Explanatory Statement

Competition and Consumer (Consumer Data Right) Rules 2020

Prepared by the Australian Competition and Consumer Commission

Contents

Explanatory Statement – Competition and Consumer (Consumer Data Right) Rules 2020

Background

1. This explanatory statement accompanies the *Competition and Consumer (Consumer Data) Rules 2020* (**rules**).

2. The Consumer Data Right (**CDR**) is an economy-wide reform that will apply sector-by-sector, starting with the banking sector. A sector must be designated by the responsible Minister (**Minister**) before it is subject to the CDR. The objective of the CDR is to provide individual and business consumers (**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 CDR is designed to promote competition and give consumers more control over their data which will facilitate innovative new products and services for consumers.

3. 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 and has a role in the enforcement of the regime. The ACCC is also currently undertaking the role of the Data Recipient Accreditor and the Accreditation Registrar. The OAIC leads on matters relating to the protection of individual and small business consumer privacy and confidentiality, and compliance with the CDR Privacy Safeguards (**Privacy Safeguards**).

4. The 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 shared with consumers and accredited data recipients within the CDR system.

5. Banking is the first sector to be designated by the Minister. On 7 September 2019, the *Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019* (**Banking Designation Instrument**) commenced. The Banking Designation Instrument sets out the types of data the CDR will apply to in the banking sector and 1 January 2017 as the earliest date that this data is held subject to the CDR. It also sets out the designated data holders for the banking sector.

6. 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.

Authority and purpose for making the rules

7. The *Treasury Laws Amendment (Consumer Data Right) Act 2019* introduced Part IVD into the *Competition and Consumer Commission Act 2010* (the **Act**) to provide the legislative framework for the CDR.

8. Under section 56BA(1) of the Act, the ACCC is empowered to make rules with the consent of the Minister (section 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 rules in relation to the Privacy Safeguards. Subject to transitional provisions under the Act, before making the rules, the ACCC is required to consult with the public, the OAIC and any other relevant regulators.

9. The rules have been structured with the general body of the rules intended to apply across sectors, and sector-specific rules to be contained in schedules. An overview of the current version of the rules is as follows:

    a. Part 1 deals with preliminary matters, such as definitions;

    b. Part 2 deals with product data requests;

    c. Part 3 deals with consumer data requests made by eligible CDR consumers;

    d. Part 4 deals with consumer data requests made by accredited persons;

    e. Part 5 deals with accreditation;

    f. Part 6 deals with dispute resolution;

    g. Part 7 deals with the Privacy Safeguards;

    h. Part 8 deals with the data standards;

    i. Part 9 deals with miscellaneous matters such as review of decisions, record keeping and reporting obligations and civil penalty provisions;

    j. Schedule 1 deals with default conditions on accreditations;

    k. Schedule 2 sets out the steps for the purpose of Privacy Safeguard 12 (the security of CDR data);

    l. Schedule 3 is the banking sector schedule.

10. 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

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

12. These rules are compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Human right implications

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

14. The rules provide for important mechanisms to protect consumers' privacy. This includes rules that supplement the Privacy Safeguards in the Act. The Privacy Safeguards are comparable to the Australian Privacy Principles in the *Privacy Act 1988* and seek to ensure the privacy and confidentiality of consumers' data by providing for only authorised access to, and use of, CDR data. Additionally, the rules include strict requirements for consumer consent to the collection and use of their data. A consumer must also authorise any disclosure of their CDR data to accredited parties. The rules set out requirements for transparency on who has requested access to the data and how it will be used.

15. The accreditation of persons to enable them to collect and use CDR data subject to the Privacy Safeguards is a key protection against arbitrary or unlawful interference with privacy. The rules specify that the criterion for accreditation at the 'unrestricted' level of accreditation is that the Data Recipient Accreditor is satisfied that an applicant for accreditation would be able to comply with the obligations of an accredited person. The obligations include that the person:

    a. is 'fit and proper';

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

    c. has internal dispute resolution processes that meet the requirements in Part 5 of Schedule 3 to the rules; and

    d. is a member of a recognised external dispute resolution scheme.

16. 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.

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

Conclusion

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

Self-Assessment and Certification

19. The ACCC has certified that the processes and analysis previously undertaken for the purposes of development and implementation of the CDR are equivalent to a Regulation Impact Statement for the purposes of this instrument.

Consultation

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

21. On 21 December 2018, the ACCC released the *Consumer Data Right Rules Outline* (**Rules Outline**) which set out the ACCC's position on the rules in response to stakeholder consultation on the Rules Framework.

22. An Exposure Draft of the rules, published on 29 March 2019, covered the key aspects of the rules required to implement the CDR in the banking sector. The ACCC sought feedback from consumers, businesses and community organisations on the position and approach taken to the rules in the Exposure Draft. The ACCC considered and took into account stakeholder feedback on the Exposure Draft in finalising the rules.

23. In addition to the ACCC's consultation on the rules, 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

24. The rules are made by the ACCC under section 56BA of the Act. Further information on the authority and purpose for making the rules is at paragraph 8 of this explanatory statement.

Division 1.2 – Simplified outline and overview of these rules

Rules 1.4 to 1.6

25. There are three types of requests that can be made to a data holder to disclose CDR data under the rules:

    a. product data requests made by any person

    b. consumer data requests made by eligible CDR consumers

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

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

27. Product data requests can be made in respect of **required product data** and **voluntary product data**. Required product data includes:

    a. eligibility criteria, terms and conditions, price;

    b. availability or performance of a product (if publicly available); and

    c. **product specific data**

28. Consumer data requests can be made in respect of **required consumer data** and **voluntary consumer data**. Required consumer data includes:

    a. **customer data** identifying or about a particular person;

    b. **account data** about the operation of an account;

    c. **transaction data** identifying or describing a transaction; and

    d. **product specific data** in relation to a particular product that a particular person uses.

29. The simplified outline and overview of the rules provides a summary of how the rules operate. The rules should be read in conjunction with:

    a. the Act, in particular Part IVD of the Act, which provides the legislative framework for the CDR

b. designation instruments made under section 56AC(2) of the Act

c. guidelines made by the Information Commissioner under section 56EQ(a) of the Act

d. data standards made under section 56FA(1) of the Act (and related guidelines issued by the Data Standards Body)

e. regulations made under section 172, section 56BK(3) and section 56GE(2) of the Act.

Division 1.3 – Interpretation

Rules 1.7 to 1.10

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

31. Certain terms in the rules are 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.

32. 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 Act, however, only 'eligible' CDR consumers are able to make consumer data requests under the rules. Schedule 3, clause 2.1 provides, amongst other things, that a CDR consumer for the banking sector is eligible if the consumer:

    a. is 18 years or older (if the person is an individual as opposed to a business); and

    b. has at least one account with the data holder (receiving the request) that is an open account and set up in such a way that it can be accessed online.

33. It is intended that the rules will progressively apply to a broader range of consumers over time.

34. In this explanatory statement references to consumers are references to eligible CDR consumers, unless stated otherwise.

35. The rules contain references to '**accredited persons**' and '**accredited data recipients**' as defined in the Act. Under the Act, 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 only apply when an accredited person receives CDR data. For the avoidance of doubt, all accredited data recipients are also accredited persons.

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

Data minimisation principle

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

CDR data, when providing the goods or services requested by the relevant CDR consumer. An accredited person must not seek to collect more CDR data, or CDR data that relates to a longer time period, than is reasonably needed to provide the goods or services requested by the CDR customer.

Example 1: To assess consumer eligibility for home loans, an accredited person asks consumers to consent to, among other things, the collection of their past 12 months of transaction data and, on an ongoing basis, the next 12 months of their transaction data. However, future transaction data is not reasonably needed for the delivery of the assessment service. The accredited person is in breach of the data minimisation principle.

38. When providing the requested good or service, the accredited person must not use the CDR data it has collected, or CDR data derived from it, beyond what is reasonably needed in order to provide the requested goods or services.

Example 2: Umbel asks consumers for consent to provide an account aggregation service. After Umbel receives CDR data, it uses it for the purposes of providing the account aggregation service, but also to create a profile of consumers' spending habits and disposable income. By creating profiles of consumers, Umbel has used the CDR data beyond what is reasonably needed in order to provide the account aggregation service requested and consented to by the consumer.

Fit and proper person criteria

39. One of the criteria to become accredited (and maintain accreditation) is that the Data Recipient Accreditor is satisfied that the applicant (and **associated persons**, as defined in the rules) is a person who is fit and proper to manage CDR data. Rule 1.9 specifies the criteria to be taken into account by the Data Recipient Accreditor in determining this. The fit and proper person criteria cover 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**, which includes the Act and the Australian Consumer Law.

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

Subdivision 1.4.1 – Preliminary

Rule 1.11

40. This division sets out:

    a. the obligations on data holders for **product data requests** and **consumer data requests**;

    b. the obligations on 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

41. A data holder must provide online services that can be used to make and manage requests for CDR data under the rules.

42. Data holders must provide online services that can be used:

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

    b. by consumers to make requests for their CDR data (**direct request service**). The service must be of comparable timeliness, efficiency and convenience to online services ordinarily used by customers of the data holder. It must also enable data to be disclosed in human-readable form, set out any fees for disclosure of any **voluntary consumer data** (as defined in the rules), and conform to the data standards; and

    c. by 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

43. 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 to disclose CDR data.

44. The rules set out requirements for information that must be displayed on a dashboard and a minimum level of functionality.

45. The rules require a level of dashboard functionality that allows a consumer to, at any time, withdraw consent from an accredited person to collect and use or withdraw authorisation from a data holder to disclose, and for such functionality to be prominently displayed. These withdrawal functions must be simple and straightforward for a CDR consumer to use. The dashboard provided by the accredited person must also enable a CDR consumer, at any time, to elect that their redundant data be deleted, or to withdraw such an election. The dashboard provided by the data holder must provide a withdrawal process that is no more complicated than the process for giving authorisation to disclose.

46. The dashboard is required to be an online service and may be incorporated into online banking or mobile apps.

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

CDR outsourcing arrangements

Rule 1.16

47. An accredited person may disclose CDR data to another person under an outsourcing arrangement, and if it does so, must ensure that the recipient complies with the requirements under the arrangement.

48. A **CDR outsourcing arrangement** is defined in rule 1.10 as an arrangement where a person (the **discloser**) discloses CDR data to another person (the **recipient**) pursuant to 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;

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

        iii. the recipient must, when 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;

        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 3: B3 is an accredited data recipient. In order to make its service economical, B3 enters into an outsourcing arrangement with B4. B4, in turn, relies on services provided by a third company, Bat.

B3 must ensure that it has a written contract with B4 that is an outsourcing arrangement in order for it to disclose CDR data to B4. Likewise, B4 must have a written contract with Bat that is an outsourcing arrangement. Each outsourcing

arrangement must require the recipient of the data to comply with the outsourcing requirements 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.

49. Disclosure under an outsourcing arrangement is an authorised use or disclosure for the purposes of privacy safeguard 6 (see rule 7.7). Any use or disclosure of CDR data by a recipient (whether or not in accordance with the arrangement) is taken to have been use or disclosure by the accredited person (see rule 7.6).

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

Rules 1.17, 1.17A, 1.18

CDR data de-identification process

50. 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 7.12) when the data has become redundant

    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)).

51. 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**).

52. 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 to de-identify data;

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

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

53. 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.

54. 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.

55. If, in making the assessment described in paragraph 51, 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.

56. 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.

57. 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 or techniques applied to the data; and

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

58. 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.

59. The ACCC considers that the development of a data standard for de-identification will be useful to supplement these rules. This may be provided for in a later version of the rules.

Identification of otherwise redundant data that is not to be deleted

60. Where an accredited data recipient has identified CDR data as redundant, it must identify whether certain provisions of the Act apply to the data. These include if it is required to retain the redundant data under an Australian law or a court or tribunal order. If so, the accredited person must retain the CDR data for so long as any of those provisions apply.

CDR data deletion process

61. If an accredited data recipient is required to delete CDR data, including redundant data for the purposes of Privacy Safeguard 12, 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 (currently only outsourced service providers) 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

62. One of the objectives of the CDR is to enable efficient and convenient access to standardised information about products or services in a particular sector, also referred to as product reference data. The disclosure of product data in a standardised form will facilitate easier product comparison for consumers through existing and new services.

Example 4: A product comparison website makes a series of product data requests to a range of banks. The product reference data collected enables the comparison site to publish a report on the highest interest rates currently available for savings accounts.

63. Product data for the purposes of the CDR is data for which there are no CDR consumers. It includes information about terms and conditions, eligibility criteria, and the pricing and availability of products.

64. A product data request may be made for the disclosure of **required product data**, **voluntary product data**, or both kinds of product data. Required and voluntary product data for the banking sector are defined at Schedule 3, clause 3.1 of the rules. While a data holder cannot charge a fee for the disclosure of required product data, a data holder may choose to charge a fee for disclosing voluntary product data.

65. Data holders are required to provide a **product data request service** that any person can use to make product data requests. The requester must make their request in accordance with the data standards. The standards require the product data request service to be made available via an application programming interface (**API**).

66. Subrule 2.4(3) provides that the data holder must disclose product data to the requester. The data must be in machine readable form and disclosed in accordance with the data standards as required by rule 1.12.

67. In responding to a request for required product data, a data holder must disclose required product data that is contained on the data holder's website or in a product disclosure statement that relates to the product. This qualitative rule ensures that the product data available is no less detailed than the product data made available publicly by a data holder on its website or in the relevant product disclosure statement.

Example 5: Bilby Bank's product disclosure statement for a deposit account contains additional fees and charges relevant to the transfer of money overseas that are not product-specific. As these are contained in the product disclosure statement, they are 'required product data' that must be shared in response to a request.

68. A data holder must not impose conditions, restrictions or limitations of any kind on the use of the disclosed product data. The person who receives the product data may use the data in any way they wish.

69. Rule 2.5 provides that the data standards may set out circumstances where a data holder can refuse to disclose required product data in response to a request. Where this occurs, the data holder must inform the requester of the refusal in accordance with the data standards. The standards provide for a range of generic error codes to

be used to notify the refusals and do not require the precise reasons to be identified as to why the request has been rejected.

Part 3 – Consumer data requests made by eligible CDR consumers

Division 3.1 – Preliminary

Rules 3.1 and 3.2

70. The CDR facilitates consumers requesting their own CDR data directly from a data holder. The data holder must disclose the data in human-readable form. The obligation to share CDR data directly with consumers will commence at different times for different classes of data holder (see Part 6 of Schedule 3).

71. Consumer data requests can be made in respect of **required consumer data** and **voluntary consumer data**, which in relation to the banking sector, is defined at Schedule 3, clause 3.2. While a data holder cannot charge a fee for the disclosure of required consumer data, a data holder may choose to charge a fee for disclosing voluntary consumer data.

Division 3.2 – Consumer data requests made by CDR consumers

Rules 3.3 to 3.5

72. If a data holder holds CDR data that relates to a CDR consumer, the consumer may, through that data holder's direct request service, request the data holder to provide them with all or part of that data.

73. For the banking sector, a CDR consumer is eligible to make a direct request if, at the time of making the request, they have at least one account with the relevant data holder that is open and can be accessed online (for example, by using an internet browser or mobile phone application) and, if they are an individual, are 18 years of age or older.

74. If a data holder receives what it reasonably believes to be a **valid** consumer data request a data holder must disclose the requested required consumer data, and may disclose requested voluntary consumer data, in response to that request (subject to the exceptions below) through the direct request service and in accordance with the data standards.

75. Data holders are required to provide a **direct request service** that, among other things, must allow consumers to make a direct request in a manner that is at least as timely, efficient and convenient as existing online services ordinarily used by consumers to deal with the data holder.

Example 6: A consumer data request service could form part of a data holder's online banking website or mobile banking app.

76. A data holder may refuse to disclose required consumer data in the limited circumstance where the data holder considers this to be necessary to prevent physical or financial harm or abuse, or the additional circumstances set out in the data standards. This is to accommodate existing procedures a data holder may have to protect consumers, for example, particular account arrangements relating to consumers who may be experiencing family violence. Where a refusal occurs, the data holder must inform the CDR consumer of such a refusal in accordance with the data standards. The standards provide for a range of generic error codes to be used

to notify the refusals and do not require the precise reasons to be identified as to why the request has been rejected. Generic error codes are used for security reasons and to ensure safety in situations involving potential harm to individuals.

77. For consumer data requests made by consumers with a joint account, see paragraphs 327 to 331.

Part 4 – Consumer data requests made by accredited persons

Division 4.1 – Preliminary

Rules 4.1 and 4.2

78. If an accredited person needs to access a CDR consumer's CDR data in order to provide goods or services to the consumer, the accredited person must obtain the consumer's consent in order to request CDR data from the relevant data holder.

79. If the request is valid, 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 to the accredited person the required consumer data requested and may disclose any voluntary data requested.

80. Consumer data requests by accredited persons are made via APIs. The rules and data standards prescribe the process for making and responding to such requests. This includes the format in which the data must be disclosed and circumstances in which a data holder may refuse to disclose data in response to a valid request.

81. While a data holder cannot charge a fee for the disclosure of required consumer data, a data holder may choose to charge a fee for disclosing voluntary consumer data.

Division 4.2 – Consumer data requests made by accredited persons

Rules 4.3 and 4.4

Requests to collect CDR data

82. The rules permit an accredited person to ask for a CDR consumer's consent to collect and use their CDR data in order to provide goods or services if:

    a. the CDR consumer has requested that the accredited person provide them, or another person, those goods or services; and

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

83. In requesting such consent, the accredited person is required to comply with the requirements set out in Subdivision 4.3.2 of the rules. If consent is obtained in accordance with those requirements, the CDR consumer will have given the accredited person a valid request to seek to collect CDR data from the data holder.

84. Where an accredited person has a valid request and current consent from a CDR consumer, it may request the relevant data holder to disclose some or all of the CDR data that is the subject of the consent provided that it is able to collect and use that data in compliance with the data minimisation principle.

85. An accredited person must make all such consumer data requests through the data holder's accredited person request service and in accordance with the data standards.

86. The accredited person may need to collect data from more than one data holder in order to provide the consumer with the good or service, for example, in the context of an account aggregation service. A single consent from a CDR consumer can be a valid consent that, if current, enables the accredited person to make consumer data requests in respect of CDR data held by multiple data holders.

Rules 4.5 to 4.7

Authorisations to disclose CDR data

87. A data holder that receives a consumer data request that it reasonably believes was made by an accredited person on behalf of an eligible consumer must seek authorisation from the CDR consumer on whose behalf the request was made in accordance with Division 4.4 of the rules and the data standards (unless there is already a current authorisation to disclose the requested data to that accredited person).

88. If the data holder is considering disclosing any requested voluntary consumer data, it must ask for authorisation in accordance with Division 4.4 of the rules and the data standards.

89. For the banking sector, Schedule 3 contains various specific provisions regarding authorisation and joint accounts.

90. If a data holder receives authorisation from the relevant consumer to disclose some or all of the CDR data referred to in a consumer data request, it:

    a. may disclose any of the voluntary consumer data that it is authorised to disclose; and

    b. must disclose the required consumer data that it is authorised to disclose,

    to the accredited person from whom it received the relevant consumer data request through its accredited person request service and in accordance with the data standards

91. A data holder may refuse to seek authorisation in relation to CDR data, or refuse to disclose required CDR data:

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

    b. if 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; or

    c. in the circumstances set out in the data standards.

92. A data holder must inform the accredited person of such a refusal in accordance with the data standards. The standards provide for a range of generic error codes to be used to notify the refusals and do not require the precise reasons to be identified as

to why the request has been rejected. Generic error codes are used for security reasons and to ensure safety in situations involving potential harm to individuals.

Division 4.3 – Consents to collect and use CDR data

Sub-division 4.3.1 – Preliminary

Rules 4.8 and 4.9

93. Consent is one of the key concepts underlying the CDR system. The rules are intended to ensure that requests for consent to collect and use CDR data are transparent and that consumers understand the potential consequences of what they are consenting to.

94. The rules in Division 4.3 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

95. The accredited person's process for seeking consent (**consent process**) must accord with the data standards and be as easy to understand as practicable, having regard to any consumer experience guidelines developed by the Data Standards Body. Accredited persons may be guided by the language and processes of such guidelines and by consumer experience testing regarding consumers' comprehension of the consent process.

96. Visual aids may be used where appropriate, such as in circumstances where they are likely to improve consumer comprehension. For example, visual aids may improve consumer comprehension where they clearly and efficiently convey relationships, processes, concepts or results. On the other hand, visual aids may be less likely to improve consumer comprehension where they are not clear, concise and of an appropriate size and quality.

97. 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. This does not preclude accredited persons from adopting a layered approach where appropriate by, for example, including references or hyperlinks to documents that contain more detailed information. However, consumer comprehension is likely to be improved where all key elements associated with the consent, including an appropriate level of

detail regarding the specific proposed uses of the relevant data, is available to consumers without having to refer to other documents or sources.

98. Consents must not be bundled together, or with other directions, permissions, or agreements.

Example 7: Gregor offers consumers a service that relies on the use of a consumer's CDR data, as well as data sourced through other avenues. Gregor must carefully design its consent flows and consider the impression it creates in its interactions with consumers to ensure it complies with the CDR framework and is not likely to mislead consumers or bundle consents. For example:

- Any request to a consumer or agreement by a consumer to share data that is outside the CDR must not purport to be or be presented as part of the CDR consent flow, otherwise Gregor may breach the rules relating to bundling, referring to other documents, and the requirement to make consent as easy to understand as practicable.
- Gregor should inform the consumer that to provide the service it intends to access non-CDR data also, and should explain the consequences of doing so, including any risks which may arise from the alternative method of sharing.
- Gregor must not create the impression that data collected via mechanisms other than the CDR is subject to the same protections as CDR data when it is not, or otherwise lead a consumer to be likely to be misled about CDR.
- Gregor must treat CDR data in certain ways. Co-mingling CDR data with non-CDR data will not excuse Gregor from adhering to these high standards, and it may need to be prepared to treat all data to those high standards if co-mingled in one pool.

99. The consent process must allow the consumer to actively select or otherwise clearly indicate:

a. which of the particular types of CDR data (referred to as 'data clusters' in the data standards) they are consenting to the accredited person collecting;

b. the specific uses of that data to which they are consenting;

c. the period over which CDR data will be collected and used, up to a maximum of 12 months, and whether the CDR data would be;

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

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

100. The accredited person must ask the consumer for their express consent:

a. for the accredited person to collect those types of CDR data over that period of time;

b. for those uses of the collected CDR data; and

c. to any direct marketing the accredited data recipient intends to undertake as permitted by the rules.

101. Additional requirements apply in circumstances where the data holder proposes to charge a fee for the disclosure of voluntary data.

102. The consent process must also allow the CDR consumer to make an election in relation to deletion of redundant data, in accordance with rule 4.16.

103. In order to allow CDR consumers to make the relevant choices and selections referred to in subrule 4.11(1), an accredited person must not present pre-selected options to the consumer.

Example 8: Milky Whey Bank allows consumers to tick boxes that correspond to the types of CDR data they consent to Milky Whey Bank collecting and using in order to receive Milky Whey Bank's service. Milky Whey Bank complies with the requirement to allow consumers to actively select or otherwise clearly indicate their consent.

104. When asking for consent, the accredited person must give the CDR consumer:

a. the accredited person's name;

b. the accredited person's accreditation number;

c. how the relevant collection and use of data complies with the data minimisation principle;

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

i. that fact;

ii. the amount of the fee; and

iii. 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: the information required under Rule 4.15 (see below);

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 CDR 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; and

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.

Restrictions on seeking consent

Rule 4.12

105. When asking a consumer to provide consent to an 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.

106. An accredited person must not ask a CDR consumer to consent to the collection or use of their CDR data unless the accredited person would comply with the data minimisation principle in respect of that collection or those uses. For example, an accredited person must not seek consent to collect data in excess of what is needed in order to provide the requested good or service.

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

    a. selling the CDR data (unless the data will be 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:

        i. identifying;

        ii. compiling insights in relation to; or

        iii. building a profile in relation to;

    any identifiable person who is not the CDR consumer who made the consumer data request (unless an exclusion in rule 4.12(4) applies).

Example 9: Shoe String Travel offers a service to consumers that tracks their travel spending. It breaks spending down into categories as well as charts 'real spend' against 'budgeted spend'. During its consent process, Shoe String Travel asks consumers to consent to it selling their data to local accommodation businesses so that those businesses can provide offers to consumers within their budget.

Shoe String Travel does not comply with the rules as it asks consumers to consent to the sale of their data that has not been de-identified in accordance with the CDR de-identification process.

108. The requirement above (to not use the CDR 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 CDR 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 that CDR data, CDR data about that person's interactions with the CDR consumer; and

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

Withdrawal of consent

Rule 4.13

109. The rules require accredited persons to allow CDR consumers to withdraw consent 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 accredited person's consumer dashboard. As noted above, consumers must be notified of the consequences if they withdraw their consent. This would include any contractual consequences.

110. If a consumer withdraws their consent in writing, an accredited person must give effect to a withdrawal as soon as practicable, and in any case within two business days after receiving the written request.

111. 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.

112. Withdrawal of consent to collect and use CDR data does not impact a consumer's election to have their redundant data deleted. Withdrawal of consent may bring the time of redundancy forward and therefore, the time of deletion.

Duration of consent

Rule 4.14

113. Consent to collect and use particular 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; or

        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 data holder's authorisation to disclose that data, when the accredited person received that notification;

    d. 12 months after the consent was given; or

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

114. If an accredited person's accreditation is revoked or surrendered, all consents for the accredited person to collect and use data expire 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

115. During a current consent to collect and use CDR data, CDR data can only be disclosed to a person (other than an outsourced service provider) if the data has been de-identified in accordance with the CDR data de-identification process (rule 1.17) and with a CDR consumer's consent (rule 4.11(3)(e)).

116. A use of de-identified CDR data while consent is current may be to sell the data. De-identifying CDR data for sale may enable an accredited data recipient to provide a good or service to the CDR consumer at no charge. To comply with the data minimisation principle, however, an accredited person may only seek to collect CDR it reasonably needs in order to provide the requested goods or service. An accredited person therefore may not collect additional data, namely data that goes beyond what is allowed by the data minimisation principle, if it does so only for the purpose of de-identification and sale.

117. Further, the sale of de-identified CDR data is a disclosure permitted by the rules (rule 7.5(1)(e)) only if the CDR data has been de-identified in accordance with the CDR de-identification process described at rule 1.17. In that respect, the CDR data must have been de-identified such that no person is identifiable or reasonably identifiable from the data.

118. 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 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; and

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

Subdivision 4.3.4 – Election to delete redundant data

Rule 4.16

Election to delete redundant data

119. 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, save for data that is de-identified in accordance with the CDR data de-identification process, be deleted when it becomes redundant data.

120. 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. A consumer may make the election by communicating it to the accredited person in writing, or by using the accredited person's consumer dashboard.

121. 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.

122. 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

123. When asking for consent, 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; or

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

124. If, at the time a particular CDR consumer consented to the collection and use of their CDR data, the relevant accredited person gave a statement of the kind referred to in paragraph 123(a) above, the accredited person must delete that consumer's redundant CDR data, even if the accredited person's general policy has since changed to state that it de-identifies, or may de-identify, redundant data. This is because the treatment of redundant data is governed by Privacy Safeguard 12 and rules 7.12 and 7.13. Rule 7.13 applies in circumstances where an accredited person informed the consumer at the time of consent that the general policy of the accredited person was to delete redundant data and the CDR consumer gave consent on that basis. Deletion of redundant data is the only option in such circumstances.

125. An accredited person that makes a statement of the kind referred to in 122(b) or (c) above, must also state:

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

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

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

    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 its 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

126. An accredited person must give the CDR consumer a notice (**CDR receipt**) as soon as practicable after the consumer provides consent to the accredited person

collecting and using their CDR data or withdraws their consent. It is expected that CDR receipts are provided as close to real time as possible.

127. The CDR receipt must set out specified details relating to the consent under the rules, including the name of each relevant data holder and any other information the accredited person provided to the consumer when obtaining the consent, including any additional terms and conditions or fees.

128. The CDR receipt for a withdrawal of a consumer's consent in accordance with rule 4.13 must state when the consent expired.

129. All CDR receipts must be in writing, and provided otherwise than through the consumer dashboard, although an accredited data recipient may also include a copy on the dashboard if they wish. CDR receipts 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 of consent, and states the time and date when the consent expired. Rainy Day Savings complies with the CDR receipt requirements.

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

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

    a. the consumer's consent is current; and

    b. 90 days have elapsed 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; or

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

132. This notification ensures CDR consumers are reminded of their current consents, which is intended to encourage consumers to actively manage their data sharing arrangements.

Division 4.4 – Authorisations to disclose CDR data

Rules 4.21 to 4.24

133. A data holder's processes for asking CDR consumers to authorise the data holder to disclose their CDR data to an accredited person must:

    a. accord with the data standards; and

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

134. During the authorisation process, a data holder must give the consumer:

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

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

c. the types of CDR 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 can be withdrawn by the consumer at any time; and

g. instructions for how authorisation can be withdrawn.

135. 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; or

d. include or refer to other documents.

Example 11: Caudex Bank's authorisation processes include an interstitial page featuring advertisements for its range of consumer banking products and services. This is not compliant with the rules, which prohibit a data holder from offering additional or alternative services when asking for authorisation.

Withdrawal of authorisation to disclose CDR data and notification

Rule 4.25

136. 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.

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

138. 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

139. 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 using the dashboard, when the authorisation was withdrawn;

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

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

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

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

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

140. 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.

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

142. In order to collect CDR data under the CDR regime, a person must be accredited. A person may apply to the Data Recipient Accreditor (currently the ACCC) to become accredited under Part 5 of the rules. The Data Recipient Accreditor may accredit a person if satisfied that the person meets the criteria for accreditation.

143. Part 5 of the rules also deals with:

    a. how accreditation applications are dealt with by the Data Recipient Accreditor;

    b. obligations of accredited persons;

c. the transfer, suspension, surrender and revocation of accreditation; and

d. related functions of the Data Recipient Accreditor.

Division 5.2 – Rules relating to accreditation process

Subdivision 5.2.1 – Applying to be accredited person

Rule 5.2

144. 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. Accreditation applies to a legal or natural person.

145. The application to be an accredited person must:

a. be in the form approved by the Data Recipient Accreditor (the **approved form**);

b. include any documentation or other information required by the approved form;

c. state:

i. the applicant's **addresses for service**; or

ii. if the applicant is a foreign entity, the applicant's local agent and the local agent's addresses for service;

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

e. if the applicant is not a person specified in a designation instrument, indicate whether it is, or expects to be, the data holder of any CDR 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.

146. An address for service means both a physical address in Australia and an electronic address. Any change to the addresses for service must be notified to the Data Recipient Accreditor.

147. There is currently no fee to apply for accreditation.

Example 12: Pennies from Heaven is a non-bank lender that offers personal loans and therefore is not a person specified in the Banking Designation Instrument. In its application for accreditation, Pennies from Heaven must indicate that it holds data of the type specified in the Banking Designation Instrument because it provides lending products.

Subdivision 5.2.2 – Consideration of application to be accredited person

Rules 5.3 to 5.11

148. 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.

149. If the applicant does not provide the further information in response to a request, the Data Recipient Accreditor might not be in a position to be satisfied that the applicant meets the accreditation criteria.

150. The Data Recipient Accreditor may consult with other Commonwealth, State or Territory authorities as relevant in making its decision to accredit a person, or similar authorities of foreign jurisdictions. This includes, but is not limited to, the Information Commissioner, the Australian Securities and Investments Commission, the Australian Prudential Regulation Authority and the Australian Financial Complaints Authority.

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

152. Alternatively, an applicant may be accredited at the unrestricted level by meeting the criterion for streamlined accreditation set out in the rules for the relevant designated sector. For the banking sector, the criterion, at clause 7.3 of Schedule 3, is that the applicant is an ADI but not a restricted ADI.

153. If an applicant is accredited, the Data Recipient Accreditor must give the applicant a unique number (**accreditation number**) that identifies it as an accredited person.

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

155. If the Data Recipient Accreditor decided to accredit the applicant, the notice must include:

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

    b. the level of accreditation;

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

    d. their accreditation number.

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

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

    b. the applicant's rights to have the decision reviewed by the Administrative Appeals Tribunal.

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

158. Accreditation is subject to the default conditions set out in Schedule 1, and any conditions imposed or varied under rule 5.10. The default conditions are a rule requirement that apply to all accredited persons. They ensure that all accredited persons will have to regularly provide a report or statement about the controls applied

to CDR data. The default condition is fundamental to the protection of CDR data. The Data Recipient Accreditor cannot vary or remove the default conditions and as such the default condition cannot be the subject of review by the Administrative Appeals Tribunal.

159. 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.

160. 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.

161. The Data Recipient Accreditor may impose or vary a condition without notice, if giving 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 CDR data.

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

163. A condition imposed, or varied, under rule 5.10 must include the time or date on which it takes effect.

164. The Data Recipient Accreditor may, but need not, give public notice of a condition or variation imposed or removed under rule 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.

165. 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.

166. 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.

167. 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

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

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

i. misuse, interference and loss; and

ii. unauthorised access, modification or disclosure;

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

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

d. have addresses for service; and

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

169. 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 CDR data; and

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 the rules, to the extent that they are relevant to the management of data. Further information to assist in complying with this obligation is available in guidelines on the ACCC's website. The adequate insurance requirement does not apply to ADIs unless they are a restricted ADI.

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

171. 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 CDR data; or

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.

172. The Data Recipient Registrar must:

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

i. an accreditation;

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

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

iv. a suspension ceasing to have effect;

v. a revocation of an accreditation; or

vi. a notification under subrule 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

173. Accreditation cannot be transferred.

Surrender of accreditation

174. 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 accept the surrender.

Suspension and revocation of accreditation

175. The Data Recipient Accreditor under rule 5.17 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 the 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**. For the rules about revocation and suspension of accreditation, '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

176. The Data Recipient Accreditor also may suspend (but not revoke), in writing, 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 the rules; or

        ii. one or more data standards; or

    b. the Data Recipient Accreditor reasonably believes that a relevant contract between the accredited person and a consumer has a term that is unfair.

Revocation and suspension processes and durations

177. Before revoking an accredited person's registration, the Data Recipient Accreditor must apply the following process:

    a. inform the accredited person of the proposed revocation and when it proposes the revocation to take effect; and

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

    c. notify the person, in writing, of a decision to revoke the person's accreditation.

178. The decision to revoke a person's accreditation can be reviewed by the Administrative Appeals Tribunal under subrule 9.2(b).

179. 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)).

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

181. Before suspending an accreditation, or extending a suspension, the Data Recipient Accreditor must apply the following process:

    a. inform the accredited person of the proposed suspension or extension, including the proposed duration; and

    b. inform the accredited person of when it is proposed the suspension will take effect; and

    c. give the accredited person a reasonable opportunity to be heard in relation to the proposed suspension or extension.

182. If the Data Recipient Accreditor makes a decision to suspend an accredited person's accreditation, the Data Recipient Accreditor must notify the person, in writing, of the suspension and the period of suspension. The decision to suspend an accredited person's accreditation can be reviewed by the Administrative Appeals Tribunal (see subrule 9.2(b)).

183. 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. The decision to extend a suspension can be reviewed by the Administrative Appeals Tribunal (subrule 9.2(b)).

184. The Data Recipient Accreditor may suspend the accreditation or extend the suspension of a person without first applying the prescribed process if there are urgent grounds for the suspension and, because of the urgency, it is not possible to apply the process prior to the suspension.

185. However, if the Data Recipient Accreditor does so, 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.

186. 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

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

    a. Privacy Safeguard 6 (authorised use and disclosure of CDR data);

    b. Privacy Safeguard 7 (authorised use and disclosure of CDR data that relate to direct marketing); and

c. Privacy safeguard 12 (security of CDR data, and de-identification and deletion of CDR data).

188. 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.

189. 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 including the obligations of an accredited person under rule 5.12.

190. 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.

191. 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;

b. the person has collected data under these rules;

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; and

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

i. legal proceedings; or

ii. dispute resolution proceedings;

to which the CDR consumer is a party.

Division 5.3 – Rules relating to the Register of Accredited Persons

Rules 5.24 to 5.32

192. The Accreditation Registrar (currently the ACCC) must enter the following details on the Register of Accredited Persons:

    a. the following details about the accredited person:

        i. name; and

        ii. accreditation number; and

        iii. addresses for service; and

        iv. if 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 an accreditation has been revoked, or the suspension is otherwise no longer in effect, that fact and the date from which the accreditation is once more in effect;

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

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

193. In association 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;

ii. a hyperlink to:

A. the relevant website address of the data holder;

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 Uniform 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

194. The Accreditation Registrar may request a data holder or accredited person to provide the information for inclusion in the associated database, 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 must comply with such a request.

195. Where a data holder or accredited person has provided such information to the Accreditation Registrar and 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, it must inform the Accreditation Registrar of the amendment in the form approved by the Registrar as soon as practicable after it becomes aware.

196. The Accreditation Registrar may, to the extent the Accreditation Registrar considers necessary, amend the associated database to reflect any such amendment of which it has been informed.

197. 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.

198. 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.

199. 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.

200. The Accreditation Registrar must, in the manner it thinks fit, make publicly available;

a. the information that it is required to enter on the information referred to in rule 5.24 regarding the maintenance of the Register of Accredited Persons as provided by the Data Recipient Accreditor; and

b. the information to be kept in association with the Register of Accredited Persons as provided by data holders and accredited persons.

201. On request, the Accreditation Registrar must make available to the ACCC, 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;

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

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

202. The ACCC 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

203. 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; and

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.

204. 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). This civil penalty provision underscores the importance attached to the capability of accredited persons to process requests securely and effectively in accordance with the rules and the data standards. This capability is fundamental to the CDR regime and the transfer and protection of CDR consumer data.

Example 13: A request of this kind may be made where the accreditation status of an accredited person has changed and therefore the Register has been updated and data holders are required to update their information to reflect this change.

205. Exercising such functions, the Accreditation Registrar may test the capacity of accredited persons and data holders to securely share CDR data consistent with the requirements of the CDR regime. Such information can be requested by the Data Recipient Accreditor (and the Information Commissioner or the ACCC) and may be relevant to decisions made by the Data Recipient Accreditor.

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

Part 6 – Rules relating to dispute resolution

Rules 6.1 and 6.2

207. A data holder for a particular sector must have internal dispute resolution processes that meet the internal dispute resolution requirements in relation to that sector. For the banking sector, these requirements are set out in Schedule 3 and require processes that comply with provisions of the Australian Securities & Investments Commission Regulatory Guide 165 (see paragraphs 342-346).

208. Accredited persons are also required, as a result of their ongoing obligations of accreditation, to have internal dispute resolution processes that meet the same internal dispute resolution requirements in relation to one or more sectors (rule 5.12(b)).

209. 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 the Australian Financial Complaints Authority (**AFCA**).

Part 7 – Rules relating to the Privacy Safeguards

Division 7.1 – Preliminary

Rule 7.1

210. 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, voluntary product data and data that has been de-identified in accordance with the CDR data de-identification process at rule 1.17).

211. The OAIC publishes guidance on the Privacy Safeguards.

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

212. 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. The rules

set out additional information that must be included in the policy and also set out how the CDR policy should be made available to consumers.

213. 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, the person may have two separate CDR policies or a single CDR policy, provided that the information contained covers the person acting in both capacities.

214. A data holder's CDR policy must indicate whether it accepts requests for voluntary product or consumer data and, if so, the types of such data that can be requested, 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 assist CDR consumers in knowing what data can be accessed. It also will help inform accredited data recipients as to whether they can seek a CDR consumer's consent for the disclosure of such voluntary data and any fees that may be applicable.

215. 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, for example, could include information about any early cancellation fees.

216. The CDR 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 the countries in which it proposes to disclose CDR data.

217. 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.

218. 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 include 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; and

    b. the further information specified in paragraph 221 below.

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

    a. the following information about deletion of redundant data:

        i. when the accredited data recipient deletes redundant data

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

        iii. how the redundant data is deleted; and

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

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

ii. the further information specified in paragraph 221 below.

220. 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; and

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

221. 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:

i. that fact; and

ii. to what classes of persons it ordinarily discloses such data; and

iii. why it so discloses such data.

222. Accredited data recipients and data holders must also include information in their CDR policies about their internal dispute resolution processes, including how a complaint can be made and the participant's process for handling CDR consumer complaints.

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

Privacy Safeguard 2 – anonymity and pseudonymity

Rule 7.3

224. 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 14: Where relevant to its commercial activities, an accredited data recipient may be required to deal with an identifiable CDR consumer to meet 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

225. Section 56EH of the Act provides that an accredited data recipient must take the steps specified in the rules to notify consumers of the collection of data. The rules provide that a consumer must have a consumer dashboard for each accredited data recipient to which they have given consent to collect and use their data. The accredited data recipient's consumer dashboard must contain a record of collections of CDR data from a data holder. This record must be updated to show, as soon as practicable, what data was collected, when it was collected, and from which data holder.

226. A complete log of collections is not required to be displayed, but an accredited data recipient may choose to provide this level of functionality.

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 7.7, excluding subrule 7.5(3)

227. Section 56EI(1)(b) of the Act outlines that an accredited data recipient must not use or disclose CDR data unless:

    a. the disclosure is required under the consumer data rules in response to a valid request from a CDR consumer;

    b. the use or disclosure is required or authorised under the consumer data rules without requiring the consent of the CDR consumer for the CDR data; or

    c. the use or disclosure is required or authorised by or under another Australian law or a court/tribunal order and the accredited data recipient makes a written note of the use or disclosure.

228. Rules 7.5 and 7.7 authorise an accredited data recipient to use CDR data for certain permitted uses or disclosures. This includes using CDR data to provide goods or services requested by the CDR consumer and disclosing any of a CDR consumer's CDR data to that consumer for the purpose of providing such goods or services. These authorised uses allow the accredited data recipient to, for example, display the details of the consumer's financial position to the consumer as part of providing a financial management service. The rules authorise, but do not require, an accredited data recipient to disclose CDR data to a CDR consumer.

229. Accredited data recipients are also authorised to disclose CDR data, which includes derived CDR data such as insights, to outsourced service providers who are engaged under an outsourced service provider arrangement. CDR data, including insights, may otherwise only be disclosed to third parties where it has been de-identified in

accordance with the CDR data de-identification process under rule 1.17, and where the accredited person has either:

a. a current consent from a CDR consumer to de-identify and disclose some or all of their collected CDR data; or

b. a general policy on de-identifying redundant data or deciding, when the CDR data becomes redundant, whether to delete or de-identify it, and the relevant CDR consumer has not elected to have their redundant data deleted (as available under rule 4.16).

230. Rule 7.5(2) clarifies that the selling of data that has not been de-identified, and the identification, compiling of insights, or profiling of a person other than the CDR consumer or a person interacting with that CDR consumer whose identify is readily apparent from the CDR data, are not permitted uses or disclosures.

Example 15: Olivia uses an app, Aslan, that needs her CDR data in order to provide its budgeting service. Fabian, Olivia's housemate, often transfers Olivia money for rent, bills and other expenses. In Olivia's transaction data, Fabian's identity is readily apparent. Aslan may use the CDR data that relates to Fabian only as reasonably needed in order to provide Olivia with the budgeting service. Such permitted use may include, for example, categorising those transactions in order to better display and understand Olivia's spending and saving habits.

231. Rule 7.6(1) is a civil penalty provision that provides that an accredited data recipient must not use or disclose CDR data that it has collected, or CDR data directly or indirectly derived from it, other than for a permitted use or disclosure. Where an accredited data recipient uses an outsourced service provider, any use or disclosure of that data by the outsourced service provider or a recipient of that data under a further CDR outsourcing arrangement is taken to have been use or disclosure by the accredited data recipient.

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

Rule 7.8 and 7.5(3)

232. Subclause 56EJ(1)(b) of the Act provides that an accredited data recipient of CDR data must not use or disclose data 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 if it is within the scope of the permitted use or disclosure in rule 7.5(3).

233. 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)(c) (iii)). Such consent must be current.

234. The authorisation is limited to those situations where an accredited data recipient or an outsourced service provider acting on behalf of the accredited data recipient, uses the CDR data to send to the CDR consumer:

a. information about upgraded or alternative goods or services to existing goods or services;

b. an offer to renew existing goods or services when they expire; or

c. information about the benefits of the existing goods or services.

235. The information that the accredited data recipient sends to the CDR consumer may include or may be based on an analysis of the CDR data. The CDR data can be used in this way but only to the extent reasonably needed in order to undertake the kinds of direct marketing that are authorised. The use of CDR data in this way will allow the accredited data recipient to use the CDR data to tailor the direct marketing to the CDR consumer. Where the accredited data recipient sends an offer to renew the goods or services, it can only do so prior to expiry of any consent, as the use of CDR consumer data for direct marketing expires at the same time that a consent to use expires.

236. The benefits of the existing goods or services refers to those goods or services requested by the CDR consumer and for which the accredited data recipient obtained the CDR consumer's consent to collect and use the CDR data, in accordance with the data minimisation principle and Privacy Safeguard 6.

Example 16: 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 for direct marketing. Metal Bank analyses Kelly's data and discovers Kelly may 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 permitted uses or disclosures that relate to direct marketing.

237. 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 use and disclosure of CDR data for that purpose is authorised under rule 7.5(1)(a) if 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

238. Section 56EM of the Act provides that a data holder must take the steps 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 as soon as practicable with information about disclosures, including what data they disclosed, when, and to which accredited data recipient.

239. A complete log of disclosures is not required to be displayed on consumer dashboards, but a data holder may choose to provide this level of functionality.

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

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

Privacy Safeguard 11 – quality of CDR data

Rule 7.10

241. 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.

242. The rule relating to Privacy Safeguard 11 requires the data holder to notify consumers of this fact electronically, in writing, including identifying the accredited person/s 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 relevant accredited person/s.

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

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

    a. the security of CDR data; and

    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.

244. Once data has become redundant, the obligation to take the Privacy Safeguard 12 steps for redundant data commences immediately. The expectation is that these steps be taken within a reasonable time frame.

The security of CDR data

Rule 7.11

245. 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.

246. 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 recipients 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; and

    e. manage and report security incidents.

247. The steps are accompanied by a series of information security controls listed at Part 2 of Schedule 2. Additional guidance on the security steps and controls is available in 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

248. 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; and

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

249. 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

250. 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 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 be deleted; and

    c. it is possible 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.

251. If the de-identification of redundant data rule applies, the accredited data recipient must:

    a. apply the CDR data de-identification process outlined in rule 1.17 to the data; and

    b. direct any outsourced service provider that had been provided with a copy of the redundant data either to:

        i. return it to the accredited data recipient; or

        ii. delete the redundant data and any CDR data directly or indirectly derived from it and notify the accredited data recipient of deletion; and

iii. if the outsourced service provider has provided the data to another person to:

A. direct the person to take either of the above steps; and

B. cause similar directions to be made to any other person to whom the data has been further disclosed.

Deletion of redundant data

252. 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.

253. If rule 7.13 applies, the accredited data recipient must apply the CDR data deletion process to the data (rule 1.18).

254. Section 56BAA of the Act includes an additional circumstance in which CDR data is not required to be deleted – where the CDR data relates to any current or anticipated legal proceedings or dispute resolution proceedings to which the CDR consumer is a party.

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

255. 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 (section 56EP of the Act), consumers can make requests to both data holders and accredited data recipients seeking the correction of their data.

256. In response to such a request, a data holder or accredited data recipient must either correct the data or include a qualifying statement with the data to ensure that, having regard to the purpose for which it is held, the data is accurate, up to date, complete and not misleading. The statement should be attached to the data in such a way that it is apparent to users of the data within the data holder or accredited data recipient. Where practicable, this statement must be attached to the data in such a way that it will be apparent to any subsequent users of the data also.

257. Data holders and accredited data recipients cannot charge a fee for responding to or actioning such requests.

258. 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 (section 56EP(3)(b) of the Act). The notice advising the consumer of the outcome of their correction request must set out the complaint mechanisms available to the consumer if they are not satisfied with the outcome of their correction request.

259. If a data holder has corrected 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 will be 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

260. 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

261. The Data Standards Chair must establish and maintain a committee to advise the Chair about data standards (the **Data Standards Advisory Committee**). The written 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.

262. The Chair must appoint, in writing, at least one privacy representative and at least one consumer representative to the Data Standards Advisory Committee. There is no limit on the number of persons who can be on the Committee.

263. The ACCC, OAIC, and Department of the Treasury may elect to be an observer on the Committee and the Chair may invite any other person to be an observer.

Division 8.3 – Reviewing, developing and amending data standards

Rules 8.8 to 8.10

264. 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.

265. The Chair will consult on a standard or amendment to a data 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 or an amendment will not affect its validity or enforceability.

266. 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.

267. The consultation requirements for the making or amendment of data standards do not apply to data standards made before 1 August 2020, such that the Chair need not consult for versions of the standards made prior to that date. This reflects a similar transitional provision in the Act under which consultation on the rules for the banking sector is not required to be undertaken in accordance with requirements in the Act, if the rules are made prior to July 2020. The transitional rule allows an additional month to accommodate the making of, or amendments to, the standards.

Division 8.4 – Data standards that must be made

Rule 8.11

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

269. 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;

    b. the process for obtaining authorisations and consents and withdrawals of authorisations and consents;

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

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

    e. the disclosure and security of CDR data, including seeking authorisations to disclose data in response to consumer data requests;

    f. the types of CDR data to be used by participants in making and responding to requests;

    g. the formats in which CDR data is to be provided in response to requests;

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

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

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

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

270. 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.

271. 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

272. 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

273. The rules must permit the making of applications to the Administrative Appeals Tribunal for review of decisions to vary, suspend or revoke accreditations (section 56BH(4) of the Act). Under the rules, 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; or

    e. revoke an accreditation.

274. The availability of review in these instances is in addition to the section 56CB of the Act which provides for review by the Administrative Appeals Tribunal of a decision of the Data Recipient Accreditor to refuse to accredit a person.

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

275. Records created under the CDR regime may be subject to 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*.

276. 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; and

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

277. 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. collections of CDR data 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 CDR data was de-identified in accordance with rule 1.17, records that are required to be made for the purposes of the CDR data de-identification process;

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

l. 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 17: FastSaver records its consent flows in video format, showing step-by-step what a consumer may consent to while using its app, as well as the format in which 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 the requirement to keep a video record of its consent process.

278. 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. Under rule 9.3(2)(e), to record and explain CDR data that it has collected, an accredited data recipient will need to maintain ‘collection logs’ evidencing the type of CDR data that was collected, when the CDR data was collected (including time and date) and the relevant data holder of the CDR data.

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

280. 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.

281. 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.

282. 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

283. A data holder must prepare a report for each period that is in the form, if any, approved by the Commission and summarises the CDR complaint data that relates to that reporting period.

284. 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.

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

286. The report must:

    a. describe any goods or services using CDR data that were provided or offered to CDR consumers;

    b. describe the types of data that are needed in order to provide those goods or services; and

    c. explain why that data is needed to provide the goods or services to CDR consumers.

287. To the extent that the goods or services, or the types of CDR data needed to provide them were previously described or contained in the person's application to be an accredited person or a report prepared under this rule, the report may refer to the previous description or explanation and set out only any material changes.

288. The report must also:

    a. set out the number of consumer data requests made by the accredited data recipient during the reporting period; and

b. set out the proportion of CDR consumers who, at the date of the report, had exercised the election to delete, by reference to each brand (good or service) of the accredited person.

289. 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 its report, on its website.

290. 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

291. A consumer may request a data holder provide copies of records that relate to them and relate to their authorisations, disclosures of CDR data made in response to a request, and CDR complaint data.

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

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

294. 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.

295. Data holders and accredited data recipients must not charge a fee for making or responding to a consumer's request for copies of the consumer's records.

Subdivision 9.3.2 – Audits

Rules 9.6 and 9.7

296. 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; and

c. the data standards.

297. 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); and

b. these rules to the extent that they relate to the privacy safeguards or the privacy and confidentiality of CDR data.

298. For the purposes of conducting such audits, 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. The data holder or accredited data recipient must comply with any such request.

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

300. The Data Recipient Accreditor may give an accredited data recipient a written notice that requests they produce copies of such records and an accredited data recipient must comply with such a request.

301. 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

302. Under section 56BL of the Act, the rules may specify that certain provisions of the rules are civil penalty provisions (within the meaning of the *Regulatory Powers (Standard Provisions) Act 2014*). Rule 9.8 lists those of the rules that are civil penalty provisions.

303. The obligations in the rules that are fundamental to the CDR regime and the protection of CDR consumers are subject to the maximum penalty. These include obligations relating to seeking consent, disclosing data and complying with the data standards, as well as the obligation upon a data holder and accredited person under rule 5.31 to 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. This level of penalty reflects the seriousness of a contravention of these obligations.

304. A lower maximum penalty level has been adopted for some provisions relating to recordkeeping and notifications and where a data holder or accredited person fails to comply with a request by the Accreditation Registrar to provide information for the associated database or updates to that information.

305. Some rules, such as rules 7.4 (notifying of the collection of CDR data) and 7.10 (notifying of the disclosure of CDR data), set out operative rules for the purpose of the Privacy Safeguards and a person who fails to comply with these requirements may be subject to a civil penalty under the Act.

Schedule 1 – Default conditions on accreditations

Part 1 – Preliminary

Clause 1.1

307. 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

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

309. 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.

310. Further information on ongoing reporting is available in the ACCC's Accreditation Guidelines.

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

311. 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.

312. 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.

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

314. Part 1 sets out the steps an accredited data recipient must take to secure CDR data, which encompasses:

    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; and

    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

315. 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 its CDR data environment, 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 information security training and awareness program.

Schedule 3 – Provisions relevant to the banking sector

Part 1 – Preliminary

Clauses 1.1 to 1.3

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

317. Part 1 also specifies certain information into four broadly grouped categories: 'customer data', 'account data', 'transaction data' and 'product specific data' for the purposes of the Schedule.

318. 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.

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

320. 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.

321. 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 name, 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

322. An 'eligible' consumer, for the purposes of the banking sector is a consumer that is 18 years of age or older (if they are an individual) and (whether or not they are an individual) 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).

323. For the purposes of the above paragraph, if an account:

    a. is a debit card, personal credit or charge card, or a business credit or charge card account; and

    b. the account is in the name of a single person (the 'account holder'); and

    c. has more than one individual authorised to make transactions on the account;

the CDR consumer is the 'account holder'.

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

Clauses 3.1 and 3.2

324. 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.

325. 'Required product data' means CDR data that does not relate to any particular identifiable consumer. 'Required product data' is data that falls 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), is product specific data, and is held in a digital form.

326. '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 be product specific data.

327. 'Required consumer data' for the banking sector means CDR data for which there are one or more CDR consumers that:

a. is within a class of information specified in the banking sector designation instrument; and

b. is:

i. customer data in relation to that consumer; or

ii. account data in relation to an account held by one CDR consumer:

A. in their name alone; or

B. if the person is an individual – jointly with one other individual (**joint account**); or

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

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

c. is held in a digital form by the data holder.

Example 18: Anjuli has two accounts with Eucalypt Bank. Both accounts meet the criteria of 'required consumer data'. However, only one account is able to be accessed by Anjuli online. As one account can be accessed online by Anjuli, and provided that the other account details are also held by Eucalypt Bank in digital form, Anjuli is able to make consumer data requests for both of her accounts with Eucalypt Bank.

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

329. There is certain CDR data that is neither 'required' nor 'voluntary' consumer data and therefore, cannot be shared under the regime. This includes account data, transaction data and product specific data for any account that is:

a. not held in the name of a single person or a joint account with two individuals;

b. a joint account with two individuals where any of the account holders are less than 18 years;

c. an account held in the name of a single CDR consumer where more than one individual is authorised to make transactions on the account; or

d. a joint account where more than two individuals are authorised to make transactions on the account.

Example 19: Theo, Miles and Ella have a personal loan. As the account for the personal loan is held in all of their names, the account is not in scope for the CDR.

330. For a particular joint account holder, customer data in relation to the other joint account holder is not required or voluntary consumer data.

331. In relation to 'required consumer data', there are additional limitations that apply. These include that CDR data is not required consumer data at that particular time, where a transaction on an open account occurred more than seven years previously, or where the account is closed and was closed more than two years before that time. Where an account has been closed within the previous 24 months before a request is made, the data that is required to be shared on that account is a maximum of 12 months prior to the closure of the account. Direct debits that occurred more than 13 months ago are also not in scope.

Part 4 – Joint accounts

Division 4.1 – Preliminary

Clauses 4.1 and 4.2

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

333. 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 from the joint account. The preferences apply at the account level. The joint account holders must have both elected to share CDR data from the account in order for consumer data requests to be made in respect of that account. Data holders must give effect to preferences selected by consumers as soon as practicable.

334. Both joint account holders must be able to elect for each joint account holder to be able to 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. Any elections must also be able to be revoked via the joint account management service.

335. 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 it is intended that this will be a requirement in the future.

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

Clauses 4.3 to 4.6

336. A data holder must not disclose data in response to a consumer data request (either by a consumer or by an accredited person) if one of the joint account holders has not made an election as described in clause 4.2.

337. In these circumstances, if the consumer data request is made by an accredited person, the data holder must not seek a consumer's authorisation to disclose the relevant data.

338. 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 an equivalent dashboard.

339. Customer data in relation to the other joint account holder is neither **required consumer data** or **voluntary consumer data**, and therefore cannot be shared under the CDR regime (clause 3.2(3)(b) of Schedule 3).

340. 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 who may be experiencing family violence.

341. Where a joint account holder revokes an authorisation under clause 4.2(1)(iii), the relevant account data must no longer be shared. However, all other existing authorisations continue under the same terms as the original consent.

Part 5 – Internal dispute resolution – banking sector

Clause 5.1

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

343. CDR participants must apply their internal dispute resolution 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.

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

345. 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.

346. 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; and

viii. internal reporting and analysis of complaint data.

b. outsourcing internal dispute resolution procedures;

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

d. multi-tiered internal dispute resolution procedures;

e. tailoring internal dispute resolution procedures to its business;

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

g. establishing appropriate links between internal dispute resolution and external dispute resolution;

as if references in Regulatory Guide 165 to:

h. complaints or disputes were references to CDR consumer complaints; and

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

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

Division 6.1 – Preliminary

Clauses 6.1 to 6.3

347. Product and consumer data sharing obligations under the CDR are subject to a phased commencement timeline.

348. Part 6 defines the particular types of data holder for the CDR in banking, and sets out when their obligations to share CDR data from particular products commence subject to the phased commencement timeline.

349. For the banking sector, the data holders are:

    a. Initial data holder.

    b. Accredited ADI.

    c. Voluntarily participating ADI.

    d. Any other relevant ADI.

    e. Accredited non-ADI.

350. The initial data holders are the four major banks: Australia and New Zealand Banking Group Limited (ANZ), Commonwealth Bank of Australia (CBA), National Australia Bank Limited (NAB), and Westpac Banking Corporation (Westpac). The data sharing obligations on the four major banks commence first for requests made in relation to products that are branded with the name/s of, or a name similar to, the name of the initial data holder (see clause 6.1 and clause 6.2, row 1). A non-brand request to an initial data holder is made where the request is in respect of a brand of the initial data holder and the brand is not marketed under the name/s of the initial data holder (clause 6.2, row 1) or a name similar to those names (clause 6.1). Data sharing obligations for non-brand requests commence later, and at the same time as the default data sharing obligations for non-major banks (see clause 6.6).

351. An ADI that becomes accredited (accredited ADI) will have data sharing obligations that commence earlier than the default for non-major banks.

352. An ADI that is not accredited, and is not one of the four major banks nor a restricted ADI, may elect to be treated as a voluntarily participating ADI. An ADI can elect to voluntarily participate in the CDR early by notifying the Accreditation Registrar in writing.

353. An ADI that is not a major four bank, and does not elect to participate early or become accredited, is subject to the obligations that apply to *any other relevant ADI*. Foreign ADIs, foreign branches of domestic ADIs, and restricted ADIs are exempted from this.

354. An accredited non-ADI is a reciprocal data holder for the purpose of the rules.

355. **Division 6.2 – Staged application of rules**

Clauses 6.4 to 6.6

356. Division 6.2 sets out the staged application of the rules. The various types of data holders are required to respond to requests under Parts 2, 3 or 4 of the rules (including product and consumer data requests) in respect of the specified phase 1, 2 or 3 products from the specified dates.

Example 20: On 1 June 2020, an initial data holder is required to respond to a product data request for a publicly offered mortgage product.

357. Clause 6.5 authorises the early sharing of CDR data. The purpose of this rule is two-fold. First, it is to facilitate the testing process which will require testing with consumer CDR data ahead of a data holder being on-boarded to the Register. Secondly, it authorises the early sharing of CDR data for any particular stage of data sharing (subject to any testing and on-boarding requirements). A list of the products in scope at each phase is at clause 1.4 of schedule 3 to the rules.

358. Where a data holder becomes accredited or elects to voluntarily participate early, the data sharing obligations for that particular data holder will commence from the date that accreditation takes effect, or the date from which the voluntary election to participate early takes effect.

Table 1: Summary of data sharing obligations

Type of request	Part of these rules	1/2/20[1] to 30/6/20	1/7/20 to 31/10/20	1/11/20 to 31/1/21	1/2/21 to 30/6/22	1/7/21 to 31/1/22	1/2/22 to 30/6/22	from 1/7/22
A brand request to an initial data holder	Part 2 (PRD)	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
	Part 3 (Consumer)	–	–	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
	Part 4 (ADR)	–	Phase 1[2]	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
A non-brand request to an initial data holder; or a request to any other relevant ADI	Part 2 (PRD)	–	Phase 1	Phase 1	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
	Part 3 (Consumer)	–	–	–	–	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
	Part 4 (ADR)	–	–	–	Phase 1[3]	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
A request to a voluntarily participating ADI	Part 2 (PRD)	–	Phase 1	Phase 1	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
	Part 3 (Consumer)	–	–	–	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
	Part 4 (ADR)	–	–	Phase 1	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
A request to an accredited ADI; or a request to an accredited non-ADI	Part 2 (PRD)	–	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
	Part 3 (Consumer)	–	–	–	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3
	Part 4 (ADR)	–	–	Phase 1	Phase 1 Phase 2	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3	Phase 1 Phase 2 Phase 3

[1] See clause 6.4(1)(c). If the rules commence after 1 February 2020, this column takes effect after the rules commence.

[2] See clause 6.4(3) of Schedule 3. At this stage, the data holder is not required to disclose required consumer data about a phase 1 product that relates to any of the following: (1) a joint account (2) a closed account (3) direct debits (4) scheduled payments (5) payees; or (6) the "get account detail" or "get customer detail" APIs.

[3] See clause 6.4(3) of Schedule 3. At this stage, the data holder is not required to disclose required consumer data about a phase 1 product that relates to any of the following: (1) a joint account (2) a closed account (3) direct debits (4) scheduled payments (5) payees; or (6) the "get account detail" or "get customer detail" APIs.

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

Clauses 7.1 to 7.4

Conditions for an accredited person to be a data holder

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

360. 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.

361. For section 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 has acquired a product from the person

c. the person reasonably believes that the relevant CDR data is relevant to its provision of the product to the CDR consumer; and:

i. has asked the consumer to agree to the person being a data holder, rather than an accredited data recipient, of the relevant CDR data; and

ii. has explained to the CDR consumer:

A. that as a result, the Privacy Safeguards would no longer apply to the person in relation to the relevant CDR data; and

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

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

iii. has outlined the consequences to the consumer of not agreeing to this; and

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

362. The conditions are intended to cover situations that include where a 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 is intended to cover the kinds of situations set out in Examples 1.3 and 1.17 in Explanatory Memorandum for the CDR Bill.

363. An accredited person must not ask a CDR consumer to agree to hold their data as a data holder unless the conditions are met. For example, a person who is not an ADI, or a person who does not reasonably believe the CDR data is relevant to its provision of the product, must not ask consumers to agree to them holding the data as a data holder instead of an accredited data recipient.

364. The consumer is to remain in control of their CDR data and is to be in the position where they can make an informed decision whether their CDR data is held subject to

the Privacy Safeguards. The offer to hold data as a data holder, rather than an accredited data recipient (offer), must always be an *offer* and must never be a *requirement* for the person to be able to provide the good or service.

365. A person must reasonably believe that the relevant CDR data is relevant to its provision of the product to the CDR consumer. This threshold is intended to ensure the person does not rely on this provision to hold data outside of the CDR regime where it would not provide a benefit to the CDR consumer. 'Product' is a defined term under clause 1.2 of schedule 3 and takes its meaning from the Banking Designation Instrument.

366. If a consumer expressly agrees to the accredited person holding the data as a data holder, rather than as an accredited data recipient, the Privacy Safeguards will no longer apply to the relevant data. However, if the data holder is an entity subject to the *Privacy Act 1988* and the relevant data contains personal information, it may be subject to protections available under the *Privacy Act 1988*.

Streamlined accreditation

367. For the banking sector, ADIs (other than restricted ADIs) meet the criteria for the streamlined accreditation process for the unrestricted level of accreditation. Once accredited, ADIs must comply with the ongoing obligations of a person accredited at the unrestricted level, with the exception of the insurance obligation. Restricted ADIs are not eligible for streamlined accreditation.