person's accreditation, as appropriate, if:

a. the Data Recipient Accreditor is satisfied that their accreditation was granted as the result of statements or other information that were false or misleading in a material particular. The false or misleading statements or information may be made by the accreditation applicant or by any other person.

b. subject to items 6 and 7 in subrule 5.17(1), the Data Recipient Accreditor is satisfied that the accredited person or an associated person of the accredited person has been found to have contravened a law. The contravention must be

of a law relevant to the management of CDR data as defined in rule 1.7. An associated person has the meaning given by rule 1.7.

c. the Data Recipient Accreditor reasonably believes that revocation or suspension is necessary in order to:

   i. protect consumers; or

   ii. protect the security, integrity and stability of:

      a. the Register of Accredited Persons; or

      b. information and communication technology systems that are used by CDR participants to disclose or collect CDR data.

d. the following are satisfied:

   i. the accredited person was, at the time of the accreditation, an ADI (including a restricted ADI); and

   ii. the accredited person is no longer an ADI for the reason that its authority to carry on banking business is no longer in force.

e. the accredited person has been found to have contravened:

   i. an offence provision of the Act or a civil penalty provision of the Act or these rules; or

   ii. one or more data standards

f. the Data Recipient Accreditor is no longer satisfied that the accredited person is, having regard to the fit and proper person criteria at rule 1.9, a fit and proper person to manage CDR data

g. a relevant contract between the accredited person and a consumer has been found to have a term that is unfair where 'relevant contract' means a contract that arises from a request by a consumer under subrule 4.3(1). 'Unfair' has the meaning given by section 24 of the Australian Consumer Law. 'Australian Consumer Law' has the meaning given by section 130 of the Act.

Suspension of accreditation

1.161. The Data Recipient Accreditor may, in writing, suspend an accredited person's accreditation if:

a. the Data Recipient Accreditor reasonably believes that the accredited person has or may have contravened:

   i. an offence provision of the Act or a civil penalty provision of the Act or these rules; or

   ii. one or more data standards

b. the Data Recipient Accreditor reasonably believes that a relevant contract between the accredited person and a consumer has a term that is unfair. Where 'relevant contract' means a contract that arises from a request by a consumer under subrule 4.3(1). 'Unfair' has the meaning given by section 24 of the Australian Consumer Law. 'Australian Consumer Law' has the meaning given by section 130 of the Act.

Revocation and suspension processes and durations

1.162. Before revoking an accredited person's registration under rule 5.17, the Data Recipient Accreditor must inform the accredited person of the proposed revocation and when it proposes the revocation to take effect. The Data Recipient Accreditor must also give the accredited person a reasonable opportunity to be heard in relation to the proposed revocation (subrule 5.18(1)).

1.163. The Data Recipient Accreditor must also notify the person, in writing, of a decision to revoke the person's accreditation under rule 5.17 (subrule 5.18(2)). The decision to revoke a person's accreditation can be reviewed by the Administrative Appeals Tribunal under paragraph 9.2(b).

1.164. The Data Recipient Accreditor may suspend an accreditation for a period of time that ends at a specified date, or for a period of time that ends with the occurrence of a specified event. The Data Recipient Accreditor may also, subject to the same conditions on which an accreditation was suspended, extend the suspension (subrule 5.19(1)).

1.165. The Data Recipient Accreditor may, at any time and in writing, remove a suspension (subrule 5.19(2)).

1.166. Before suspending an accreditation under rule 5.17, or extending a suspension, the Data Recipient Accreditor must inform the accredited person of the proposed suspension or extension, including the proposed duration. The Data Recipient Accreditor must also, in the case of suspension, inform the accredited person of when it is proposed the suspension will take effect. The Data Recipient Accreditor must also give the accredited person a reasonable opportunity to be heard in relation to the proposed suspension or extension (rule 5.20).

1.167. If the Data Recipient Accreditor makes a decision to suspend an accredited person's accreditation under rule 5.17, the Data Recipient Accreditor must notify the person, in writing, of the suspension and the period of suspension (subrule 5.20(3)). The decision to suspend an accredited person's accreditation can be reviewed by the Administrative Appeals Tribunal.

1.168. If the Data Recipient Accreditor makes a decision to extend a suspension, the Data Recipient Accreditor must notify the person, in writing, of the extension and the period of the suspension as extended (subrule 5.20(4)). The decision to extend a suspension can be reviewed by the Administrative Appeals Tribunal.

1.169. The Data Recipient Accreditor may suspend the accreditation or extend the suspension of a person without first complying with rule 5.20 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 5.20 prior to the suspension or extension.

1.170. However, if the Data Recipient Accreditor suspends the accreditation or extends the suspension without complying with rule 5.20, the Data Recipient Accreditor must, as soon as practicable, inform the accredited person of the suspension or extension and give the accredited person a reasonable opportunity to be heard in relation to whether the suspension should be removed (subrule 5.21(3)).

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

Consequences of surrender, suspension or revocation or accreditation

1.172. If a person's accreditation has been surrendered or revoked, the person must comply with the following provisions as if the person still were an accredited data recipient:

a. Privacy Safeguard 6; and

b. Privacy Safeguard 7; and

c. Privacy safeguard 12.

1.173. In addition, if an accreditation is revoked or surrendered, any consents to collect and use data expire, as well as any authorisations to disclose data.

1.174. If a person's accreditation is suspended, the person remains an accredited person, and must continue to meet the same obligations as an accredited person whose accreditation has not been suspended. In addition, if an accreditation is suspended, the accredited person is prohibited from seeking to collect data while the suspension is in effect.

1.175. A person who has surrendered their accreditation, or has had their accreditation revoked, or has a current suspension, must:

a. not seek to collect any, or collect any further, data under these rules; and

b. if the person has collected data under these rules, notify each person who has consented to the accredited person collecting data:

i. that their accreditation has been surrendered, suspended or revoked, as the case may be; and

ii. in the case of a suspension:

a. that any consents to collect and to use data may be withdrawn at any time; and

b. the effect of such withdrawal.

1.176. Under subrule 5.23(4), a person must delete or de-identify collected data by taking the steps specified in rule 7.12 as appropriate, if:

a. the person's accreditation has been surrendered, or revoked; and

b. the person has collected data under these rules; and

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

d. the data does not relate to any current or anticipated:

i. legal proceedings; or

ii. dispute resolution proceedings;

to which the person is a party.

Division 5.3 – Rules relating to the Register of Accredited Persons

Rules 5.24 to 5.32

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

a. the following details about the accredited person:

i. their name; and

ii. their accreditation number; and

iii. their addresses for service; and

iv. if they are a foreign entity, the name and addresses for service of the accredited person's local agent; and

b. the level of the person's accreditation;

c. either any conditions on the accreditation, or if the Data Recipient Accreditor so directs, a description of the effect of any such conditions;

d. if the accreditation has been revoked, that fact and the date of the revocation;

e. if the accreditation has been suspended, that fact and the period of the suspension;

f. if a decision to suspend and accreditation has been revoked, or the suspension otherwise is no longer in effect, that fact and the date from which the accreditation is once more in effect;

g. if the accreditation is suspended, that fact and the date of the surrender;

h. each brand name under which the accredited person provides goods or services where, in order to provide the good or service, the accredited person needs to access a consumer's data;

i. a hyperlink to each of the following:

i. the relevant website address of the accredited person;

ii. the accredited person's CDR policy;

iii. if the accredited person has a CDR policy for a brand name under which the accredited person provides goods or services where, in order to provide the good or service, the accredited person needs to access a consumer's data – that policy.

1.178. Along with the Register of Accredited Persons, the Accreditation Registrar must create and maintain a database that includes:

a. a list of data holders; and

b. for each data holder:

i. every brand name under which the data holder offers products for which data requests may be made under these rules; and

ii. a hyperlink to:

A. the relevant website address of the data holder; and

B. the data holder's CDR policy; and

C. if the data holder has a CDR policy for a brand name under which the data holder offers products for which data requests may be made under these rules – that policy; and

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

c. such other information relating to each data holder and each accredited person as the Accreditation Registrar considers is required in order for requests under these rules to be processed in accordance with these rules and the data standards. This is expected to include technical information (metadata) about accredited person request services of data holders and the individual CDR apps or services of accredited persons so that CDR participants can verify the identity of other CDR participants to send requests and notifications in accordance with the data standards (for example, notification of withdrawal of authorisation).

Updating the Register

1.179. The Accreditation Registrar may request a data holder or accredited person to provide the information referred to in subrule 5.25(1), or any updates to that information, and may specify the form in which the information or updates are to be provided. A data holder or accredited person much comply with such a request.

1.180. The data holder or accredited person, as appropriate, must inform the Accreditation Registrar of the amendment that should be made to the database, in the form approved by the Registrar, if:

a. it has provided information to the Accreditation Registrar in accordance with rule 5.25; and

b. it becomes aware that the information is out of date or needs to be amended in order for product data requests and consumer data requests made under these rules to be processed in accordance with the rules or data standards.

1.181. The Accreditation Registrar must, as soon as practicable after receiving information from the Data Recipient Accreditor that must be entered on the Register, enter that information on the Register.

1.182. The Accreditation Registrar must also, as soon as practicable after receiving information from the Data Recipient Accreditor that requires the Accreditation Registrar to update information on the Register, update the Register.

1.183. The Accreditation Registrar may, to the extent the Accreditation Registrar considers necessary, amend the database referred to in subrule 5.25(1) to reflect any amendment the Accreditation Registrar has been informed of in accordance with subrule 5.25(4).

1.184. The Accreditation Registrar may also may make clerical amendments to entries in the Register or database as appropriate to ensure the accuracy of the Register or database.

1.185. The Accreditation Registrar must, in the manner the Accreditation Registrar thinks fit, make publically available:

a. the information referred to in rule 5.24 regarding the maintenance of the Register of Accredited Persons; and

b. the information referred to in paragraphs 5.25(1)(a) and (b) regarding other information to be kept in association with the Register of Accredited Persons.

1.186. On request, the Accreditation Registrar must make available to the Commission, the Information Commissioner and the Data Recipient Accreditor (rule 5.28):

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

b. specified information in the Register or the associated database; or

c. any information held by the Accreditation Registrar or the associated database; or

d. any information held by the Accreditation Registrar in relation to the Register or the associated database.

1.187. The Commission may publish information made available to it by the Accreditation Registrar relating to the performance and availability of systems to respond to requests under these rules (rule 5.29).

Accreditation Registrar's other functions

1.188. The Accreditation Registrar also has other functions (rule 5.30), including the following:

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

b. maintaining the security, integrity and stability of the Register and associated database, including undertaking or facilitating any testing, including making requests to participate in testing, for that purpose

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

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

1.189. The Accreditation Registrar has the power to do all things necessary or convenient to be done for or in connection with the performance of its functions.

1.190. A data holder and accredited person must comply with any request from the Accreditation Registrar to do a specific thing in order to ensure the security, integrity and stability of the Register of Accredited Persons or associated database (rule 5.31). A request of this kind may be made where the accreditation status of an accredited person has changed and the Register has been updated.

1.191. The Accreditation Registrar may automate any processes, including decision-making.

Part 6 – Rules relating to dispute resolution

Rules 6.1 and 6.2

1.192. A data holder for a particular sector must have internal dispute resolution (**IDR**) processes that meet the IDR requirements in relation to that sector. For the banking sector, these requirements are set out in Schedule 3 (see from paragraph 1.266 below).

1.193. Accredited persons are also required, as a result of their ongoing obligations of accreditation, to have IDR processes that meet the IDR requirements in relation to one or more sectors.

1.194. Data holders are required to be a member of a recognised external dispute resolution scheme in relation to CDR consumer complaints. Accredited data recipients are also required to be a member of the scheme under the accreditation rules. For the banking sector, the ACCC intends to recognise AFCA.

Part 7 – Rules relating to the privacy safeguards

Division 7.1 – Preliminary

Rule 7.1

1.195. The Privacy Safeguards, contained in Part IVD of the Act, provide additional protection to CDR data. They apply only to CDR data for which there are one or more CDR consumers and do not apply to CDR data for which there are no CDR consumers (such as required product data and voluntary product data).

Division 7.2 – Rules relating to privacy safeguards

Subdivision 7.2.1 – Rules relating to consideration of CDR data privacy

Privacy Safeguard 1 – open and transparent management of CDR data

Rule 7.2

1.196. Data holders and accredited data recipients are required to have a policy about the management of CDR data that they make readily available online (***CDR policy***). Section 56ED of the Act sets out the matters that the policy must contain and the rules set out additional information that the policy must contain and how it should be made available to consumers.

1.197. A CDR policy is taken to be in the approved form if it follows the approach to content and structure set out in OAIC Guidelines, or any other guidance on Privacy Safeguard 1 referred to in those Guidelines. A CDR policy must be a separate document to the entity's general privacy or other policies. Where a person is both an accredited data recipient and a data holder they may have two or a single CDR policy, provided the information required to be contained in the policy is captured for the person acting in both capacities.

1.198. The CDR policy must indicate whether a data holder accepts requests for voluntary product or consumer data and, if so, whether it charges a fee for the disclosure of such data and if it does, how information about those fees can be obtained. This is to help facilitate accredited data recipients knowing whether they can request consent for the disclosure of such data for particular CDR consumers.

1.199. The CDR policy must also inform consumers of what the consequences will be, if any, if they withdraw their consent during the consent period. This could include information about any early cancellation fees.

1.200. The policy must provide a list of outsourced service providers used by the accredited data recipient, the nature of the services they provide and the types of data that may be disclosed to those outsourced service providers. If any of the outsourced service providers are based overseas and are not accredited themselves, the accredited data recipient must include the countries in which those outsourced service providers are based. If an accredited data recipient proposes to disclose CDR data overseas, its CDR policy must specify in which countries it proposes to disclose CDR data.

1.201. The policy is also intended, in addition to the consent process, to give consumers transparency around the de-identification and destruction of CDR data processes.

1.202. For de-identification that occurs as a use of CDR data that is consented to in order to disclose (by sale or otherwise) de-identified CDR data, accredited data recipients must including information about:

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

b. the information specified in paragraph 1.162 below

1.203. For the treatment of redundant data, the policy must include information on:

a. the following information about deletion of redundant data:

    a. when the accredited data recipient deletes redundant data

    b. how a CDR consumer may elect for this to happen

    c. how the redundant data is deleted; and

b. if applicable – the following information about de-identification of redundant CDR data:

    a. if the de-identified is used by the accredited data recipient, examples of how the accredited data recipient ordinarily uses de-identified data, and

    b. the information specified in paragraph 1.162 below.

1.204. The policy must also include information about the CDR consumer's election to delete, being:

a. information about how the election operates and its effect

b. information about how CDR consumers can exercise the election.

1.205. The further information about de-identification is:

a. How the accredited person de-identifies CDR data, including a description of the techniques it uses; and

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

    a. that fact

b. to what classes of persons it ordinarily discloses such data

c. why it so discloses such data.

1.206. The CDR policy also requires both accredited data recipients and data holders to include information about their IDR processes including how a complaint can be made and the participant's process for handling CDR consumer complaints.

1.207. If an accredited person proposed to store CDR data other than in Australia or an external territory, its CDR policy must specify any country in which it proposes to store CDR data.

Privacy Safeguard 2 – anonymity and pseudonymity

Rule 7.3

1.208. Privacy Safeguard 2 in section 56EE of the Act provides that accredited data recipients must give consumers the option of using a pseudonym, or not identifying themselves, when dealing with the accredited data recipient. Exceptions to this are set out in the rules and are as follows:

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.

Example 12: A bank may be required to deal with an identifiable CDR consumer in order to meet its responsible lending obligations.

Subdivision 7.2.2 – Rules relating to collecting CDR data

Privacy Safeguard 5 – notifying of the collection of CDR data

Rule 7.4

1.209. Section 56EH of the Act provides that an accredited data recipient must take the step in the rules to notify consumers of the collection of data. The rules provide that a consumer will have a consumer dashboard for each accredited data recipient to which they have given consent to collect their data. The accredited data recipient's consumer dashboard will contain a record of each time the data recipient has collected CDR data from a data holder in response to a request to collect by the consumer. This record will show what data was collected, when it was collected, and from which data holder.

1.210. The dashboard must be updated by the accredited data recipient as soon as practicable each time data is collected. This is expected to occur in as close to real time as possible.

Subdivision 7.2.3 – Rules relating to dealing with CDR data

Privacy Safeguard 6 – use or disclosure of CDR data by accredited data recipients

Rules 7.5 to 7.9

1.211. Paragraph 56EI(1)(b) of the Act provides that an accredited data recipient of CDR data must not use or disclose CDR data unless the use or disclosure is otherwise required, or authorised, under the consumer data rules. For paragraph 56EI(1)(b) of the Act, the use or disclosure of CDR data for which there is a CDR consumer by an accredited data recipient of the CDR data is authorised under these rules if it is a permitted use or disclosure. A permitted use or disclosure is defined in rule 7.5.

Privacy Safeguard 7 – use or disclosure of CDR data for direct marketing

1.212. Subclause 56EJ(1)(b) of the Act provides that an accredited data recipient of CDR data must not use or disclose it for direct marketing unless the consumer consents and such use or disclosure is required or authorised under the consumer data rules. Rule 7.8 provides a limited authorisation for that purpose.

1.213. Under the authorisation, an accredited data recipient can provide information about products or services direct to the CDR consumer in limited circumstances.

1.214. The authorisation only applies if the consumer has given express consent to direct marketing that the accredited person intends to undertake (subrule 4.11(1)(iii)). Such consent must be current.

1.215. The scope of the authorisation, which is a permitted use or disclosure under rule 7.5, is limited to those situations where an accredited data recipient uses the CDR data to:

a. send the CDR consumer information about upgraded or alternative goods or services to the existing goods or services being used by the CDR consumer;

b. send the CDR consumer:

(i) an offer to renew the goods or services the accredited data recipient is providing to the CDR consumer when it expires; or

(ii) information about the benefits of the existing goods or services.

Example 13: Kelly uses Metal Bank's free service, Bronze Medallion. In providing consent for Metal Bank to collect and use Kelly's CDR data, Kelly consented to Metal Bank using her CDR data to direct market. Metal Bank analyses Kelly's data and discovers Kelly would benefit from upgrading to its premium version, Silver Service. Metal Bank asks Kelly if she would like to upgrade to Silver Service. Metal Bank's actions are in accordance with the authorisation.

1.216. Where marketing forms part of the service requested by the CDR consumer, such as where a comparator site provides tailored quotes to the CDR consumer, the provision of such information is authorised under rule 7.5(1)(a). It is in compliance with the data minimisation principle and in accordance with a current consent from the CDR consumer. When providing such a service, an accredited data recipient does not need to rely on the direct marketing authorisation under rule 7.8.

Privacy Safeguard 10 – notifying of the disclosure of CDR data

Rule 7.9

1.217. Section 56EM of the Act provides that a data holder must take the step in the rules to notify consumers of the disclosure of data. The rules provide that data holders are required to create a dashboard for each consumer that has granted authorisation to the data holder to disclose their CDR data to an accredited person under the regime. The rules for Privacy Safeguard 10 require that data holders must update the dashboard with information about each authorisation, including what data they disclosed, when, and to which accredited data recipient.

1.218. The dashboard must be updated by the data holder as soon as practicable each time data is disclosed. This is expected to occur in as close to real time as possible.

1.219. In the case of joint accounts, all account holders are required to receive notification on their dashboard of a disclosure, unless the conditions in rule 4.6 of Schedule 3 are satisfied, that is, a data holder considers not updating the dashboard of the other joint account holder necessary in order to prevent physical or financial harm or abuse (see paragraph 1.265).

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

Privacy Safeguard 11 – quality of CDR data

Rule 7.10

1.220. Privacy Safeguard 11, in section 56EN of the Act, requires a data holder to, in accordance with the rules, notify the consumer where the data holder becomes aware that some or all of the CDR data disclosed to an accredited data recipient was incorrect.

1.221. The rule relating to Privacy Safeguard 11 requires the data holder to notify consumers of this fact in writing, including identifying the accredited persons to whom the incorrect data was disclosed and the date on which it was disclosed. The notice must identify the CDR data that was incorrect and give the CDR consumer the opportunity to request the data holder disclose the corrected data to the earlier accredited person recipient/s.

1.222. The rules for Privacy Safeguard 11 currently apply to disclosures made by data holders to accredited persons. In a later version of the rules, these rules will also apply to disclosures made by data holders to CDR consumers directly (as of July 2020) and any disclosures that are authorised to be made by accredited data recipients.

Privacy Safeguard 12 – security of CDR data, and destruction or de-identification of redundant CDR data

1.223. There are two components to Privacy Safeguard 12 (section 56EO of the Act):

a. the security of CDR data

b. the treatment of redundant CDR data by destruction or de-identification. For the purposes of the rules, the terms destruction and deletion are synonymous.

The security of CDR data

Rule 7.11

1.224. Accredited data recipients must take the steps specified in the rules to protect CDR data from:

a. misuse, interference and loss

b. unauthorised access, modification or disclosure.

1.225. The steps to be taken by accredited data recipients are set out at Schedule 2 to the rules. Broadly speaking, the steps require accredited data recipient to:

a. define and implement security governance in relation to CDR data

b. define the boundaries of the CDR data environment

c. have and maintain an information security capability

d. implement a formal controls assessment program

e. manage and report security incidents.

1.226. The steps are also accompanied by a series of information security controls listed at Part 2 of Schedule 2. Additional guidance on the security steps and controls will be available in the Accreditation Guidelines on the ACCC's website. The OAIC's Privacy Safeguard 12 guidelines also provide guidance on the security steps in the context of Privacy Safeguard 12 compliance.

The treatment of redundant data

Rules 7.12 and 7.13

1.227. Under section 56EO of the Act, CDR data will become 'redundant' when an accredited data recipient no longer needs any of the data for either:

a. a purpose permitted under the rules; or

b. a purpose for which the accredited data recipient can use or disclose the data under Division 5 of Part IVD of the Act;

and:

c. the data is not otherwise required to be retained by or under an Australian law or court/tribunal order;

d. the data does not relate to current or anticipated legal or dispute resolution proceedings to which the accredited data recipient is a party.

1.228. Under Privacy Safeguard 12, when data has become redundant, accredited data recipients must take the steps set out in the rules to destroy or de-identify it.

De-identification of redundant data

1.229. The rules for the de-identification of redundant data only apply if:

a. the accredited person, when it asked for consent to collect and use the CDR data, gave the consumer the statement referred to in rule 4.17(1)(b) or (c) that the accredited person has a general policy of either:

i. de-identifying redundant data; or

ii. deciding, when CDR data becomes redundant, whether to delete or de-identify it; and

b. the consumer did not elect, in accordance with rule 4.16, that their redundant data should be deleted; and

c. it is possibly to de-identify the CDR data in accordance with the CDR data de-identification process; and

d. in the case of a statement of the kind described above, the accredited person thinks it appropriate in the circumstances to de-identify rather than delete the redundant data.

1.230. If the de-identification of redundant data rule applies, the accredited data recipient must apply the CDR data de-identification process outlined in rule 1.17 to the data.

Deletion of redundant data

1.231. The rule for the deletion of redundant data, rule 7.13, applies if rule 7.12 (the de-identification of redundant data) does not apply.

1.232. If rule 7.12 applies, the accredited data recipient must apply the CDR data deletion process to the data (rule 1.18).

Subdivision 7.2.5 – rules relating to correction of CDR data

Privacy Safeguard 13 – steps to be taken when responding to a correction request

Rules 7.14 and 7.15

1.233. The ability for a consumer to request the correction of their CDR data is important to ensure the integrity and quality of data within the CDR ecosystem. Under Privacy Safeguard 13, in section 56EP of the Act, consumers can make requests to both data holders and accredited data recipients seeking the correction of their data. In response to such a request, a data holder or accredited data recipient must either correct the data or, if the data holder or accredited data recipient considers that the data is correct for the purposes for which it is held, it must include a statement with the data to this effect. This statement must be attached to the data in such a way that it will be apparent to any subsequent users of the data. Data holders and accredited data recipients cannot charge a fee for responding to or actioning such requests.

1.234. In some circumstances, a data holder or accredited data recipient may consider that a correction or statement is inappropriate or unnecessary, and a consumer must be so advised. The notice advising the consumer of the outcome of their correction request must set out the complaint mechanisms available to the consumer for instances where they are not satisfied with the action taken (or not taken) in response to their request.

1.235. If a data holder has made a correction to CDR data in response to a consumer's request and the corrected CDR data was earlier disclosed to an accredited data recipient or recipients, the data holder has therefore become aware that data it earlier disclosed was incorrect at the time of disclosure for the purpose of Privacy Safeguard 11. Accordingly, the data holder must also take the steps required under that safeguard, including to give notice to the consumer that the consumer can request the re-disclosure of their corrected data to the earlier recipients.

Part 8 – Rules relating to data standards

Division 8.1 – Simplified outline

Rule 8.1

1.236. Product data requests and consumer data requests under these rules are made in accordance with data standards. Part 8 sets out the rules relating to data standards, including the role of the Data Standards Chair, the Data Standards Advisory Committee and the process for making, amending and reviewing data standards.

Division 8.2 – Data Standards Advisory Committee

Rules 8.2 to 8.7

1.237. The Data Standards Chair must establish and maintain a committee to advise the Chair about data standards (the **Data Standards Advisory Committee**). The instrument establishing the Data Standards Advisory Committee may set out matters for which the Data Standards Advisory Committee is to advise the Chair. In addition, the Chair can refer any matter to the Committee for consideration. For example, the Chair may ask the Committee to provide technical advice on the operation of a standard.

1.238. The Chair must appoint, in writing, at least one privacy representative and at least one consumer representative to the Data Standards Advisory Committee. Membership of the Committee is not limited to any number of persons.

1.239. The Committee may have observers including the ACCC, OAIC, Department of the Treasury and any other person invited by the Chair to be an observer.

Division 8.3 – Reviewing, developing and amending data standards

Rules 8.8 to 8.10

1.240. The Chair must notify the ACCC and the Information Commissioner, in writing, of a proposal to make or amend a standard. However, the Chair may notify the ACCC and the Information Commissioner after the fact if the making or amendment of a standard is urgent or minor.

1.241. The Chair will consult on a standard before it is made. This will involve consultation with key stakeholders and a public consultation period, where submissions may be made. The failure to consult on a standard will not affect its validity.

1.242. Where an amendment to a standard is urgent or minor, the Chair is not required to consult on the amendment before making it. An urgent amendment could include a change necessary to protect the security, integrity or stability of the CDR ecosystem. A minor change may include fixing a typographical error in the standard or other low order issues. The rules also provide a transitional provision for the making of data standards until 1 August 2020, such that the Chair need not consult for versions of the standards made prior to that date. This is consistent with the transitional provision that applies to the CDR rules to be made for the banking sector prior to July 2020 and allows an additional month to accommodate making of or amendments to the standards.

Division 8.4 – Data standards that must be made

Rule 8.11

1.243. The Data Standards Chair is required to make standards on certain matters.

1.244. At a minimum, the Data Standards Chair must make standards for:

a. the process for making and responding to product data requests and consumer data requests

a. the process for obtaining authorisations and consents and withdrawals of authorisations and consents

b. the collection and use of data, including requirements such as accessibility, to be met by CDR participants in relation to seeking consent from consumers

c. the disclosure and security of data, including authentication of consumers to a standard that meets, in the opinion of the Chair, best practice security requirements

d. the disclosure and security of data, seeking authorisations to disclose data in response to data requests

e. the types of data to be used by participants in making and responding to requests

f. the formats in which data is to be provided in response to requests

g. requirements to be met by CDR participants in relation to performance and availability of systems to respond to requests

h. requirements to be met by CDR participants in relation to compliance with those requirements

i. the processes for CDR participants to notify other CDR participants of withdrawal of consent or authorisations by consumers

j. the provision of administrative or ancillary services by CDR participants to facilitate the management and receipt of communications between CDR participants.

1.245. Every standard required to be made by the rules must indicate that it is binding and must specify the date on which it commences and the date by which it must be fully complied with.

1.246. The data standards must be subject to such consumer testing, if any, as considered appropriate by the Data Standards Chair.

Part 9 – Other matters

Division 9.1 – Preliminary

Rule 9.1

1.247. This part deals with a range of miscellaneous matters including review of decisions, reporting, record keeping and audit rules, and civil penalty provisions.

Division 9.2 – Review of decisions

Rule 9.2

1.248. An accredited person may make an application to the Administrative Appeals Tribunal to review the Data Recipient Accreditor's decision to:

a. impose a condition on accreditation

b. vary a condition that has been imposed

c. suspend an accreditation

d. extend a suspension

e. revoke an accreditation.

1.249. All decisions of the Data Recipient Accreditor that are reviewable will continue to operate unless the Administrative Appeals Tribunal has ordered the decision be suspended while the review takes place.

Division 9.3 – Reporting, recording keeping and audit

Subdivision 9.3.1 – Reporting and record keeping

Records to be kept and maintained

Rule 9.3

1.250. Records made under the CDR regime are subject to responsibilities under the *Privacy Act 1988* to the extent they contain personal information, except where the records are made by an entity not subject to the *Privacy Act 1988*. Accredited entities and most data holders are subject to the *Privacy Act 1988*.

1.251. A data holder must keep and maintain records that record and explain:

a. authorisations given by consumers to disclose data;

b. withdrawals of authorisations to disclose data;

c. notifications of withdrawals of consents to collect data;

d. disclosures of data made in response to consumer data requests;

e. instances where data has not been disclosed in reliance on an exemption from the obligation to disclose;

f. CDR complaint data, as defined in rule 1.7.

1.252. An accredited data recipient must keep and maintain records that record and explain the following:

a. consents to collect and use data provided by consumers, including, if applicable, the uses of the data the consumer has consented to;

b. withdrawals of consents by consumers

c. notifications of withdrawals of authorisations received from data holders

d. CDR complaint data, as defined in rule 1.7

e. the types of data collected under these rules

f. elections to delete and withdrawals of those elections

g. the use of data by the accredited data recipient

h. the processes by which the accredited data recipient asks consumers for their consent, including a video of that process

i. if applicable, arrangements that may result in sharing data with outsourced service providers, including copies of agreements with outsourced service providers and the use and management of data by those providers.

j. if data was de-identified in accordance with a consent referred to in paragraph 4.12(3)(e):

i. how the data was de-identified; and

ii. how the accredited data recipient used the de-identified data; and

iii. it the accredited data recipient disclosed (by sale or otherwise) the de-identified data to another person as referred to in paragraph 4.17(b):

I. to whom the data was so disclosed; and

II. why the data was so disclosed;

k. records that are required to be made for the purposes of the CDR data de-identification process when applied as part of privacy safeguard 12;

l. records of any matters that are required to be retained under Schedule 2 to these rules;

m. any terms and conditions on which the accredited data recipient offers goods or services where the accredited data recipient collects or uses data in order to provide the good or service.

Example 14: FastSaver records its consent flows in a video format, showing step-by-step what a consumer may consent to while using its app, as well as the format this information is presented to consumers. When FastSaver makes updates to its consent flows, it creates new records of all possible consent decisions and retains its previous consent flows for 6 years dating from the last time a consumer was able to consent using the previous consent flow. FastSaver is complying with paragraph 9.3(2)(g) of the rules.

1.253. The record keeping requirements in the rules do not include a requirement to keep a copy or copies of collected CDR data itself. Records should only contain personal information where it is necessary to comply with these rules.

1.254. Records should be kept securely and access should be restricted as appropriate. This includes providing for extra protections where records include personal or sensitive information, in accordance with obligations under the *Privacy Act 1988*.

1.255. All records required to be kept must include the date and time when the record was made and, if applicable, the date and time when the event described by the record occurred.

1.256. Where a record referred to in this rule is kept in a language other than English, an English translation of the record must be made available within a reasonable time to a person who is entitled to inspect the records and asks for the English translation.

1.257. All records required to be kept must be kept for a period of six years beginning on the day the record was created.

Reporting requirements

Rule 9.4

1.258. A data holder must prepare a report for each period that is in the form approved by the Commission and summarises the CDR complaint data that relates to that reporting period. The report must also set out the number (if any) of product data requests, consumer data requests made by eligible consumers, and consumer data requests made by accredited persons on behalf of eligible consumers. The report must also set out the number of times the data holder has refused to disclose data and the rule or data standard relied upon to refuse to disclose that data, and the proportion of CDR consumers who had exercised the right to delete.

1.259. An accredited data recipient must prepare a report for each reporting period that is in the form approved by the Commission and summarises the CDR complaint data that relates to that reporting period.

1.260. The report must also describe any goods or services that the accredited data recipient offers to consumers using data that that were not described in the relevant application to be an accredited person, or previously included in a report prepared under this rule. The report must also describe the types of data that are required in order to offer its goods or services, and explain why that data is required in order to offer goods or services to consumers. The report must describe any material changes that have been made to any good or service offered by the accredited data recipient since the previous reporting period, including any changes to the goods or services that they offer to consumers using data that is not subject to one of the exceptions in paragraph (c). The report must also set out the number of consumer data requests made by the accredited data recipient during the reporting period.

1.261. All reports must be submitted to the Commission and the Information Commissioner within 30 days after the end of the reporting period. Both the Commission and the Information Commissioner may publish any report received under this rule, or require an accredited data recipient to publish, on its website, a report that it has prepared for subrule 9.4(2).

1.262. The reporting periods are 1 January to 30 June of each year, and 1 July to 31 December of each year.

Requests from CDR consumers for copies of records

Rule 9.5

1.263. A consumer may request a data holder provide copies of records that relate to them and relate to their authorisation to disclose data, the data disclosed in response to a request and CDR complaint data.

1.264. A consumer may request an accredited data recipient provide copies of records that relate to them and relate to their consent to collect and use data, and any notification of withdrawals of authorisations received from data holders.

1.265. A request under rule 9.5 must be in the form, if any, approved by the Commission.

1.266. A person who receives a request under this rule must provide the requested copies in the form, if any, approved by the Commission. A person must provide the copies as soon as practicable, but no later than ten business days after receiving the request.

1.267. A data holder and accredited data recipient must not charge a fee for making or responding to a consumer's request for copies of records.

Subdivision 9.3.2 – Audits

Rules 9.6 and 9.7

1.268. The Commission may, at any time, audit any data holder or accredited data recipient to consider their compliance of 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.

1.269. The Information Commissioner may, at any time, audit any data holder or accredited data recipient to consider their compliance 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 the privacy safeguards or the privacy and confidentiality of data.

1.270. The Commission and the Information Commissioner may give a data holder or an accredited data recipient a written notice that requests they produce copies, within the time specified, of records that are required by these rules to be kept, or information from such records, as limited by subrule 9.6(1) and (2).

1.271. The data holder or accredited data recipient must comply with any request provided by the Commission or the Information Commissioner to produce copies of records that are required to be kept by these rules, or information from such records.

Example 15: The Commission is concerned about Fund X's compliance with the data minimisation principle in relation to its premium service, Budget X. It requests, in writing, Fund X provides it with its records relating to paragraphs 9.32(2)(e) and (f) for its Budget X service. Fund X must comply with the Commission's request.

1.272. The Data Recipient Accreditor may, at any time, audit any accredited data recipient to consider their compliance with the obligations under rule 5.12 or any conditions imposed on their accreditation.

1.273. The Data Recipient Accreditor may give an accredited data recipient a written notice that requests they produce copies of records that they are required by these rules to keep, or information from such records, as limited by subrule 9.7(1).

1.274. An accredited data recipient must comply with a request by the Data Recipient Accreditor to produce copies of records that are required to be kept by these rules, or information from such records.

1.275. 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

Rule 9.8

1.276. Rule 9.8 outlines the rules that are civil penalty provisions for s 56BL of the Act, within the meaning of *Regulatory Powers (Standard Provisions) Act 2014*.

1.277. Those obligations that are fundamental, such as obligations relating to seeking consent, disclosing data and complying with the data standards, are subject to the maximum penalty, with the intention that the ACCC seek appropriate levels of penalty for contraventions of different degrees of seriousness. A lower maximum penalty level has been adopted for some provisions relating to recordkeeping and notifications.

Schedule 1 – Default conditions on accreditations

Part 1 – Preliminary

Clause 1.1

1.278. Part 2 of Schedule 1 sets out the default conditions that apply to accreditation for the purposes of rule 5.9.

Part 2 – Default conditions on accreditations

Clause 2.1

Ongoing reporting obligation on accredited persons

1.279. An accredited person has ongoing reporting obligations with respect to attestation statements and assurance reports for each reporting period.

1.280. An attestation statement must be provided to the Data Recipient Accreditor for each reporting period within three months after the end of that reporting period. Similarly an assurance report must be provided to the Data Recipient Accreditor for each reporting period within three months after the end of that reporting period.

Schedule 2 – Steps for privacy safeguard 12–security of CDR data held by accredited data recipients

Part 1 – Steps for privacy safeguard 12

Clauses 1.1 to 1.7

1.281. The steps that an accredited data recipient must take under Privacy Safeguard 12 for the security of CDR data are set out in Schedule 2 to the rules.

1.282. The information security requirements must be met by all persons accredited at the unrestricted level, both at the point of accreditation and on an ongoing basis once accredited. Accredited data recipients may choose to put in place protection that exceeds these minimum requirements.

1.283. Additional guidance on how an applicant for accreditation can demonstrate to the Data Recipient Accreditor that it satisfies these requirements will be available in the Accreditation Guidelines on the ACCC's website and the OAIC's guidelines on Privacy Safeguard 12.

1.284. Part 1 sets out the steps an accredited data recipient must take to secure CDR data which encompass:

a. defining and implementing an overarching information security governance framework

b. defining the boundaries of the accredited data recipient's CDR data environment

c. implementing and maintaining an information security capability which applies the controls set out in Part 2

d. implementing a formal controls assessment program

e. managing and reporting security incidents. Accredited data recipients are expected to report security incidents to the Australian Cyber Security Centre.

Part 2 – Minimum information security controls

Clauses 2.1 and 2.2

1.285. An accredited data recipient must have and maintain the mandatory controls set out in Part 2 of Schedule 2. These controls include steps to limit the risk of inappropriate or unauthorised access to CDR data, steps to secure access to networks and systems, steps to secure management of information assets, processes to identify, track and remediate vulnerabilities, steps to prevent, detect and remove malware and steps to implement a formal training and awareness program.

Schedule 3 – Provisions relevant to the banking sector

Part 1 – Preliminary

Clauses 1.1 to 1.3

1.286. Schedule 3 deals with how these rules apply in relation to the banking sector. Part 1 of this Schedule includes a number of definitions that apply only in relation to the banking sector.

1.287. Part 1 specifies certain information as meaning 'customer data', 'account data', transaction data' and 'product specific data' for the purposes of this Schedule.

1.288. The first type of information is 'customer data' in relation to a particular person. This includes their name, contact details, information provided at the time of acquiring the product or relating to their eligibility to acquire that product (although not extending to information relating to the actual decision on eligibility, such as a credit decision), and certain information if the person operates a business (such as their ABN, and type of business). Customer data does not include the person's date of birth.

1.289. The second type of information is 'account data' in relation to a particular account. This includes the type of information that a customer would commonly see about their account, including the account number and name, opening and closing balances and authorisations on the account.

1.290. The third type of information is 'transaction data' in relation to a particular transaction. This includes information about the date on which the transaction occurred, a description of the transaction, and the amount debited or credited.

1.291. The fourth type of information is 'product specific data'. This includes information that identifies or describes the characteristics of the product, including its type, its price (including fees, charges and interest rates however these are described), terms and conditions and eligibility criteria that a customer needs to meet. This also includes information about associated features and benefits, such as a credit card's loyalty scheme (but not the points accrued on such a scheme).

Part 2 – Eligible CDR consumers – banking sector

Clause 2.1

1.292. An 'eligible' consumer, for the purposes of the banking sector, means a consumer that is 18 years of age or older and has an account with the data holder that is open and can be accessed online (for example, by using an internet browser or an application accessed on a mobile phone).

Part 3 – CDR data that may be accessed under these rules – banking sector

Clauses 3.1 and 3.2

1.293. This part sets out the meaning of certain terms such as 'required product data' and 'voluntary product data', and 'required consumer data' and 'voluntary consumer data' in relation to the banking sector.

1.294. 'Required product data' means CDR data that does not relate to any particular identifiable consumer. 'Required product data' must fall within a class of information specified in the designation instrument, is about certain characteristics of the product

(such as the product's eligibility criteria, price, terms and conditions, availability or performance) and is held in a digital form. Information about the availability or performance of the product should be publicly available.

1.295. 'Voluntary product data' means CDR data that is not 'required product data'. 'Voluntary product data' must fall within a class of information specified in the designation instrument and is product specific data about a product.

1.296. CDR data is 'required consumer data' where it relates to a particular consumer. For CDR data to be required customer data, it must fall within the meaning of CDR data contained in s 56AI(1)(a) of the Act, or a 56AI(1)(b) of the Act but is not materially enhanced information. 'Required consumer data' can include customer data in relation to that consumer, their account or transaction data, or product specific data in relation to a product that the consumer uses. This data must be held in a digital form by the data holder.

1.297. 'Voluntary consumer data' is any data that relates to a particular consumer and is not 'required product data'.

1.298. There is certain CDR data that falls outside of both required and voluntary consumer data. This includes account data that is not held in the name of a single person, or account data for a joint account where any of the account holders are less than 18 years. For a particular joint account holder, customer data in relation to the other joint account holder is also not required or voluntary consumer data.

1.299. In relation to 'required consumer data', there are certain time limitations that apply. For example, CDR data is not required consumer data at that particular time, where a transaction on an open account occurred more than 7 years previously, or where the account is closed and was closed more than two years before that time.

Part 4 – Joint accounts

Division 4.1 – Preliminary

Clauses 4.1 and 4.2

1.300. This part sets out how the rules apply in relation to joint accounts within the banking sector.

1.301. Data holders are required to provide a joint account management service for consumers with joint accounts to enable them to set preferences in relation to CDR data sharing. This service must be implemented and ready for consumers to use by 1 July 2020, when joint accounts are in scope. Data holders must give effect to preferences set in the joint account management service as soon as practicable.

1.302. Using this joint account management service, joint account holders must be able to elect to each individually make consumer data requests directly to the data holder, and also to give and revoke authorisations to disclose CDR data in response to a consumer data request made by an accredited data recipient. Such elections must also be able to be revoked via the joint account management service.

1.303. A data holder may include as part of the joint account management service a functionality that permits joint account holders to elect to authorise the sharing of CDR data together, that is, to allow multi-party authorisation of individual data sharing arrangements. For this first version of the rules, this functionality is an optional implementation for data holders. However, data holders are expected to work towards

the implementation of multi-party authorisation as this will become a requirement in the future.

Division 4.2 – Operation of these rules in relation to joint accounts

Clauses 4.3 to 4.6

1.304. If the joint account holders of an account have not made an election as described in clause 4.2 then a data holder is not required to seek authorisation to disclose the data. A data holder also cannot disclose data where the request does not accord with the election made by the joint account holders. That is, if no election has been made by two joint account holders to authorise the sharing of CDR, or if the two joint account holder elections are not identical, then requests for data cannot be made to that account.

1.305. If a joint account holder authorises the disclosure of data, consistent with an election made by both joint account holders, they will be provided with a consumer dashboard. Data holders must also provide the other joint account holder with a dashboard equivalent to the dashboard provided to the joint account holder that has authorised the disclosure of data.

1.306. Data holders are required, under rule 7.9, to update each consumer dashboard that relates to a request, including the dashboard of the other joint account holder in the case of joint accounts. However, the obligation to update each consumer dashboard does not apply if the data holder considers it necessary in order to prevent physical or financial harm or abuse not to update the consumer dashboard of the other joint account holder. This is to accommodate existing procedures a data holder may have to protect consumers, for example particular account arrangements relating to consumers that may be experiencing family violence.

Part 5 – Internal dispute resolution – banking sector

Clause 5.1

1.307. CDR participants (both data holders and accredited data recipients) are required to have in place internal dispute resolution (**IDR**) procedures that meet the requirements in the rules (rules 6.1 and 5.12(1)(b)).

1.308. CDR participants must apply their IDR procedures to any expression of dissatisfaction that meets the definition of ***CDR consumer complaint*** in the rules. Data holders and accredited data recipients are expected to address and respond to complaints where they come to the participant's attention and the complainant is identifiable and contactable, even if the complaint has not been made through traditional channels such as via phone or in writing. CDR participants should take a proactive approach to identifying complaints, including those made on social media.

1.309. As a result of other regulatory regimes, many CDR participants will already have IDR procedures in place. These CDR participants must review their existing procedures to ensure that they include CDR consumer complaints, and otherwise meet the IDR requirements.

1.310. For the banking sector, participants will need to comply with parts of ASIC's Regulatory Guide 165. ASIC's Regulatory Guide 165 is available, free of charge, on their website: www.asic.gov.au. Regulatory Guide 165, as in force from time to time, contains references to the Australian complaints management standard, which can be purchased online.

1.311. The internal dispute resolution requirements are that the CDR participant's procedures comply with provisions of Regulatory Guide 165 that deal with:

a. Guiding principles or standards that its internal dispute resolution procedures or processes must meet regarding the following:

(i) commitment and culture

(ii) the enabling of complaints

(iii) resourcing

(iv) responsiveness

(v) objectivity

(vi) fairness

(vii) complaint data collection or recording

(viii) internal reporting and analysis of complaint data

b. outsourcing internal dispute resolution procedures

c. the manner in which, and timeframes within which, it should acknowledge, respond to and seek to resolve complaints

d. multi-tiered internal dispute resolution procedures

f. tailoring internal dispute resolution procedures to its business

g. documenting internal facing internal dispute resolution processes, policies and/or procedures

h. establishing appropriate links between internal dispute resolution and external dispute resolution

as if references in Regulatory Guide 165 to:

i. complaints or disputes were references to CDR consumer complaints

j. financial firms and financial service providers were references to CDR participants.

Part 6 – Staged application of these rules to the banking sector

Division 6.1 – Interpretation

Clauses 6.1 to 6.5

1.312. This part provides the meaning of certain terms including 'initial data holder', 'accredited ADI', 'voluntarily participating ADI' and 'any other relevant ADI'.

1.313. For the banking sector, the initial data holders are the four major banks meaning, Australia and New Zealand Banking Group Limited, Commonwealth Bank of Australia, National Australia Bank Limited, and Westpac Banking Corporation.

1.314. For initial data holders, the rules initially apply in relation to products that are branded with the name of the data holder.

1.315. An ADI that is a data holder, but is not one of the four banks or a restricted ADI, may elect to be treated as a voluntarily participating ADI from the data disclosure commencement date. An ADI can elect to voluntarily participate in CDR early by notifying the Accreditation Registrar in writing. The Accreditation Register is required to include this notification on the Register of Accredited Persons and make the notification publicly available.

1.316. This part also provides the meaning of certain terms such as ‘phase 1 product’, ‘phase 2 product’ and ‘phase 3 product’. These terms should be read in conjunction with Division 6.2 – Staged application of rules.

Division 6.2 – Staged application of these rules

Clauses 6.7 to 6.25

1.317. Data sharing obligations for the CDR in the banking sector are phased and apply progressively to more data holders over time, as illustrated in Table 1 below.

1.318. The obligation to share phase 1 product reference data for initial data holders commences on the '***data disclosure commencement date***', being 30 days after the date on which the data standard described in rule 8.11(1)(e) is made. Voluntarily participating ADIs may also commence sharing product reference data at this time, subject to their registration and the satisfactory completion of testing for the Register. Under rule 6.4, the means by which the ADI may notify the Accreditation Registrar to become a voluntarily participating ADI will be notified on the ACCC's website.

1.319. Consumer data sharing commences on 1 July 2020 for initial data holders. At this time, initial data holders may voluntarily share phase 2 products in addition to phase 1 products. Voluntarily participating ADIs, accredited ADIs and accredited non-ADIs (the latter being reciprocal data holders) commence sharing of consumer data in July 2020. ADIs that do not elect to participate early, and do not become accredited beforehand, commence sharing consumer data on 1 February 2021 along with the brands of the initial data holders.

Key to Table 1
For product reference data sharing:
Required to share: - Particular phases of product reference data
For consumer data sharing:
Required to share data from: - Accounts held in the name of an individual CDR consumer - Open accounts **May share the following data voluntarily:** - CDR data that relates to a joint accounts - CDR data that relates to a closed accounts - CDR data that relates to direct debits - CDR data that relates to scheduled payments - CDR data that relates to payees - CDR data that is "get account detail" or "get customer detail" (within the meaning of the standards
Required to share data from: - Accounts held in the name of one CDR consumer in their name alone - Open accounts - CDR data that relates to a joint accounts - CDR data that relates to a closed accounts - CDR data that relates to direct debits - CDR data that relates to scheduled payments - CDR data that relates to payees - CDR data that is "get account detail" or "get customer detail" (within the meaning of the standards
For *phase 1*, *phase 2*, and *phase 3* products, see Schedule 3, cl. 6.5 of the CDR rules.

Table 1: Commencement schedule

Data holders	**Data sharing obligations**	**1st stage:** data disclosure commencement date - 31 January 2020	**2nd stage**: 1 February 2020 – 30 June 2020	**3rd stage**: 1 July 2020 – 31 January 2021	**4th stage**: 1 February 2021 – 30 June 2021	**5th stage**: 1 July 2021 – 31 January 2022	**6th stage**: from 1 February 2022
Initial data holders (branded NAB, CBA, ANZ, Westpac)	*Product reference data*	Phase 1	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
	Part 3: Consumer data requests made by eligible CDR consumers	-	-	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
	Part 4: Consumer data requests made by accredited persons	-	Phase 1	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
	Part 4: Consumer data requests made by accredited persons (voluntary)	-	Phase 2	-	-	-	-
Any other relevant ADI and initial data holder brands	*Product reference data*	-	-	Phase 1	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
	Part 3: Consumer data requests made by eligible CDR consumers	-	-	-	-	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3
	Part 4: Consumer data requests made by accredited persons	-	-	-	Phase 1	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3

Table 1 (cont.)

Data holders	**Data sharing obligations**	**1st stage:** data disclosure commencement date - 31 January 2020	**2nd stage**: 1 February 2020 – 30 June 2020	**3rd stage**: 1 July 2020 – 31 January 2021	**4th stage**: 1 February 2021 – 30 June 2021	**5th stage**: 1 July 2021 – 31 January 2022	**6th stage**: from 1 February 2022
Voluntarily participating ADI (subject to registration and satisfactory completion of testing)	*Product reference data*	Phase 1	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
	Part 3: Consumer data requests made by eligible CDR consumers	-	-	-	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
	Part 4: Consumer data requests made by accredited persons	-	-	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
Accredited ADI and accredited non-ADI (reciprocal data holder)	*Product reference data*	-	-	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
	Part 3: Consumer data requests made by eligible CDR consumers	-	-	-	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
	Part 4: Consumer data requests made by accredited persons	-	-	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3

Part 7 – Other rules, and modifications of these rules, for the banking sector

Clauses 7.1 to 7.4

1.320. Part 7 outlines other modifications of these rules for the banking sector.

1.321. For the definition of "law relevant to the management of CDR data" in rule 1.7, clause 7.1 specifies that the *Australian Securities and Investments Commission Act 2001* is a law relevant to the management of CDR data for the banking sector.

1.322. For paragraph 56AJ(4)(c) of the Act, the conditions on which an accredited data recipient (the 'person' in rule 7.2(2)) may become a data holder are that:

a. the person is an ADI

b. the CDR consumer, for whom the person has collected CDR data under a consumer data request, has acquired a product from the person

c. the person:

i. reasonably believes that the relevant CDR data is relevant to its provision of the product to the consumer

ii. asked the consumer to agree to the person being a data holder, rather than an accredited data recipient of the CDR data

iii. has explained to the consumer:

A. that as a result, the Privacy Safeguards would no longer apply to the consumer's CDR data

B. the manner in which it proposes to treat the relevant CDR data

C. why it is entitled to provide consumers with this option

iv. has outlined the consequences to the consumer of not agreeing to this

d. the consumer has agreed to the person being a data holder, rather than an accredited data recipient of the relevant CDR data.

1.323. The conditions are intended to cover situations in which the consumer 'switches' to a new ADI to acquire a new product that is substantially the same or similar to the product it previously held. This rule is intended to cover the kinds of situations set out in Examples 1.3 and 1.17 in Explanatory Memorandum for the CDR Bill.

1.324. For the banking sector, ADIs (other than restricted ADIs) meet the criteria for the streamlined (unrestricted) accreditation process. However, once accredited, ADIs must still comply with the ongoing obligations of a person accredited at the unrestricted level (excluding the insurance obligation).

1.325. Restricted ADIs, unlike full ADIs, are however required to meet the insurance obligation.