AUSTRALIAN COMPETITION
& CONSUMER COMMISSION

Consumer data right

Rules outline

December 2018

Contents

Glossary

Term	Description
ACCC	Australian Competition and Consumer Commission
Accreditation Registrar	The person who holds an appointment under section 56CK(1) of the Bill or, if no appointment is made, the ACCC
ACL	Australian Consumer Law
ADI	Authorised deposit-taking institution
AFCA	Australian Financial Complaints Authority
API	Application programming interface
APRA	Australian Prudential Regulation Authority
ASIC	Australian Securities and Investment Commission
ASIC Act	*Australian Securities and Investment Commission Act 2001* (Cth)
Bill	Exposure draft of the *Treasury Laws Amendment (Consumer Data Right) Bill 2018* (Cth)
CCA	*Competition and Consumer Act 2010* (Cth)
CDR	Consumer Data Right
CDR consumer/consumer	CDR consumer as defined in the Bill and the Rules
CDR data	CDR data as defined in the Bill and the Rules
Corporations Act	*Corporations Act 2001* (Cth)
Data Recipient Accreditor	The person appointed under section 56CG of the Bill (initially expected to be the ACCC)
Data Standards Chair	The person appointed under section 56FG of the Bill
Designation Instrument	The draft Open Banking Designation Instrument
DSAC	Data Standards Advisory Committee
EDR	External dispute resolution
OAIC	Office of the Australian Information Commissioner
PPF providers	Purchased payment facility providers
Privacy Act	*Privacy Act 1998* (Cth)
Register	Register of Accredited Persons required by section 56CE of the Bill to be established and maintained by the Accreditation Registrar
Rules	Rules made by the ACCC under section 56BA of the Bill
Rules Framework	CDR Rules Framework published by the ACCC on 12 September 2018
Standard/s	The technical CDR standards made by the Data Standards Chair

Introduction

The ACCC published the CDR Rules Framework on 12 September 2018. The Rules Framework sought comment in relation to a range of issues relating to rules to be made to implement the CDR in the banking sector. Submissions on the Rules Framework closed on 12 October 2018.

In response to the Rules Framework, the ACCC received 55 written submissions (available on our website). We also received extensive feedback at our public consultation forums in Sydney and Melbourne and during our online webinar (also viewable online). The feedback received covered a broad range of issues from a wide range of interested parties.

In the Rules Framework the ACCC stated that it would publish draft Rules for consultation in December 2018. However, given the range of complex issues that have been raised during the consultation process, the ACCC has decided to take an alternative approach and publish this Rules Outline which sets out the ACCC's position in relation to version one of the Rules. Conscious of the need for the Standards to align with version one of the Rules, the ACCC has worked closely with Data61 in developing the Rules Outline.

In line with the Treasurer's announcement on 21 December 2018, the Rules Outline reflects the revised commencement schedule with 1 July 2019 being the date for product reference (generic) data being made publicly available and 1 February 2020 the date by which the remaining obligations to share the first tranche of consumer data will commence.[1] The Rules Outline highlights a number of areas where the ACCC is further considering the implications of the revised timeline for the scope of version one of the Rules.

The positions in the Rules Outline assume that the Bill will be passed in the first quarter of 2019. The Rules Outline is intended to provide guidance to stakeholders, including designated data holders, potential data recipients, and consumers, on what version one of the Rules will require of CDR participants. Text in italics is explanatory and notes areas where positions have changed from the Rules Framework. The policy positions in the Rules Outline will be reflected in the draft Rules which the ACCC intends to publish for consultation in the first quarter of 2019. After consultation on the draft Rules, the ACCC may make further refinements before submitting version one of the Rules to the Treasurer for consent.

In the Rules Framework we stated that the ACCC would not address all potential issues in version one of the Rules but would instead seek to make rules on the matters that are essential to the commencement of the CDR in the banking sector. We maintain this approach in the Rules Outline and intend to do so for all other documents related to version one of the Rules.

[1] The ACCC will keep this date under review in light of legislative and other developments.

Rules outline

1. General obligations

Sharing CDR data with consumers

1.1. In response to a request from a consumer, a data holder must share that consumer's data with either:

a. an accredited data recipient to whom the consumer has provided their consent, or

b. the consumer themselves.

1.2. An accredited data recipient must obtain consent from a consumer to collect and use their CDR data in accordance with the Rules (see section 7 below).

1.3. The sharing of CDR data with an accredited data recipient must occur via APIs and in accordance with the Standards.

1.4. A data holder must enable consumers to make a request to share their CDR data via existing mechanisms on their account(s). The mechanisms provided to enable consumers to make a request must allow:

a. a request to be made in a manner that is no less timely, efficient, and convenient than the mechanisms ordinarily used by the data holder to communicate with consumers

b. consumers to nominate specific CDR data as part of their request.

The Rules Framework proposed that all data sharing occur via APIs. The ACCC has changed its position in light of feedback that it is not practical for consumers to receive their data through APIs and due to the added security risks of this approach.

Making generic product data publicly available

1.5. A data holder must share product reference (generic) data (as defined in paragraph 4.19) in relation to products as set out at paragraphs 4.2 to 4.11.

1.6. The sharing of product reference (generic) data must occur via APIs and in accordance with the Standards.

Exemptions to sharing CDR data with an accredited data recipient

1.7. Data holders will be exempted from the obligation to share CDR data in response to a valid request in limited circumstances. These include where the data holder has reasonable grounds to believe that denying the consumer's request is necessary as an emergency measure to avoid imminent risk of serious harm to an individual or for the security, integrity or stability of the CDR system. Data holders will be required to inform the Data Recipient Accreditor of instances of reliance on an exemption within 24 hours.

1.8. An exemption will apply at the authorisation level; that is, if an exemption applies the data holder will be exempted from the obligation to share the consumer's CDR data in response to a particular request in its entirety.

2. Data holders

2.1. Data holders include 'initial data holders', 'subsequent data holders' and 'reciprocal data holders'.

2.2. The ACCC may grant a data holder a temporary exemption from obligations under the Rules, where the ACCC considers it appropriate to do so.

Initial data holders

2.3. The following entities, who are ADIs within the meaning of the *Banking Act 1959* (Cth), are initial data holders:

a. Australia and New Zealand Banking Group Limited

b. Commonwealth Bank of Australia

c. National Australian Bank Limited

d. Westpac Banking Corporation.

2.4. The entities specified above are initial data holders in relation to their primary banking brands and will be subsequent data holders in relation to their related or subsidiary banking brands.

2.5. The Rules will provide a mechanism for an ADI (other than the entities specified above) to elect to become a data holder for product reference (generic) product data on 1 July 2019 and for all other CDR data from 1 February 2020[2].

Subsequent data holders

2.6. Subsequent data holders are ADIs within the meaning of the *Banking Act 1959* (Cth), other than:

a. initial data holders

b. foreign bank branches licensed to conduct banking business in Australia through branches

c. foreign bank branches of domestic banks.

Reciprocal data holders

2.7. ADIs (other than initial data holders) who are accredited data recipients will be reciprocal data holders from 1 February 2020. This means that those ADIs who seek to receive CDR data will be required to share CDR data in accordance with the Rules from 1 February 2020 in response to a valid request from a consumer.

2.8. Applicants for accreditation that are not ADIs but that hold, or expect to hold, data that falls within the data specified in a CDR designation instrument, must declare this in their application for accreditation. If accredited, the accredited data recipient will be considered a reciprocal data holder and required to share CDR data in accordance with the Rules from a date to be determined by the ACCC in response to a valid request from a consumer.

[2] This paragraph was corrected on 25 January 2019 to include reference to sharing generic product data from 1 July 2019.

2.9. Reciprocal data holders are not obliged to share data that is held by the reciprocal data holder only as a result of the CDR regime; that is, an accredited data recipient is not required to 'on-share' CDR data.

2.10. Reciprocal data holder obligations will ultimately apply across sectors, with data sharing between sectors once each sector is designated. Therefore, entities from a sector other than banking will be able to become an accredited data recipient and receive CDR data but reciprocal data holder obligations will only apply to them once their relevant sector is designated.

3. CDR consumer

3.1. A CDR consumer may be an individual or an entity. A CDR consumer who is an individual must be 18 years or older.

3.2. A CDR consumer must:

a. be a customer of a data holder

b. be enabled to access the data holder's products via online channels, including web browsers or mobile applications

c. have a relevant account with a data holder being an active account with a data holder or an account that was closed on or after 1 January 2017 (an inactive account), and

d. hold a relevant authority to share data.

3.3. The ACCC may, after consultation with relevant stakeholders, specify a date or dates on which a CDR consumer will include:

a. a former customer of a data holder

b. a customer not enabled to access data holder products via online channels

c. an individual younger than 18 years of age.

3.4. A CDR consumer will hold a relevant authority to share data if:

a. the CDR consumer has individual authority to share data

b. in relation to a joint account, the rules below in relation to joint accounts are met (see paragraphs 7.7 to 7.8 below).

3.5. A subsequent version of the Rules will deal with the authority to share data relating to multi-party accounts (other than joint accounts).

The CDR will initially be available to online customers (existing and new) of data holders. These customers will be able to access data from active accounts and inactive accounts. Offline and former customers will come within scope in a subsequent version of the Rules. The ACCC has changed its position on including minors in version one of the Rules given that stakeholders did not support their inclusion.

Individual and joint accounts will be in scope from 1 February 2020. In the case of credit card accounts, secondary card holders will not fall within the definition of CDR consumer in version one of the Rules.

In relation to multi-party accounts (other than joint accounts) which were referred to in the Rules Framework as 'complex accounts' and include accounts held by business entities or multi-entity corporate structures (for example, large companies and associations, partnerships, trustees, joint ventures, and self-managed super funds), or accounts with multiple authorisations, the ACCC is considering how to incorporate them in a subsequent version of the rules.

4. Data sets

4.1. CDR data is data in relation to a product and includes customer data, account data, transaction data and product data (as defined in paragraphs 4.12 to 4.20 below).

Products

4.2. Products are phase 1 products, phase 2 products and phase 3 products.

Phase 1 products

4.3. Phase 1 products are those products offered to the general public and commonly understood as:

a. savings accounts

b. call accounts

c. term deposits

d. current accounts

e. cheque accounts

f. debit card accounts

g. transaction accounts

h. personal basic accounts

i. GST and tax accounts

j. credit and charge cards (personal)

k. credit and charge cards (business).

4.4. Obligations on initial data holders to share CDR data in respect of the phase 1 products commence:

a. on 1 July 2019 for product reference (generic) product data; and

b. by no later than 1 February 2020 for all other CDR data.

4.5. Obligations on subsequent data holders to share CDR data in respect of phase 1 products commence on 1 July 2020[3] unless they are a reciprocal data holder, in which case the obligations commence when they become an accredited data recipient after 1 February 2020 (see paragraph 2.7).

[3] This paragraph was corrected on 25 January 2019 to change the reference to subsequent data holder obligations commencing on 1 February 2021. The correct date is 1 July 2020.

Phase 2 products

4.6. Phase 2 products are those products offered to the general public and commonly understood as:

a. residential mortgages

b. investment mortgages

c. mortgage offset accounts.

4.7. Obligations on initial data holders and reciprocal data holders to share CDR data in respect of phase 2 products commence on 1 February 2020.

4.8. Obligations on subsequent data holders to share CDR data in respect of phase 2 products commence on 1 February 2021.

Phase 3 products

4.9. Phase 3 products are those products available to the general public and commonly understood as:

a. business finance

b. personal loans

c. lines of credit (personal)

d. lines of credit (business)

e. overdrafts (personal)

f. overdrafts (business)

g. asset finance (including leases)

h. cash management accounts

i. farm management accounts

j. pensioner deeming accounts

k. retirement savings accounts

l. trust accounts

m. foreign currency accounts

n. consumer leases.

4.10. Obligations on initial data holders and reciprocal data holders to share CDR data in respect of phase 3 products commence on 1 July 2020.

4.11. Obligations on subsequent data holders to share CDR data in respect of phase 3 products commence on 1 July 2021.

CDR data

Customer data

4.12. Customer data is data that identifies a consumer and any persons authorised to act on the consumer's account. Customer data includes, at a minimum:

   a. the consumer's name, which may include a business name and number(s) (such as ABN or ACN)

   b. the consumer's contact details, which may include phone numbers, email addresses and physical addresses.

4.13. Customer data may include other identifying information, including where that information assists to distinguish one consumer from another.

4.14. Customer data does not include the date of birth of an individual.

4.15. In relation to business consumers, customer data may include the type of business, establishment date, registration date, organisation type, country of registration, and whether the business is a charitable or non-profit organisation.

4.16. Customer data also includes information the consumer provided to the data holder at the time of opening the account that relates to the consumer's eligibility to acquire the product (that is, in connection with an application process). However, this information will not be required to be shared via an API and must be shared directly with the consumer in response to the consumer's valid request.

Account data

4.17. Account data includes, at a minimum:

   a. information identifying the account, including account number and account name(s)

      i. credit card account numbers must be treated in accordance with any applicable laws, obligations and/or standards that apply to the data holder, which may include masking credit card numbers to meet security requirements

   b. the opening and closing balances for the account, including a current balance and available funds

      i. account data may include a running balance, though a data holder is not obliged to share a running balance

   c. authorisations on the account, including:

      i. direct debit deductions, which will include, to the extent available:

         - identifying information for the merchant or party that has debited the account
         - the amount the merchant or party has debited on each occasion
         - the date the merchant or party has debited the account

      ii. scheduled payments, which may include regular payments, payments to billers and international payments

iii. details of payees stored with the account, such as those entered by the customer in a payee address book.

The ACCC recognises the limitations in providing direct debit information, hence the information is to be provided to the extent available in version one of the Rules. The ACCC expects that as more information becomes available, and better processes develop over time in relation to direct debits, more detailed direct debit information will be included in subsequent versions of the Rules.

Transaction data

4.18. Transaction data includes, at a minimum:

a. the date on which the transaction occurred

b. the relevant identifier for the counter-party to the transaction

i. where the counter-party is a merchant, transaction data must include information provided by the merchant

ii. where the counter-party is a merchant, transaction data may include additional merchant identifiers where they have been added by the data holder, though the data holder is not obliged to share this data

c. the amount debited or credited pursuant to a transaction

d. any description of the transaction

e. the 'simple categorisation' of the transaction (e.g. whether the transaction is a debit, credit, fee, interest, etc.)

i. transaction data may include any additional descriptive categorisation of the transaction added by the data holder (e.g. 'transport', 'health', 'entertainment', etc.), though a data holder is not obliged to share this data.

The Rules Framework noted that the ACCC was considering whether 'transaction metadata' should be included within the scope of transaction data for the first version of the Rules, and sought views from stakeholders. The ACCC does not propose to define 'transaction metadata' in addition to the data described above for the first version of the Rules, and will give the issue further consideration for a subsequent version of the Rules.

Product data

The Designation Instrument refers to 'information about a product' and provides that this may relate to the product as offered or provided to particular classes of consumer, or as tailored to a particular consumer. This is consistent with the ACCC's position in the Rules Framework that product data includes 'product reference data' which does not relate to an identifiable or reasonably identifiable person and which may be shared publicly, and product data that does relate to an account or accounts held by an identifiable or reasonably identifiable person. The Rules will define product data in line with this approach.

Product reference (generic) data

4.19. Product data includes ‘product reference data’, which includes, at a minimum, data on:

a. product type

b. product name

c. product prices including fees, charges and interest rates (however described)

d. features and benefits, including discounts and bundles

e. terms and conditions

f. customer eligibility requirements.

Consumer product data

4.20. 'Consumer product data’ is product data that relates to an account(s) held by a consumer and includes, at a minimum, data on:

a. product type

b. product name

c. product prices, including fees, charges, and interest rates (however described)

i. interest rates include the current applicable interest rate as well as any other interest rates applicable to the product, and any terms and conditions associated with those interest rates

ii. product prices include those negotiated individually with the consumer

d. features and benefits of the product, including discounts and bundles, including features and benefits negotiated individually with the consumer

e. terms and conditions

f. customer eligibility requirements.

Authorisation data

4.21. Data relating to the authorisations given by consumers under the CDR will not be in scope for version one of the Rules but may be included at a later date.

Specification in data standards

4.22. The Standards may include further detail with respect to the relevant CDR data including specific fields and formats.

An overview of the CDR data sets as set out in the Designation Instrument, Rules and Standards is provided at **Schedule 1**.

Note also that the Bill proposes a concept of an ‘earliest holding day’, which is the earliest date from which data can be within a designated data set. The earliest holding day must not be earlier than the first day of the calendar year that is 2 years before the calendar year in which the designation instrument is made (see section 56AC(4) of the Bill).

5. Accreditation

5.1. There will be no fee for an application for accreditation in version one of the Rules.

Levels of accreditation

5.2. There will be one general level of accreditation in version one of the Rules.

In a subsequent version of the Rules, the ACCC proposes to introduce additional levels of accreditation, including levels of accreditation that accommodate business models that use third party intermediaries to collect and/or hold CDR data.

The first general level of accreditation will enable an accredited data recipient to receive all CDR data within scope for banking and will therefore be subject to stringent obligations.

The general level of accreditation will apply to additional designated sectors and on the basis that the need for additional accreditation requirements will be considered as the CDR regime is extended.

Accreditation process

5.3. An application for accreditation must be in an approved electronic form as specified by the Rules.

5.4. The approved form will require applicants to provide sufficient detail to enable identity verification of the applicant or, in the case of an applicant that is a body corporate, enable identity verification of its directors, company secretary and senior managers.

5.5. Applicants must nominate an address for service (or, in the case of foreign applicant for accreditation, its local agent's address for service) in accordance with regulation 12 of the *Competition and Consumer Regulations 2010* (Cth).

5.6. Applicants must provide a description of the services they intend to offer consumers using CDR data as an accredited data recipient.

This is relevant contextual information to enable the Data Recipient Accreditor to consider the other information and documents provided with an application for accreditation and whether the criteria for accreditation are satisfied.

5.7. Applicants that are not ADIs must indicate whether they hold, or expect to hold, data that is specified in a CDR designation instrument (see paragraph 2.8).

5.8. Applicants that are part of a group of companies that is applying for more than one accreditation must provide the names of the other applicants in the group. The Data Recipient Accreditor will use its best endeavours to assess all accreditation applications together that are made by applicants from the same group to ensure that these applications are dealt with efficiently and consistently.

5.9. Applicants for accreditation are required to notify the Data Recipient Accreditor of any material changes in circumstance that may affect their application (after it has been submitted) and the Data Recipient Accreditor's decision to grant accreditation. Any change in the nominated address for service must also be notified to the Data Recipient Accreditor.

Criteria for the general level of accreditation

5.10. To grant accreditation, the Data Recipient Accreditor must be satisfied that the applicant meets the accreditation criteria set out in Table 1.

The ACCC will publish draft accreditation application guidelines relating to assessment of the accreditation criteria with the draft Rules. Interim guidance is provided in Table 1.

5.11. In considering an application for accreditation, the Data Recipient Accreditor may consult with other relevant regulators including the OAIC and ASIC.

Table 1: Accreditation criteria (and continuing obligations on accredited data recipients)

Requirement	Matters the Data Recipient Accreditor will take into account
The applicant is a fit and proper person to manage CDR data	• Whether the applicant (or its directors, company secretary, or senior managers) have been convicted of a serious criminal offence (as defined), or an offence of dishonesty. *Serious criminal offence* for this purpose is: An offence under any law of the Commonwealth or a State or a Territory for which, if the act or omission had taken place in the Jervis Bay Territory, a person would be liable, on first conviction, to imprisonment for a period of not less than 5 years, and Where the offence has occurred within the last 10 years. Jervis Bay Territory is mentioned because it is a jurisdiction in which the Commonwealth has control over the criminal law. *Senior manager* will be defined in terms of a person who: (a) makes, or participates in making, decisions that affect the management of CDR data, and/or (b) has the capacity to affect significantly the institution's management of CDR data. • Whether the applicant (or its directors, company secretary, or senior managers) has been found to have contravened a law relevant to the management of CDR data including the CCA (including the ACL), ASIC Act, the Corporations Act and the Privacy Act. In the case of foreign accredited data recipients (or their directors, company secretary or senior managers), whether they have been found to have contravened a similar law in a foreign jurisdiction that is relevant to the management of CDR data. • Whether the applicant (or its directors, company secretary or senior managers) have been the subject of a determination by the Privacy Commissioner. • Whether any of the applicant's directors have been disqualified from managing corporations or are subject to a banning order. • Whether the applicant (or its directors, company secretary or senior managers) have a history of insolvency or bankruptcy. • Any other relevant matter. Evidence of any of the above matters will not automatically be grounds to refuse an application for accreditation. Each application will be considered on a case-by-case basis and in accordance with procedural fairness.
Has adequate practices,	To enable assessment of this criterion the applicant will need to:

Requirement	Matters the Data Recipient Accreditor will take into account
procedures, and systems in place to manage CDR data and information security risks	• provide a copy of the applicant's policy on the management of CDR data (as required by Privacy Safeguard 1) • attest that the applicant has practices, procedures and systems in place to comply with the CDR regime • provide evidence that the applicant meets the minimum requirements for information security set out in **Schedule 2** (which are the steps required to be taken under Privacy Safeguard 12) through an independent audit against the rules in Part I, including the mandatory controls listed at Part II of Schedule 2. The ACCC's intention is to allow accredited data recipients to leverage their existing industry information security certifications. However, in using such certifications to demonstrate compliance with the information security requirements in the Rules, applicants must note that existing information security certifications (e.g. ISO27001, SOC2 etc.) may not demonstrate compliance with all of the controls required to be met under the CDR regime. It is the responsibility of the applicant to provide evidence of these controls being adequately designed and implemented and operating effectively, commensurate with the expectations set out in Schedule 2.
Has internal dispute resolution procedures that meet the requirements in the Rules	An applicant will need to demonstrate that it has procedures in place that meet the internal dispute resolution rules (see paragraph 10.1).
Is a member of an EDR scheme recognised for the CDR	The ACCC intends to recognise AFCA as the EDR scheme for the banking sector. An applicant will need to provide proof that it is a member of AFCA.
Has adequate insurance or comparable guarantee to compensate consumers for loss arising from breach of obligations under the CDR regime	**Adequate insurance** The ACCC will not mandate the type of insurance to be held by an accredited data recipient. The requirement to have adequate insurance will require an applicant to consider, based on the professional services they offer and their possible exposure under the Bill and Rules, whether they require professional indemnity insurance, cyber insurance, or both. In relation to the scope of insurance cover, the ACCC expects that its guidelines will require the following: • The insurance should indemnify the accredited data recipient for any civil liability to consumers arising from the collection, use or disclosure of CDR data. • To the extent that a data recipient considers that professional indemnity insurance is necessary, it should not contain exclusions relating to privacy legislation (including the CDR regime) or data breaches, unless appropriate cyber insurance has also been obtained. • To the extent that a data recipient considers that cyber insurance is necessary, it should include cover for third party liability arising from

Requirement	Matters the Data Recipient Accreditor will take into account
	breaches of privacy legislation, including the CDR regime. • Any insurance includes any award made by an EDR scheme, including AFCA. In relation to the amount of cover that will be adequate, the ACCC expects that the requirement will generally be proportionate to the size of the business and subject to a minimum requirement to hold cover of at least $2 million per event. Copies of the relevant insurance policies and certificates of currency will need to be provided with the application for accreditation. **Comparable guarantee** In limited circumstances, the ACCC may approve alternative arrangements in the form of a comparable guarantee (for example, where an appropriate guarantee is provided by a parent or related company of an applicant).

Streamlined accreditation

5.12. Streamlined accreditation will apply to ADIs including PPF providers. Partial streamlined accreditation will apply to restricted ADIs.

5.13. Streamlined accreditation will not apply to subsidiaries of ADIs that are not ADIs.

5.14. Streamlined accreditation will not be provided to Australian Financial Services Licence and Australian Credit Licence holders.

The draft accreditation application guidelines (see paragraph 5.10) will include guidance on streamlined accreditation.

Table 2: Streamlined accreditation requirements

Requirement	ADIs	PPF providers	Restricted ADIs
The applicant is a fit and proper person to manage CDR data	**Streamlined** ADIs will be required to **attest** that their fit and proper policy covers the matters taken into account for the CDR fit and proper person test, including that it covers senior managers for the purpose of the CDR test	**Streamlined** PPF providers will be required to **attest** that their fit and proper policy covers the matters taken into account for the CDR fit and proper person test, including that it covers senior managers for the purpose of the CDR test	**Streamlined** Restricted ADIs will be required to **attest** that their fit and proper policy covers the matters taken into account for the CDR fit and proper person test, including that it covers senior managers for the purpose of the CDR test
Has adequate practices, procedures, and systems in place to manage CDR data and information security risks	**Streamlined** ADIs will be required to provide a copy of their policy about the management of CDR data (Privacy Safeguard 1) and **attest** that they have sufficient practices, procedures and systems in place to comply with	**Streamlined** PPF providers will be required to provide a copy of their policy about the management of CDR data (Privacy Safeguard 1) and **attest** that they have sufficient practices, procedures and systems in place to comply with	**Meet in full** As set out in Table 1 above

Requirement	ADIs	PPF providers	Restricted ADIs
	the CDR regime.	the CDR regime.	
Has internal dispute resolution procedures that meet the requirements in the Rules	**Streamlined** ADIs will be required to **attest** to meeting the requirements in the Rules	**Streamlined** PPF providers will be required to **attest** to meeting the requirements in the Rules	**Meet in full** As set out in Table 1 above
Is a member of an EDR scheme recognised for the CDR	**Meet in full** ADIs will be required to provide proof that they are a member of AFCA	**Meet in full** PPF providers will be required to provide proof that they are a member of AFCA	**Meet in full** Restricted ADIs will be required to provide proof that they are a member of AFCA
Has adequate insurance or comparable guarantee to compensate consumers for loss arising from breach of obligations under the CDR regime	ADIs will be **exempted** from having to meet this requirement	PPF providers will be **exempted** from having to meet this requirement	**Meet in full** As set out in Table 1 above

5.15. The ACCC may consult with APRA on any of the above requirements in considering an application for accreditation by an ADI, a PPF provider or a restricted ADI.

Continuing obligations on accredited data recipients

5.16. An accredited data recipient has continuing obligations relating to the criteria for accreditation to maintain:

a. their fit and proper person status

b. adequate practices, procedures and systems to manage CDR data and information security risks

c. internal dispute resolution procedures that meet the requirements set out in the Rules

d. membership of the recognised EDR scheme for the banking sector

e. adequate insurance or comparable guarantee to compensate consumers for loss arising from breach of obligations under the CDR regime.

5.17. These continuing obligations also apply to accredited data recipients provided with streamlined accreditation, except where the accredited data recipient was exempted from meeting any particular accreditation criteria.

5.18. Accredited data recipients are required to provide an annual attestation of compliance with their obligations under the Privacy Safeguards and the Rules.

5.19. The ACCC and OAIC will monitor compliance with the continuing obligations through an audit and compliance program (see paragraph 9.9 below).

5.20. Accredited data recipients are required to notify the Data Recipient Accreditor, as soon as practicable, of any material changes in circumstance that may affect their ability to meet their continuing obligations.

Accreditation status disclosure

5.21. The Data Recipient Accreditor will specify the manner in which an accredited data recipient is permitted to describe its accredited status. The approved form may include the use of an approved CDR logo. The use of the ACCC's logo will be prohibited.

Accreditation of foreign entities

5.22. A foreign applicant for accreditation must appoint a local agent to accept service on behalf of the applicant.

5.23. If accredited, a foreign accredited data recipient is obliged to maintain a local agent and to notify the Data Recipient Accreditor of any change in appointment of its local agent.

Transfer of accreditation

5.24. Transfer of accreditation to another person will not be provided for in version one of the Rules.

Consequences of change in control of accredited data recipient

5.25. Change in control of an accredited data recipient will not affect accredited status, however, an accredited data recipient will have ongoing obligations to notify the Data Recipient Accreditor of any material changes in circumstances that are relevant to compliance with its obligations, including the fit and proper person obligation.

Data Recipient Accreditor's powers

5.26. The Data Recipient Accreditor has the power to:

a. not consider an incomplete application

b. require further information from an applicant in order to assess an application

c. conduct interviews with an applicant in order to assess an application

d. grant accreditation subject to conditions, which may be imposed as part of the decision to accredit or imposed after accreditation has been granted

e. vary conditions applying to an entity's accreditation

f. have third parties undertake reviews as part of the accreditation process, which would form part of the material on which a decision to grant accreditation is based

g. suspend, revoke or vary an accreditation.

Suspension or revocation of accreditation

5.27. The Data Recipient Accreditor may suspend or revoke an accredited data recipient's accreditation where:

a. the Data Recipient Accreditor has reason to believe that the accredited data recipient obtained accreditation through false statements or other irregular means

b. the accredited data recipient failed to notify the Data Recipient Accreditor of a material change in circumstance that may affect its ability to meet its continuing obligations

c. the accredited data recipient (or its directors, company secretary or senior managers) is found to have contravened a law relevant to the management of CDR data including the CCA (including the ACL), the ASIC Act, the Corporations Act and the Privacy Act. In the case of foreign accredited data recipients, the accredited data recipient (or its directors, company secretary or senior managers) is found to have contravened a similar law in a foreign jurisdiction that is relevant to the management of CDR data

d. the Data Recipient Accreditor has reason to believe that suspension is necessary for the protection of consumers, or to protect the security, integrity, stability of, or trust in, the CDR regime.

Additional grounds for suspension

5.28. The Data Recipient Accreditor may also suspend an accredited data recipient's accreditation where:

a. in the case of an accredited data recipient that is an ADI (including PPF providers and restricted ADIs), the ADI's licence expires or is revoked

b. the Data Recipient Accreditor has reason to believe that the accredited data recipient has or may have contravened a civil penalty provision of the CDR regime, including the privacy safeguards, the Rules, the Standards or a condition of its accreditation (where applicable).

Additional grounds for revocation

5.29. The Data Recipient Accreditor may also revoke an accredited data recipient's accreditation where:

a. the accredited data recipient requests that the Data Recipient Accreditor revoke its accreditation

b. the accredited data recipient has been found to have contravened a civil penalty provision of the CDR regime, including the privacy safeguards, the Rules, the Standards or a condition of its accreditation (where applicable).

Consequences of suspension of accreditation

5.30. A suspended accredited data recipient will:

a. continue to have all the obligations of an accredited data recipient in relation to the CDR data that the accredited data recipient has received and continues to hold

b. be prevented from receiving any further CDR data

c. be required to notify each affected consumer of the fact of their suspension.

5.31. The Data Recipient Accreditor must notify the Accreditation Registrar of the suspension and the Registrar must amend the entry relating to the accredited data recipient in the Register to reflect the suspension.

Consequences of revocation of accreditation

5.32. The revoked accredited data recipient will have all the obligations as set out at paragraph 5.30 and in addition will be required to destroy or de-identify CDR data already received in accordance with paragraph 8.15.

5.33. The Data Recipient Accreditor must notify the Accreditation Registrar of the revocation and the Registrar must amend the entry relating to the accredited data recipient in the Register to reflect the revocation.

Review of decisions to suspend, revoke, or vary accreditation

5.34. As required by section 56BH(4) of the Bill, decisions of the Data Recipient Accreditor to suspend, revoke or vary accreditation will be subject to review by the Administrative Appeals Tribunal.

6. The Register

6.1. The Accreditation Registrar must keep a register (the Register) in electronic format that contains such information as the Accreditation Registrar considers appropriate, provided that the Register identifies all accredited persons and, where different levels of accreditation exist (which will be provided for in a later version of the Rules), the person's level of accreditation.

6.2. The Accreditation Registrar may make amendments to the Register to ensure its accuracy.

6.3. The Accreditation Registrar must amend entries in the Register relating to accredited persons where required to do so by the Data Recipient Accreditor.

6.4. The Accreditation Registrar must amend entries in the Register relating to accredited persons where their accreditations have been revoked, suspended or varied.

7. Consumer consent and authorisation

7.1. An accredited data recipient will be required to obtain a consumer's consent to collect and use that consumer's specified CDR data for a specified purpose, either once or for a specified continuing period of not more than 12 months.

7.2. A data holder will be required to obtain a consumer's authorisation to share that consumer's specified CDR data with an accredited data recipient either once or for a specified continuing period of not more than 12 months.

7.3. The Rules will prescribe the requirements for:

a. valid consent for an accredited data recipient to collect and use CDR data,

b. authorisation for a data holder to share CDR data with an accredited data recipient.

7.4. An accredited data recipient will be prohibited from collecting or using CDR data other than in accordance with the terms on which a consumer has provided consent (see Privacy Safeguard 6 at paragraph 8.8).

7.5. An accredited data recipient will be required to minimise its collection and use of CDR data to the extent that is reasonably necessary to provide the products or services sought by the consumer (the 'data minimisation principle').

Individual authority

7.6. An individual consumer with an individual account may:

a. give consent to an accredited data recipient to collect and use their CDR data, and

b. authorise the data holder to share their CDR data with an accredited data recipient.

Joint authority

7.7. Joint accounts will be in scope in version one of the Rules from 1 February 2020.

7.8. Each consumer who is a joint account holder may:

a. permit another joint account holder to authorise a data holder to share CDR data relating to the joint account with an accredited data recipient, and

b. elect whether, in that circumstance, the data holder must notify any other joint account holders that data from the joint account has been shared.

A notification of this kind will be a notification for the purposes of Privacy Safeguard 10.

Default position

7.9. Where an election in relation to the sharing of CDR data has not been made by joint account holders, the default position for joint accounts, irrespective of any existing non-CDR permissions on the joint account, is that:

a. any consumer who is a joint account holder may give consent for an accredited data recipient to collect and use CDR data relating to the joint account, subject to

b. each consumer who is an account holder on the joint account providing authorisation to the data holder to share CDR data relating to the joint account with an accredited data recipient.

Authorisation for joint accounts may be provided at the account level, rather than for each transaction.

While the approach for joint accounts differs from the proposal in the Rules Framework, the ACCC considers that putting the election in the hands of consumers presents an appropriate balance between the divergent views received from stakeholders on appropriate permissions for joint accounts.

Nature and form of consent

7.10. A consent provided to an accredited data recipient by a consumer for the collection and use of CDR data will not be valid unless it satisfies the requirements of paragraphs 7.11 to 7.14 below, and meets the following requirements:

a. Consent must be voluntary, express, informed, specific as to purpose, time limited and easily withdrawn.

Consent must be voluntary and consistent with the OAIC's Australian Privacy Principles guidelines on voluntary consent. Consent is voluntary if an individual has a genuine opportunity to provide or withhold consent. Consent is not voluntary where duress, coercion or pressure is applied by any party involved in the transaction. Factors relevant to deciding whether consent is voluntary include:

- *the alternatives open to the individual if they choose not to consent*
- *the seriousness of any consequences to the individual if they choose not to consent*
- *any adverse consequences for family members or associates of the individual if the individual chooses not to consent.*

b. An accredited data recipient must not make consent a precondition to obtaining another unrelated product or service. The collection of CDR data must be reasonably necessary or required to provide the service the accredited data recipient is offering.

c. An accredited data recipient must not bundle consent with other directions, permissions, consents or agreements.

d. An accredited data recipient must present each consumer with an active choice to give consent, and consent must not be the result of default settings, pre-selected options, inactivity or silence.

7.11. A request for consent must be presented to a consumer using language and/or visual aids that are concise and easy to understand.

7.12. An accredited data recipient must provide consumers with a straightforward withdrawal of consent process and provide information about that process to each consumer prior to receiving the consumer's consent.

Information to be provided at the consent stage

7.13. Prior to receiving consent from a consumer to collect and use their CDR data an accredited data recipient must provide the consumer with the following information:

a. the name of the accredited data recipient

b. details of the CDR data that will be collected and used pursuant to the consent including the type of CDR data and, where relevant, the period of time covered by the CDR data

c. whether the consent is one-off or continuing and, if continuing, the period over which, and frequency with which, data will be collected pursuant to the consent

d. unambiguous disclosure of the uses to which the CDR data will be put, including the provision of the products or services sought by the consumer

e. notification as to whether the CDR data will or may be shared with an outsourced provider (including one based overseas), with a link to the accredited data recipient's CDR policy so that the consumer can obtain further information if desired

f. when the accredited data recipient's collection and use of the CDR data will expire

g. the period for which the accredited data recipient will hold the CDR data

h. a statement that at any time and without penalty the consumer can withdraw consent to collect and use their CDR data, along with instructions for how the consumer can withdraw consent.

7.14. Information provided by an accredited data recipient to a consumer relating to consent must not cross-reference to other documents, except as expressly provided for by the Rules (e.g. the provision of a link to a CDR policy to provide further information about outsourcing arrangements).

Withdrawing consent

7.15. A consumer may withdraw the consent they have provided to an accredited data recipient to collect and use their CDR data at any time and without detriment.

7.16. The process for the withdrawal of consent must be:

a. simple and straightforward

b. no more complex than the process to provide consent

c. able to be withdrawn via the consumer dashboard of the accredited data recipient.

7.17. An accredited data recipient must notify the relevant data holder when a consumer withdraws consent. Upon receipt by the data holder of notification from the accredited data recipient, the consumer's authorisation to the data holder to share CDR data will be taken to be withdrawn.

7.18. Withdrawal of consent by a consumer to collect and use data will have the consequence that the CDR data becomes redundant data for the purposes of Privacy Safeguard 12 (see further paragraph 8.15 below).

Management of consents

7.19. An accredited data recipient must provide a consumer-facing electronic dashboard that provides details of the consumer's current and historic consents including:

a. when consent was obtained

b. whether the consent was one-off or continuing and, if continuing, the period over which, and frequency with which, data will be received pursuant to the consent

c. details of the CDR data which the consumer has provided consent to be collected and used by the accredited data recipient

d. the uses for which consent has been provided, including the provision of the products or services sought by the consumer

e. when the accredited data recipient's consent to collect the data will expire

f. whether any consents have been withdrawn and, if so, when.

This requirement to provide specified information in a dashboard is considered a notification for the purpose of Privacy Safeguard 5.

The extent to which the Rules will impose requirements regarding the management of consent generally, beyond the requirement to provide a consumer dashboard and allow consumers to withdraw consent, will be determined in consultation with the Data Standards Body.

Nature and form of authorisation

7.20. Prior to receiving an authorisation from a consumer to share their CDR data with an accredited data recipient the data holder will be required to:

a. provide the consumer with information that mirrors the relevant information provided to the data holder in the request sent by the accredited data recipient, including:

i. the name of the accredited data recipient that requested the CDR data

ii. details of the CDR data that has been requested including the type of CDR data and, where relevant, the period of time covered by the CDR data

iii. whether the request is one-off or continuing and, if continuing, how frequently CDR data will be shared/collected

iv. for continuing collection, the period for which the data has been requested

v. when the accredited data recipient's consent to collect the CDR data will expire

b. provide the consumer with a statement that the consumer can withdraw authorisation at any time and without detriment along with instructions for how the consumer can do so.

Withdrawing authorisation

7.21. A consumer may withdraw the authorisation they have provided to a data holder to share their CDR data with an accredited data recipient at any time and without detriment.

7.22. The process for withdrawal of authorisation must be:

a. simple and straightforward

b. no more complex than the process to authorise

c. able to be withdrawn via the consumer dashboard of the data holder.

7.23. A data holder must notify the relevant accredited data recipient when a consumer withdraws authorisation. Upon receipt by the accredited data recipient of notification from the data holder, the consumer's consent to the accredited data recipient to collect and use CDR data will be taken to be withdrawn.

Management of authorisations

7.24. Data holders must provide a consumer-facing electronic dashboard that provides details of the consumer's current and historic authorisations including:

a. which CDR datasets the consumer has authorised to be shared

b. when authorisation was provided

c. the accredited data recipient with whom the CDR data has been shared

d. the period over which authorisation was provided for

e. whether any authorisations have been withdrawn and, if so, when.

Duration of consent and authorisation

7.25. Consent and authorisation will automatically expire after 12 months.

This represents an increase from the 90-day duration proposed in the Rules Framework. The decision to extend the period was made on the balance of stakeholder submissions, many of which noted the need for a longer duration to support important use cases, and on the basis of adding a requirement to remind consumers of continuing data sharing arrangements.

7.26. Accredited data recipients must remind consumers every 90 days that an ongoing data sharing arrangement is in place.

This proposal was not canvassed in the Rules Framework but was suggested by stakeholders.

7.27. The Standards may provide for a simplified process for the renewal of consent/authorisation.

Authorisation standards

7.28. The Data Standards Chair must make a standard relating to authorisation and authorisation flows.

7.29. The authorisation Standards must:

a. be subject to consumer testing and may contain service level requirements

b. provide for multi-factor authentication requirements consistent with the requirement for strong customer authentication under the revised Payment Services Directive (EU) (PSD2) and the European regulatory technical standard for strong consumer authentication under PSD2 regulatory technical standards (RTS)

c. provide for the ability for a consumer to grant authorisation for a specific, once-off request, or authorisation that continues over time

d. specify permissions for applications to access CDR data.

7.30. A data holder will be prohibited from:

a. adding any requirements to the authorisation process beyond those specified in the Standards,

b. requesting additional information from the consumer during the authorisation process beyond that specified in the Standards, or

c. offer additional or alternative services to the consumer.

Service level standards/non-functional requirements

7.31. The Rules will specify non-functional or service level requirements to be complied with by data holders (for example, in relation to API performance and availability) and will authorise the Standards to specify additional requirements.

The ACCC and Data61 are working closely on the development of non-functional requirements.

8. Rules relating to the Privacy Safeguards (including use of CDR data)

Rules are not required or contemplated for the operation of Privacy Safeguards 3, 4 and 9. Privacy Safeguard 8 is not included in the Rules Outline because the ACCC does not intend to make rules to expand the circumstances in which an accredited data recipient may disclose CDR data overseas.

Privacy safeguard 1: open and transparent management of data

8.1. Data holders and accredited data recipients must have a separate CDR policy which is independent of any existing privacy policy and which is easy to understand and drafted in a way that promotes consumer engagement.

8.2. The policy must be provided to a consumer, where requested, in accordance with the following requirements:

a. made available free of charge (as required by the Bill)

b. made available on a data holder or accredited data recipient's website and mobile app in a readily accessible location

c. made available electronically or in hard copy, depending on the consumer's wishes.

8.3. Privacy Safeguard 1 sets out the minimum requirements for the CDR policy to be kept by data holders and accredited data recipients.

8.4. For accredited data recipients, the requirements in section 56EF(5) of the Bill will be supplemented by the Rules and will require that the policy:

a. include a list of outsourced service providers, the nature of their services and the CDR data that has been disclosed to them

b. include a list of overseas recipients to whom CDR data may be disclosed, the classes of CDR data that may be disclosed to them and the uses of that CDR data by those recipients.

Privacy safeguard 2: anonymity and pseudonymity

8.5. As required by section 56EE of the Bill, accredited data recipients must give consumers the option of dealing with them anonymously or by pseudonym.

8.6. The ACCC intends to make rules for the purposes of Privacy Safeguard 2 that will be based on Australian Privacy Principle 2, such that the option of dealing anonymously or by pseudonym will apply except where:

a. the accredited data recipient is required or authorised by law or a court or tribunal order to deal with identified individuals, or

b. it is impracticable for the accredited data recipient to deal with individuals who have not identified themselves.

Privacy safeguard 5: notifying the collection of CDR data

8.7. If an accredited data recipient collects CDR data in accordance with Privacy Safeguard 3, then the accredited data recipient must comply with the notification requirements specified in the Rules. The notification rules for the purposes of Privacy Safeguard 3 will be the requirement for the accredited data recipient to record the collection in the consumer dashboard (see paragraph 7.19 above).

Privacy safeguard 6: use or disclosure of the CDR data

8.8. For the purposes of Privacy Safeguard 6, the Rules:

a. will authorise an accredited data recipient to use CDR data for the purposes for which the consumer has provided valid consent in accordance with the Rules.

b. will authorise an accredited data recipient to disclose CDR data to another accredited data recipient in response to a request by a consumer

c. will authorise an accredited data recipient to disclose CDR data to an outsourced service provider of the accredited data recipient. The accredited data recipient will be required to take reasonable steps to ensure that outsourced providers perform services relating to CDR data in accordance with the accredited data recipient's obligations under the CDR. The accredited data recipient will continue to be responsible for compliance with the Bill and rules in relation to the CDR data notwithstanding any outsourcing arrangements. Acts or omissions of an outsourced provider in relation to the CDR will be taken to be acts or omissions of the accredited data recipient. Information about disclosure to outsourced providers must be set out in the accredited data recipient's CDR policy (see Privacy Safeguard 1 above)

d. will not require or authorise an accredited data recipient to disclose CDR data to a non-accredited recipient at the direction of the consumer

The ACCC does not propose to include sharing of CDR data with a non-accredited entity in version one of the Rules. This is in light of concerns from stakeholders that transfer of CDR data to a non-accredited entity risks undermining the consumer protection that the accreditation process is designed to provide. The ability for consumers to direct the sharing of CDR data to certain non-accredited entities (including professional advisors such as accountants and lawyers) will be considered for inclusion in the next version of the Rules.

e. will not authorise an accredited data recipient to on-sell CDR data

f. will not authorise an accredited data recipient to aggregate CDR data to ascertain the identity of 'silent' parties.

'Silent parties' are parties about which data may be disclosed notwithstanding that they are not the consumer who has consented to the collection and use of their data, nor have they authorised the sharing of their CDR data which contains this information. For example, information such as BSB numbers, names, and account numbers may be disclosed as part of a consumer's payee list.

Privacy safeguard 7: use or disclosure of CDR data for direct marketing

8.9. An accredited data recipient will be prohibited from using CDR data for the direct marketing of products or services unrelated to the product or service a consumer has consented to the collection and use of their CDR data for.

This prohibition is not intended to prevent an accredited data recipient from providing a service the consumer has specifically consented to receiving (for example, a comparison service that gives a consumer tailored quotes for better products or services), including an improved version of that service.

Privacy safeguard 10: notifying the disclosure of CDR data

8.10. The notification rules for the purposes of Privacy Safeguard 10 (which apply to data holders and accredited data recipients) will be the requirement for a data holder or an accredited data recipient to record the disclosure of CDR data in their consumer dashboard (see paragraphs 7.19 and 7.24 above). These rules will also require data holders to notify joint account holders that data from a joint account has been shared where an election to this effect has been made by the joint account holders (see paragraph 7.8 above).

Privacy safeguard 11: quality of CDR data

8.11. Where a data holder shares CDR data as required or authorised by the Rules, the data holder must ensure that the CDR data is accurate, up-to-date and complete for the purpose for which it is held.

8.12. Similarly, an accredited data recipient must ensure that any CDR data it shares consistent with the Rules is accurate, up-to-date and complete for the purpose for which it is held.

8.13. Where a data holder or accredited data recipient becomes aware that the CDR data that was disclosed was incorrect, the data holder or accredited data recipient must notify the consumer as soon as practicable upon discovery and, in any event, no later than within 24 hours from the time of discovery that the disclosed data was incorrect.

Privacy safeguard 12: security of CDR data

8.14. The steps that accredited data recipients must take to protect CDR data from misuse, interference, loss, unauthorised access, modification or disclosure are outlined in Schedule 2.

8.15. If CDR data becomes redundant data (as specified in that clause)[4], an accredited data recipient must ensure that the redundant CDR data is either destroyed or de-identified and apply the OAIC and Data61's 'De-identification Decision-making Framework' in determining which treatment is appropriate in the circumstances.

The De-identification Decision-making Framework is a practical guide to de-identification for government agencies and businesses including not-for-profit and private sector organisations and will assist accredited data recipients to identify and address the key factors relevant to their particular CDR data sharing or release situation, including privacy risk analysis and control, stakeholder engagement, and impact management.

Privacy safeguard 13: correction of CDR data

8.16. The steps to be taken by data holders and accredited data recipients will be based on the steps outlined by the OAIC in relation to Australian Privacy Principle 13, but adapted to apply to CDR data rather than personal information as is the case under Australian Privacy Principle 13. This will include the requirement to respond to a request to correct a record or to associate a statement within 30 calendar days.

9. Record-keeping, reporting, and audit power

Record keeping and reporting

The scope and form of record-keeping and reporting obligations for data holders and accredited data recipients will be determined in consultation with the Data Standards Body, with consideration also given to the development of non-functional requirements/service level standards. These obligations may be included in the Rules or the Standards or both.

Data holders

9.1. Data holders must collect and maintain records of complaints and disputes and report this to the ACCC and OAIC on a biannual basis.

9.2. Data holders must maintain records relating to:

a. the valid requests received by consumers to share CDR data either with the consumer directly or with an accredited data recipient

b. withdrawal of authorisations by consumers

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

[4] Privacy Safeguard 12 provides that data becomes redundant if the accredited data recipient no longer needs some or all of the CDR data for the purposes permitted under the Rules or for any purpose for which the accredited data recipient is able to disclose any of that data and the accredited data recipient is not required by or under Australian law, or a Court or Tribunal order, to retain that data.

9.3. Data holders must provide a consumer with a copy of the records relating to their requests to share CDR data (including records relating to authorisation) and any disclosures made in response to such requests on request by the consumer.

9.4. Data holders must retain the records described above for 6 years.

Accredited data recipients

9.5. Accredited data recipients must collect and maintain records of complaints and disputes and report this to the ACCC and OAIC on a biannual basis. Accredited data recipients will also need to provide information about any additional services that they offer to consumers using CDR data, or material changes to the services that were described in the accreditation application.

9.6. Accredited data recipients must maintain records relating to:

a. consents to collect and use CDR data provided by consumers

b. withdrawals of consent by consumers

c. notification of withdrawals of authorisation received from data holders

d. any outsourcing arrangements which will or may result in sharing CDR data with outsourced providers and the use of CDR data by those providers.

9.7. An accredited data recipient must provide a consumer with a copy of the records relating to their consent and any disclosures made in response to such requests on request by the consumer.

9.8. Accredited data recipients must retain the records described above for 6 years.

Audit power

9.9. The ACCC and OAIC will be able to conduct audits on accredited data recipients relating to compliance with the Bill, Rules and Standards including to produce any records required to be kept under the Bill, Rules and Standards.

9.10. Similar to the power under section 51ADD of the CCA, the ACCC and OAIC will have the power to issue written notices requiring production of records that the Rules require to be created and kept by data holders and accredited data recipients.

10. Dispute resolution

Internal dispute resolution

10.1. Data holders and accredited data recipients will be required to have in place internal dispute resolution procedures that meet requirements that will be broadly similar to those set out in ASIC's Regulatory Guide 165 (or any replacement Regulatory Guide), adapted for the CDR. These requirements may be specified in a schedule to the Rules, or in a separate written instrument, which will also reflect the role of the OAIC in investigating, conciliating and resolving complaints involving individuals.

External dispute resolution

10.2. Data holders and accredited data recipients must be a member of the external dispute resolution scheme recognised by the ACCC for the banking sector. The ACCC intends to recognise AFCA as the EDR scheme for the banking sector.

10.3. Version one of the Rules will not require data holders and accredited data recipients to resolve disputes involving larger businesses or between CDR participants by alternative dispute resolution. This may be provided for in a subsequent version of the Rules.

11. Data Standards Body

The Data Standards Chair and DSAC

11.1. The Data Standards Chair must establish and maintain a DSAC. The DSAC may have more than one sub-committee.

11.2. The DSAC must include at least one consumer representative and at least one privacy representative as members.

11.3. The ACCC, the OAIC, and the Commonwealth Treasury may elect to be observer members of the DSAC.

The Standards setting process

11.4. The Data Standards Chair must undertake public consultation on draft Standards. The consultation process will only be required for new Standards and substantive or major changes to existing Standards. The consultation process will not be required for urgent, routine or minor changes to the Standards.

11.5. The Data Standards Chair will determine the consultation period for each draft Standard.

11.6. The draft Standards must be made publically available on the website of the Data Standards Body.

11.7. The Data Standards Chair must have regard to the following matters in making the standards:

a. Submissions received from stakeholders during the consultation period.

b. The advice of the DSAC.

c. Any advice from other committees, advisory panels, or consultative groups that the Data Standards Chair may have established.

d. The principles applying to the development of the Standards.

11.8. The Data Standards Chair must review the operation of a Standard where directed to do so by the ACCC.

Principles guiding the development of the Standards

Security - ensuring the privacy, security, and accountability of all participants and, in particular, the privacy and security of CDR data.

Openness - ensuring accessibility for all interested parties across a wide range of participants, thereby incentivising adoption, distribution, and participation.

Usability - facilitating ease of implementation and a smooth user experience for consumers.

Interoperability - promoting and progressing towards an environment where CDR data can be exchanged between parties in a frictionless manner across organisational and technological boundaries.

Re-use - adopting and leveraging existing standards, taxonomies, and CDR data lists where possible and practicable to avoid duplicative efforts and to maximise interoperability.

Independence - promoting competition among, and avoiding dependencies on, vendor solutions and technologies; preserving optionality in delivery models and implementation technologies.

Extensibility - establishing flexibility and encouraging adoptees to build upon the standard and innovate locally, while providing governance mechanisms to subsequently bring extensions 'back to the core'.

Stability - providing a stable environment for all participants where change is communicated, actioned, and governed in a transparent and consistent manner.

Transparency - providing visibility and clarity on issues pertaining to the standard and the environment it operates in (for instance its design, specifications, and governance).

Schedule 1
Data sets map

Note

- This table is for illustrative purposes only and should not be taken as a definitive statement of the data sets for the CDR.
- Some categories of payloads do not align precisely with the draft Designation Instrument and may be captured under multiple limbs. For example, some 'account data' is within what the Designation Instrument refers to as 'information about the user of the product'.

Designation instrument	Rules	Standards – Authorisation scopes	Standards – APIs	Payloads
Information about user of product	'**Customer data'** is data that identifies the customer and any persons authorised to act on the consumer's account and will include, at a minimum: - the customer's name, which may include a business name and number(s) (such as ABN, ACN) - the customer's contact details, which may include phone numbers, email addresses, and physical addresses. Customer data may include other identifying information, including where that information assists to distinguish one customer from another. Customer data does not include the date of birth of an individual. In relation to business customers, customer	Basic Customer data	Get Customer*	Customer type (e.g. person or organisation) *Person*: last update time, first name, last name, middle names, prefix, suffix, occupation code, *Organisation*: last update time, agent first name, agent last name, agent role, business name, legal name, short name, ABN, ACN, industry code, organisation type (e.g. 'sole trader'), registered country, establishment date
		Detailed Customer Data	Get Customer Detail*	Customer type (e.g. person or organisation), *Person*: last update time, first name, last name, middle names, prefix, suffix, occupation code,

Designation instrument	Rules	Standards – Authorisation scopes	Standards – APIs	Payloads
	data may include the type of business, establishment date, registration date, organisation type, country of registration and whether the business is a charitable/non-profit organisation. Customer data also includes information the customer provided at the time of opening the account that relates to the customer's eligibility for to acquire the product (that is, in connection with an application process). However this information will not be required to be shared via an API and must be shared directly with the consumer in response to the consumer's valid request.			*Organisation*: last update time, agent first name, agent last name, agent role, business name, legal name, short name, ABN, ACN, industry code, organisation type (e.g. 'sole trader'), registered country, establishment date Phone numbers (purpose and preferred number), Email addresses (purpose and preferred email), Physical address (mailing name and purpose).
Information about use of the product	'**Account data'** includes, at a minimum: - information identifying the account, including the account number, and account name(s) o credit card account numbers must be treated in accordance with any applicable laws, obligations and/or standards, which may include masking credit card numbers to meet security requirements - the opening and closing balances for the account, including as current	Basic Bank Account	Get Accounts	Account ID, display name, nickname, masked number (BSB/ACC, CC number, PAN) Product: category, type, name
			Get Bulk Balances	Account IDs, Balance: type (e.g. 'deposits'), amount (current and available), currency
			Get Balances For Specific Accounts	Account IDs, Balance: type (e.g. 'deposits'), amount (current and available), currency

Designation instrument	Rules	Standards – Authorisation scopes	Standards – APIs	Payloads
	balance and available funds o a running balance may be shared by the data holder, but is not a mandatory inclusion - authorisations on the account, including: o direct debit deductions, which will include, to the extent available: ▪ identifying information for the merchant/party making the debit ▪ the amount debited ▪ the date of the transaction o scheduled payments, which may include regular payments, payments to billers, international payments o details of payees stored with the account, such as if entered by the customer in a payee address book. The ACCC recognises the limitations in providing direct debit information, hence the information is to be provided to the extent		Get Payees	PayeeID, nickname, description, type (e.g. domestic, international biller)
		Detailed Bank Account	Get Account Detail	Account ID, display name, nickname, account number (BSB/ACC, CC number, PAN) Product: category, type Balance: type (e.g. 'deposits'), amount (current and available), currency Features (type and information) Fees: name, type, amount, Discounts: description, type, amount, conditions Deposit rate, lending rate, address, bundle details (i.e. details of other linked accounts)
			Get Direct Debits For Account	Direct debit authorisations: account ID, authorised entity (name, financial institution, ABN, ACN), last debit date and time, last debit amount
			Get Bulk Direct Debits	List of direct debit authorisations

Designation instrument	Rules	Standards – Authorisation scopes	Standards – APIs	Payloads
	available. The ACCC expects though that as more information becomes available, and better processes develop, over time in relation to direct debits, it will be able to be included.			Direct debit authorisations: account ID, authorised entity (name, financial institution, ABN, ACN), last debit date and time, last debit amount
			Get Direct Debits For Specific Accounts	Account ID Authorised entity information [Name, Financial institution, ABN, CAN, Last debit time, Last debit amount]
		Bank Payee	Get Payee Detail	PayeeID, nickname, description, type (domestic, international, biller) *Domestic*: account (name, BSB, account number), Card (card number), PayID (name, identifier, type-mobile, email, organisation name) *International*: (beneficiary name/country/message, bank country/account number/address/name, Beneficiary Bank BIC/fed wire number/sort code/ chip number/ routing number) *Biller*: code, name
	'**Transaction data**' includes, at a minimum:	Bank Transactions Data	Get Transactions For Account	Account ID, display name, nickname, list of transactions

Designation instrument	Rules	Standards – Authorisation scopes	Standards – APIs	Payloads

	- the date on which the transaction occurred
	- the relevant identifier for the counter-party to a transaction
	  o where the counter-party is a merchant, this will include information the merchant has provided as a mandatory inclusion, and any additional merchant identifiers the data holder may have added as an optional inclusion
	- the amount debited or credited pursuant to a transaction
	- any description of the transaction
	- the 'simple categorisation' of the transaction (e.g., whether the transaction is debit, credit, fee, interest etc.)
	  o any additional, descriptive categorisation of the transaction added by the data holder (e.g., 'transport', 'health', 'entertainment' etc.) is not a mandatory inclusion but may be included.
				(transaction ID, status, description, post time, execution time, amount, currency], reference number from merchant)

			Get Transaction Detail	Account ID, display name, nickname, list of transactions (transaction ID, status, description, post time, execution time, amount, currency, reference number from merchant), payer, payee, extended description
			Get Bulk Transactions	Account ID, list of transactions (transaction ID, status, description, post time, execution time, amount, currency, reference number from merchant),
			Get Transactions For Specific Accounts	Account ID, transactions (transaction ID, status, description, post time, execution time, amount, currency, reference number from merchant),

Designation instrument	Rules	Standards – Authorisation scopes	Standards – APIs	Payloads
Information about a product	'**Product data**' includes product reference (generic) data, which includes, at a minimum, data on: - product type - product name - product prices, including fees, charges, interest rates etc (however described) - features and benefits, including discounts, bundles etc (however described) - terms and conditions - customer eligibility requirements.	Public data	Get Products	Products ID, effective from and to, last updated, product category, product name, description, brand, application URI, overview URI, terms URI, eligibility URI, fees and pricing URI, bundle URI
			Get Product Detail	Products ID, effective from and to, last updated, product category, product name, description, brand, application URI, overview URI, Eligibility (eligibility URI, type and additional information) Fees and Pricing (fees and pricing URI, name, type, amount, balance rate, transaction rate, currency, additional info, discounts) Bundle (bundle URI, name, description, additional information URI, product IDs) Features (type and additional information) Constraints (type and additional information) Deposit rate (type, additional info)

Designation instrument	Rules	Standards – Authorisation scopes	Standards – APIs	Payloads
				Lending rates (type additional info) Repayment type (interest only, principal and interest, negotiable)
	'**Product data**' includes consumer product data, that is product data that relates to an account(s) held by a consumer and includes, at a minimum, data on: - product type - product name - product prices, including fees, charges, interest rates etc (however described) o interest rates will include the current applicable interest rate, as well as any other interest rates applicable to the product, and any terms and conditions associated with those interest rates o these will include details of any prices etc negotiated individually with the consumer - features and benefits, including	Detailed Bank Account	Get Account Detail	Account ID, display name, nickname, masked number (BSB/ACC, CC number, PAN), product category, product type (term deposit, credit card, loan), bundle name, balance type, balance, features, fees (name, type, amount, balance rate, transaction rate, currency, additional information, discounts), discounts (description, type, amount, additional info), deposit rate, lending rate, address, bundle details (i.e. details of other linked accounts)

Designation instrument	Rules	Standards – Authorisation scopes	Standards – APIs	Payloads
	discounts, bundles etc (however described), including details of any features and benefits negotiated with the customer - terms and conditions - customer eligibility requirements.			

Schedule 2
CDR information security requirements for accreditation and continuing obligations

Applicants for accreditation will need to provide evidence to the Data Recipient Accreditor, in the form of an independent audit, that they meet the rules set out in Part I including the mandatory controls set out in Part II below.

Part I: Information security rules

Privacy Safeguard 12 requires an accredited data recipient (ADR) to take the steps specified in the Rules to protect CDR data from misuse, interference and loss, and unauthorised access, modification or disclosure. For the purposes of Privacy Safeguard 12, the Rules will require that an ADR have practices, procedures, and systems in place to manage CDR data and information security risks that meet the requirements specified below.

The objective of this section is to set out appropriate high level principles for the overall governance of an ADR's CDR data framework. The draft rules included here have been broadly based on sections of APRA's *Prudential Standard CPS 234 Information Security* (CPS 234). Noting that CPS 234 has been developed with different objectives, these principles may be further developed to give greater focus on the information security of an ADR's CDR data.

Roles and responsibilities

1. The ADR (or the Board of an ADR in the case of an ADR that is a body corporate) is ultimately responsible for the management of CDR data and the information security of the ADR.
2. An ADR must clearly define the information security-related roles and responsibilities of the Board, senior management, governing bodies, and individuals with responsibility for decision-making, approval, oversight, operations, and other information security functions related to the management of CDR data[5] by the ADR and any outsourced third party providers, where they have access to the ADR's CDR data.

Information security capability

3. An ADR must maintain an information security capability commensurate with the size and extent of threats to the CDR data that the ADR manages.
4. Where CDR data is disclosed to and/or managed by an outsourced third party provider (including a cloud provider), the ADR must take reasonable steps to ensure that the third party will manage the CDR data in accordance with the ADR's obligations under the Bill and Rules.
    a. Reasonable steps will include assessing whether the information security capability of the outsourced third party provider, having regard to the nature of the services provided in relation to CDR data and the potential consequences

[5] These individuals will be 'senior managers' for the purposes of the fit and proper person criterion for accreditation.

of an information security incident affecting that CDR data, complies with the ADR's obligations under the Rules.

b. An ADR may assess information security capability of the outsourced third party provider by defining processes that allow the ADR to request information such as internal audit reports and other information security assessments and questionnaires, from the third party. The ADR may also define processes to monitor the outsourced third party provider and take appropriate action where such monitoring highlights information security risks.

5. An ADR must actively maintain processes that allow it to monitor changes in vulnerabilities and threats to its information-processing environment, including those resulting from changes to information assets or its business environment. Additionally, an ADR must maintain processes that allow its information security capability[6] to be updated in response to these changes, in a timely manner.

Information security policy

6. An ADR must establish an information security governance framework which includes the ADR's information security leadership arrangements (such as through committees), structured roles and responsibilities for managing information security risks, and processes designed to protect information processing assets. The ADR's information security governance framework should clearly articulate how risk posture is assessed and how the ADR's information security processes and controls help to mitigate those risks.
7. As part of the overall information security governance framework, an ADR must maintain an information security policy commensurate with the sensitivity of the CDR data that it manages, its exposure to vulnerabilities and threats to CDR data, and its general business environment.
8. An ADR's information security policy must provide direction on the responsibilities of all parties who have an obligation to maintain information security relating to the CDR data the ADR manages.

Information asset identification and classification

9. An ADR must define and maintain appropriate processes for identification and classification of its information assets, giving due consideration to criticality and sensitivity of these assets. Such a classification scheme must be applied by an ADR to the CDR data that it manages, including CDR data managed by outsourced third parties providers (including cloud providers). This classification must reflect the degree to which an information security incident has the potential to affect the security of that CDR data.

Implementation of controls

10. An ADR must have information security controls in place to protect CDR data, including CDR data managed by outsourced third parties providers (including cloud providers), that are implemented in a timely manner and are commensurate with:
    a. vulnerabilities and threats to the CDR data
    b. the criticality and sensitivity of the CDR data
    c. the stage at which the information assets are within their life-cycle, and

[6] The information security capability of an ADR is a combination of frameworks, governance structures, documentation hierarchy (policies, procedures, and standards) and controls, which allow the ADR to prevent, detect, monitor and/or correct information security risks to its information processing environment (and information assets).

d. the potential consequences to the CDR data of an information security incident.

11. An ADR must meet, at a minimum, the controls specified in Part II below.
12. Where an ADR's CDR data is managed by an outsourced third party provider (including a cloud provider), the ADR must evaluate the design and implementation of that party's information security system, and associated controls, that protects the CDR data of the ADR.

Testing control effectiveness

13. An ADR must test the design and implementation, and operating effectiveness of its information security controls through a systematic testing program. The nature and frequency of the systematic testing must be commensurate with:
    a. the rate at which the vulnerabilities and threats change
    b. the criticality and sensitivity of the CDR data held
    c. the consequences of an information security incident
    d. the risks associated with exposure to environments where the ADR is unable to enforce its information security policies, and
    e. the materiality and frequency of change to information assets.
14. Where an ADR's CDR data is managed by an outsourced third party provider (including a cloud provider), and the ADR is reliant on that third party's information security control testing, the ADR must assess whether the nature and frequency of testing of controls in respect of those information assets is commensurate with paragraphs (a) to (e) above.
15. An ADR must escalate and report to the Board or senior management any testing results that identify information security control deficiencies that cannot be remediated in a timely manner.
16. An ADR must ensure that testing is conducted by appropriately skilled and functionally independent specialists.
17. An ADR must review the sufficiency of its testing program at least annually or when there is a material change to information assets or the business environment.

Incident management

18. An ADR must have robust mechanisms in place to detect, record, and respond to information security incidents in a timely manner.
19. An ADR must maintain plans to respond to information security incidents that the entity considers could plausibly occur (CDR data security response plans).
20. An ADR's CDR data security response plans must include mechanisms for:
    a. managing all relevant stages of an incident, from detection to post-incident review, and
    b. escalation and reporting of information security incidents to the Board, other governing bodies, individuals responsible for information security incident management and oversight, as appropriate, and external parties, in line with legislative reporting obligations
21. An ADR must annually review and test its information security response plans to ensure they remain effective and fit-for-purpose.

PART II: information security controls

Listed below are the key information security controls that have been identified as critical and mandatory for an ADR's information security capability to adequately protect CDR data. These controls are adapted from the Australian Cyber Security Centre's 'Strategies to Mitigate Cyber Security Incidents' and the Australian Government's Information Security Manual.[7]

Application whitelisting

An ADR must implement application whitelisting of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.

Patch applications

An ADR must patch applications such as Flash, web browsers, Microsoft Office, Java and PDF viewers, and patch/mitigate computers with "extreme risk" vulnerabilities within 48 hours. ADRs must use the latest version of applications.

Configure Microsoft Office macro settings

An ADR must configure Microsoft Office macro settings to block macros from the Internet, and only allow vetted macros either in "trusted locations" with limited write access or digitally signed with a trusted certificate.

User application hardening

An ADR must configure web browsers to block Flash (ideally uninstall it), ads, and Java on the Internet. An ADR must disable unneeded features in Microsoft Office (e.g. OLE), web browsers, and PDF viewers.

Patching operating systems

An ADR must path/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours and use the latest operating version. ADRs must not use unsupported versions.

Restrict administrative privileges

An ADR must restrict administrative privileges to operating systems and applications based on user duties, regularly revalidate the need for privileges, and not use privileged accounts for reading email and web browsing.

Multi-factor authentication

An ADR must use multi-factor authentication including for VPNs, RDP, SSH, and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository.

---

[7] For further information, see https://acsc.gov.au/infosec/mitigationstrategies.htm.

Daily backups

An ADR must perform daily backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months, and test restoration initially, annually, and whenever IT infrastructure changes.

Cyber security awareness raising and training

An ADR must provide ongoing cyber security awareness raising and training to personnel that includes:

- the purpose of the awareness raising and training program
- security appointments and contacts within the organisation
- the use and protection of systems, applications, media and information
- reporting of cyber security incidents and suspected compromises
- not to introduce or use unauthorised ICT equipment, media, or applications with systems
- not to attempt to bypass, strain, or test security controls on systems
- not to attempt to gain unauthorised access to systems, applications, or information

Data loss prevention

An ADR must implement data loss and leakage prevention mechanisms over data in egress through web and email that include:

- Blocking access to unapproved cloud computing services such as file storage
- Logging the recipient, file size and frequency of outbound emails
- Blocking outbound emails with sensitive words or data patterns
- Limiting the total size of outbound emails
- Block data write access to portable storage media on organisation computers

Access security

An ADR must implement access security controls over systems that host, store or present data including at the application, database and operating system layer, in order to prevent inappropriate access to systems and data. In doing this, an ADR must implement formal processes for the following:

- Provision and timely revocation of user access
- Regular monitoring and review of the appropriateness of user access privileges, especially for transferred users whose roles change
- Sufficiently strong password security, complexity and lockout parameters

Limit physical access to premises and ICT equipment and media

An ADR must restrict physical access to its facilities where data is stored, hosted or accessed including server rooms, communications rooms, security containers, and premises of business operation, to prevent unauthorised access to or disclosure of data.