AUSTRALIAN COMPETITION
& CONSUMER COMMISSION

Consumer Data Right Rules Framework

September 2018

Australian Competition and Consumer Commission
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

Opportunity for comment on the rules framework

You are invited to examine this rules framework and comment on it by written submission to the ACCC. Submissions are due by **5 pm 12 October 2018** and can be lodged on the ACCC's Consultation Hub.

The ACCC seeks comments on the content of the proposed rules, including whether rules are required relating to issues not canvassed in the rules framework. The ACCC notes that this document sets out an initial approach to the rules, and that the views expressed may be revised, including in light of submissions received.

To foster an informed and consultative process, all submissions will be considered as public submissions and will be posted on the ACCC's website. If interested parties wish to submit commercial-in-confidence material, they should submit both a public version and a commercial-in-confidence version of their submission. Any commercial-in-confidence material should be clearly identified, and the public version of the submissions should identify where commercial-in-confidence material has been removed. Parties will be required to provide reasons in support of any claims of confidentiality.

Further information on the process parties should follow when submitting confidential information to the ACCC can be found in the ACCC/AER Information Policy which sets out our general policy on the collection, use and disclosure of information. A copy of the policy is available on the ACCC's website.

Draft rules will be prepared after submissions have been received and are expected to be published in December 2018.

Key dates

12 October 2018	Closing date for submissions on rules framework
Expected December 2018	Publication of draft rules
Following commencement of legislation	Finalisation of rules

Further information about the ACCC's consumer data right role can be found at www.accc.gov.au/consumerdataright. Questions or queries can be directed to ACCC-CDR@accc.gov.au.

For queries about the consumer data right legislation and amendments, please visit https://treasury.gov.au/consumer-data-right/ or contact the Treasury at data@treasury.gov.au.

Table of contents

Part A – Introduction

The consumer data right regime

In the 2017-18 Budget, the Australian Government announced that it would introduce an open banking regime in Australia.[1] In mid-2017, the government commissioned an independent review to recommend the best approach to implement the Open Banking regime (Open Banking review). This review released its final report, *Review into Open Banking: giving customers choice, convenience and confidence*, in December 2017. The government released its response to the Open Banking review on 9 May 2018, confirming the introduction of a consumer data right (CDR) and the regulatory framework for its implementation.[2] The objectives of the CDR are as follows:

> *The Consumer Data Right (CDR) will provide individuals and businesses with a right to efficiently and conveniently access specified data in relation to them held by businesses; and to authorise secure access to this data by trusted and accredited third parties. The CDR will also require businesses to provide public access to information on specified products they have on offer. CDR is designed to give customers more control over their information leading, for example to more choice in where they take their business, or more convenience in managing their money and services.*[3]

The legislative framework

The legislative framework for the CDR will be set out in the *Competition and Consumer Act 2010* (Cth) (CCA) through the *Treasury Laws Amendment (Consumer Data Right) Bill 2018*. The government released an exposure draft of this legislation on 14 August 2018 and it is available at the Treasury's website (draft legislation).[4] The government has also issued an exposure draft explanatory materials for the legislation, available at the same website.

Under the legislative framework, the Australian Competition and Consumer Commission (ACCC) has a role to determine rules that will govern the application of the CDR, both in particular sectors and across the economy more generally. The legislative framework also provides that technical standards dealing with matters such as data format, transfer and security will be developed by a Data Standards Body. The interim Data Standards Body, CSIRO's Data 61, is in the process of developing these standards.

The government has announced that banking will be the first sector brought within the CDR. This will be achieved by specifying the data holders and data sets to which the CDR applies by a designation instrument. The ACCC understands that a draft designation instrument will be released for consultation in September 2018.

While the various instruments giving effect to the CDR and applying it to the banking sector are under development, it will be necessary to keep under review whether issues proposed to be addressed by the ACCC rules will be more appropriately dealt with in the legislation, the designation instrument, or the standards.

---

1 Media release by the Hon Scott Morrison, then Treasurer, *Building an accountable and competitive banking system*, 9 May 2017, available at http://sjm.ministers.treasury.gov.au/media-release/044-2017/.
2 Consumer Data Right Booklet, available at https://treasury.gov.au/consumer-data-right/.
3 Draft explanatory materials, paragraph 1.1.
4 Available at https://treasury.gov.au/consultation/c2018-t316972/.

Aim of this framework

The government has outlined a timeframe for the implementation of Open Banking, with the expectation that the regime will operate in relation to the first tranche of banking products from 1 July 2019. Meeting this timeframe requires that a number of processes are run in parallel, including the drafting of legislation, the development of the rules, the development of technical standards by the Data Standards Body, and the building, testing and implementation of systems by industry stakeholders. The compressed timeframe has influenced the approach the ACCC has taken in developing this rules framework.

The aim of this rules framework is to outline, as far as possible, the approach and substantive positions the ACCC proposes to take when making rules to implement the CDR. Some proposals will apply generally to sectors that are designated for the purposes of the CDR regime, however, because the first sector to be designated is banking, the rules framework has a banking focus. It also identifies some issues upon which the ACCC is yet to form a view.

The rules framework does not outline the proposed drafting for particular rules. Rather, it outlines the substantive and/or 'in principle' position the ACCC proposes to take when making rules. This should give stakeholders transparency over the ACCC's proposed approach prior to the drafting of a detailed set of rules, and enable informed consultation.

The ACCC will not have legal authority to make the rules until the passage of the draft legislation. The ACCC understands that the draft legislation is expected to be introduced into Parliament before the end of 2018, to commence in early 2019. Once the legislation commences, the ACCC and the Minister will undertake the requisite processes to formally make the rules. The positions in this rules framework are therefore what the ACCC proposes to reflect in rules, once the rule-making power is conferred. The ACCC expects draft rules to be published in December 2018.

ACCC approach to rules development

Building upon the Open Banking review

The ACCC recognises that many stakeholders have engaged with the Open Banking review and have given consideration to many issues.

This paper takes the final report of the Open Banking review as a reference point.[5] The Open Banking review has considered a number of issues and in many instances considered those issues thoroughly. As such, in many instances the ACCC proposes to make rules that will give effect to the positions reached in the Open Banking review.

The ACCC has also had regard to the UK experience of developing and implementing its Open Banking regime, which commenced in January 2018. Under the UK regime, the nine largest UK banks are required to share data with accredited third parties using secure open application programming interfaces (APIs) at the customer's direction. While the ACCC's proposed positions have been reached with Australian circumstances in mind, the UK experience has been a useful reference point.

In other cases, the Open Banking review has identified issues that will need to be resolved by the ACCC. In these cases the ACCC has, as far as possible, sought to outline a preliminary view on how it proposes to address that issue in the rules. In reaching this view the ACCC has considered submissions made to the Open Banking review, the approach taken under the Open Banking regime in the UK, and other relevant material. However,

5 Available at https://treasury.gov.au/review/review-into-open-banking-in-australia/.

some of these issues are multi-faceted and complex, and require further consideration before the ACCC can arrive at a proposed position.

Consistent with the objectives of the CDR regime

In developing the rules that will apply from 1 July 2019, the ACCC's approach is to focus on the objectives of the regime and what is achievable by 1 July 2019 to provide benefits to consumers without compromising security of data or confidence in the CDR.

The draft legislation proposes that the ACCC have regard to the following matters when making rules: [6]

(a) the likely effect of the rules on:

- (i) consumers
- (ii) the efficiency of relevant markets
- (iii) the privacy of consumers (whether individual consumers or other kinds of consumers such as businesses)[7]
- (iv) promoting competition
- (v) promoting data-driven innovation

(b) the likely regulatory impact of allowing the rules to impose requirements on the persons covered by a designation instrument

(c) any other matters that the ACCC considers to be relevant.

Interaction between rules and standards

As recognised in the Open Banking review, there needs to be a close relationship between the rules and the standards under the CDR regulatory framework.

The ACCC recognises that a degree of flexibility is required to allow continuing development of the standards, particularly to take into account new technologies and the incorporation of other sectors within the CDR regime. If the rules set overly prescriptive requirements for the standards, this may restrict the ability of the standards to evolve, or necessitate frequent changes to the rules to accommodate new developments.

The ACCC is also aware of the implementation experience in the UK and has been advised that some challenges were created by an absence of detail in the over-arching regulatory framework.

In many instances the ACCC is proposing that the rules will create high level obligations, such that certain activities required by the rules will need to be carried out in accordance with the relevant standard. A breach of a standard would therefore constitute a breach of the rules and be actionable by the ACCC. In addition, the ACCC will monitor implementation and consider revising particular rules to be more or less specific if experience demonstrates this is necessary.

Civil penalty provisions of the rules

The rules framework does not identify which of the proposed rules will be specified as civil penalty provisions, since the penalties applying to contravention of the draft legislation and the rules may change in the final legislation. However, the ACCC's current position is that

6 Draft legislation, section 56BN (which applies the matters in section 56AD(1)).
7 The ACCC acknowledges that it may be preferable to refer to the privacy of individuals and the confidentiality of businesses.

rules imposing obligations on data holders or accredited data recipients will be specified to be civil penalty provisions.

Progressive development of rules

The ACCC does not propose to address all potential issues in the first version of the rules, but will instead seek to make rules on the matters that are essential for the commencement of Open Banking on 1 July 2019.

At points in the rules framework the ACCC identifies issues that have been raised by stakeholders in consultation on the Open Banking review, or that have been raised or addressed in the Open Banking review itself, but which the ACCC does not propose to make rules on at this time. Submissions are sought on these matters, including on whether they should be included in the first version of the rules, noting that the ACCC has discretion to determine what is addressed in the first version of the rules and will need to have regard to what is achievable by 1 July 2019.

Part B – The rules framework

1. General obligations and structure of the rules framework

The CDR aims to give consumers more access to and control over their data. The core obligations of the CDR regime will be on data holders and accredited data recipients (together known as CDR participants):

1. At a consumer's direction, a data holder will be obliged to share a consumer's data with either:
   (a) an accredited data recipient to whom the consumer has provided their consent (see section 2), or
   (b) the consumer themselves (see section 10).
2. A data holder will make certain generic product data publicly available (see section 11).

The rules and standards will jointly specify many of the issues necessary for the CDR to operate, including:

- which consumers can take advantage of the CDR (see section 3)
- the data sets that are within scope (see section 5)
- the criteria an entity must satisfy to be an 'accredited data recipient' (see section 6)
- requirements for consumer consent (see section 8)
- requirements for authorisation and authentication (see section 9)
- the limits a consumer can place around the use of their data (see sections 8 and 12).

Three key concepts in the rules framework are 'consent', 'authorisation' and 'authentication':

- Consent refers to the consumer consenting to the data recipient collecting and using the consumer's data. The consumer's express and informed consent will be required for each of the accredited data recipient collecting the data, and using the data. In practice these consents will likely be obtained at the same time.
- 'Authorisation' is used to refer the consumer permitting the data holder to share data with the accredited data recipient. 'Authorisation' also has a technical meaning that relates to a process by which the accredited data recipient's application obtains access to the consumer's data via the data holder's API.
- 'Authentication' is the process by which the data holder verifies the identity of the consumer directing the sharing of their data, and the identity of the accredited data recipient seeking to collect the consumer's data. Authentication occurs as part of the authorisation process.

The draft legislation imposes limitations on the scope of consumer data rules. The rules cannot require a data holder to disclose data before 1 July 2019 or impose a requirement that has retrospective application.[8]

[8] Draft legislation, section 56BI(1).

2. Sharing data with third party recipients

Summary of proposed rules

The ACCC proposes to make rules to the effect that:

- an accredited data recipient may only collect and use a consumer's data where it has obtained their consent, and only in accordance with that consent.
- a data holder must share a consumer's data with an accredited data recipient where the consumer directs and authorises the data holder to do so.
- data sharing must only occur where the consumer has given relevant informed consent to the accredited data recipient and authorisation to the data holder.
- authorisation and authentication processes will meet certain requirements.
- data sharing must occur via an API. The API will be implemented in accordance with the standards developed by the Data Standards Body, and data sharing must occur in accordance with those standards.

The ACCC proposes that in the first version of the rules, data sharing will not be subject to fees.

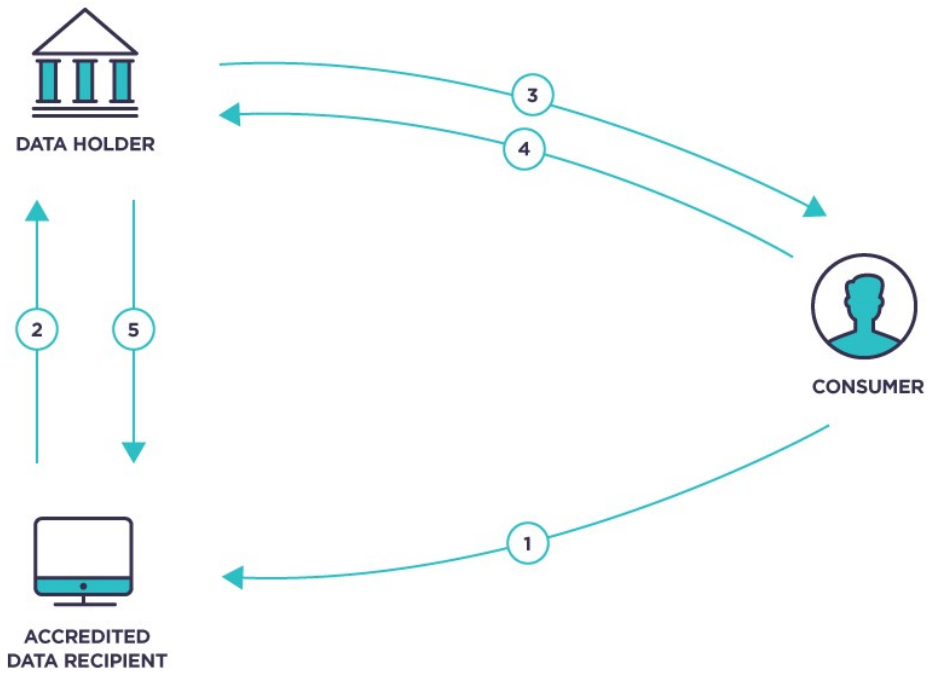
As outlined above, a core element of the CDR is to enable the sharing of designated data from a data holder to an accredited data recipient, at the direction and with the consent of a consumer. This part of the rules framework addresses requirements around the sharing of data with third party data recipients.

The ACCC proposes to make rules that create the obligation to share data where the criteria set out in the legislation and rules are satisfied. Further detail on data disclosure will be specified in the standards made by the Data Standards Body, and the rules will incorporate and cross-reference these standards where appropriate.

2.1. Process flows

It is useful to outline in a simplified form the key steps involved in the sharing of data with a third party. This assumes that data is made available via an API, as contemplated by the Open Banking review.

The simplified process is outlined in the following illustrative diagram:



1. The consumer consents to the accredited data recipient obtaining their data
2. The accredited data recipient seeks to access the consumer's data and their identity and accreditation status is authenticated by the data holder
3. The data holder authenticates the identity of the consumer
4. The consumer authorises the data holder to disclose their data to the accredited data recipient
5. The consumer's data is shared between the data holder and the accredited data recipient

2.2. Sharing via an API

The Open Banking review recommended that data holders should be required to allow customers to share their data with eligible parties via a dedicated API.[9] As the Open Banking review notes, APIs are the standard mechanism for sharing information between software securely and efficiently and some banks, including some Australian banks, already make data available through APIs.[10]

The ACCC proposes to make rules to the effect that data sharing is to occur via an API, to give effect to the Open Banking review recommendation. The ACCC also proposes to make related rules to the effect that the API must be implemented in accordance with the standards developed by the Data Standards Body, and that the sharing of data must also occur in accordance with those standards.

2.3. Sharing must not attract a fee

The draft legislation includes provisions that allow the ACCC to make rules that specify a fee to be charged for the disclosure or use of specified CDR data.[11] While these provisions enable the ACCC to specify fees in rules, they do not mandate the ACCC to do so.

9 Open banking review, recommendation 5.1.
10 See sections 2 and 5 for a detailed discussion.
11 Draft legislation, section 56BC(d).

The ACCC proposes that in the first version of the rules, the sharing of the data outlined in the Open Banking review not be subject to fees. The Open Banking review considered whether value-added data should be included within scope of Open Banking,[12] and the draft legislation includes a concept of 'derived data', both of which are relevant to the prospect of fees being charged for data sharing under the CDR regime. See section 5.2 for further discussion of these topics.

3. CDR consumer – who may take advantage of the CDR?

Summary of proposed rules

The ACCC proposes that the first version of the rules will enable a consumer to direct a bank to share their data only if they are currently a customer of that bank.

The ACCC proposes that the first version of the rules extend the CDR to consumers who have access to and use online banking, but not to offline consumers.

The ACCC seeks stakeholder views on what would be a reasonable timeframe for extending the CDR to former customers and offline consumers.

The Open Banking review recommended a broad definition of 'consumer' within the CDR regime, with the obligation to share data to apply in relation to all customers holding a relevant bank account in Australia.[13] The Open Banking review supported the ability for individual and business customers to take advantage of the CDR, but acknowledged that certain large business customers that make use of specifically tailored banking products will not be covered.[14]

The draft legislation includes a definition of 'CDR consumer', specifying that a CDR consumer for 'CDR data' (also a defined term) is a person to whom the CDR data relates, if the person is identifiable or reasonably identifiable from the data.[15] The draft explanatory materials notes that this definition is broader than the definition of 'consumer' under the CCA because it includes business consumers as well as individuals.[16] This approach is consistent with the recommendations of the Open Banking review.

The CDR will therefore be available to both individuals and other entities, such as businesses and trusts. The availability of the CDR to these parties is likely to be dealt with in the legislation and the designation instrument. The rules on this topic will therefore largely address issues around the specific delineation of a CDR consumer, as outlined in the following sections.

3.1. Former customers

The Open Banking review contemplated that the CDR apply to data held by a data holder about former customers.[17]

The ACCC recognises the utility in providing former customers with the right to access relevant data concerning their prior accounts. The ACCC also acknowledges that there are some issues to be resolved in enabling this, including the authentication process for former customers and the timeframe over which customers may seek to exercise the CDR once they cease to be a customer.

The ACCC does not consider resolution of these issues to be critical for the first version of the rules. The ACCC therefore proposes that the first version of the rules will not enable

12 Open Banking review, recommendation 3.3.
13 Open Banking review, recommendation 3.7.
14 Open Banking review, page 42.
15 Draft legislation, section 56AF(4). The data must also be held by, or on behalf of, a data holder or an accredited data recipient of the CDR data.
16 Draft explanatory materials, paragraph 1.53.
17 Open Banking review, recommendations 3.1 and 3.2.

former customers to exercise the CDR. However, the ACCC considers it desirable that former customers are brought within scope as soon as possible, and seeks stakeholder views on what would be a reasonable timeframe for requiring data holders to share the data of former customers under the CDR regime.

3.2. Offline consumers

The Open Banking review recommended the development of standards to enable consumers who do not have access to online banking to authorise the sharing of their CDR data.[18]

The ACCC recognises that a number of consumers do not use online banking, and that this should not necessarily exclude their participation in the CDR regime. That said, Open Banking and the CDR regime largely assume access to and sharing of data by digital means, and it is likely that significant benefits for consumers will be delivered where there is an initial focus on existing digital channels.

The ACCC therefore proposes that the first version of the rules extend the CDR to consumers who have access to and use online banking. This would include consumers who use a web browser or a mobile app to access their accounts. Methods by which consumers without online banking accounts can access Open Banking will be brought within scope in a subsequent version of the rules. The ACCC seeks stakeholder views on what would be a reasonable timeframe for requiring banks to share data of their offline consumers under the CDR.

4. Data holder – who is obliged to share data?

Summary of proposed rules

The ACCC proposes to make rules to give effect to the phased implementation of Open Banking as outlined by the government.

The 'four major banks' will be within scope of the rules for the initial phase. The ACCC proposes to exempt the related brands of these banks from the first version of the rules.

Other ADIs, with the exception of foreign bank branches, will be brought within scope 12 months later, including related brands of the four major banks.

The ACCC proposes to make a rule to acknowledge that exemptions for certain entities from some or all obligations may be granted in certain cases, should the need arise.

The Open Banking review recommended that the obligation to share data at a consumer's direction should apply to all Authorised Deposit-taking Institutions (ADIs), other than foreign bank branches.[19] In responding to the Open Banking review the government outlined a phased approach to the implementation of Open Banking, with staggered deadlines for datasets to come within scope, and a requirement that the 'four major' banks be within scope initially, and that other ADIs be brought within scope on a 12 month delay (see further discussion below).[20]

The draft legislation includes a definition of 'data holder' that in effect provides that a data holder is a person, or class of persons, specified in a designation instrument for that purpose.[21] The ACCC understands that the designation instrument for Open Banking will give effect to the Open Banking review's recommendation by specifying that ADIs, other than foreign bank branches, are data holders. The rules will add specificity, including to implement the government's phased approach.

18 Open Banking review, recommendation 5.9.
19 Open Banking review, recommendation 3.8.
20 Consumer Data Right Booklet, page 8.
21 Draft legislation, section 56AG(1).

4.1. ADIs

The term 'ADI' is defined in the *Banking Act 1959* (Cth) (Banking Act). An ADI is a body corporate that the Australian Prudential Regulation Authority (APRA) has granted authority to carry on 'banking business' in Australia.[22] APRA maintains a register of ADIs on its website.[23] The register categorises the following types of ADIs:

- Australian-owned banks
- foreign subsidiary banks
- branches of foreign banks
- building societies
- credit unions
- restricted ADIs
- other ADIs
- providers of purchased payment facilities.

The ACCC therefore understands that all ADIs, other than foreign bank branches, will be data holders and expected to be within the scope of the CDR unless otherwise exempted by the rules. These ADIs will not all be within scope initially, but will be brought within scope subject to the phased implementation outlined by the government.

4.2. Phased implementation

The government proposed that Open Banking would be phased in, with the aim that:

- the four major banks make data available on credit and debit card, deposit and transaction accounts by 1 July 2019, and mortgages by 1 February 2020, including for joint accounts where digital authorisations to transact on the accounts already exist
- all remaining ADIs implement Open Banking 12 months later
- consumer data on all products recommended by the Open Banking review be available by 1 July 2020
- data relating to the terms of banking products will become available at the same time as transaction data in relation to those products – in the rules framework this category of data is the generic product data discussed in section 5.3.3 and 11.[24]

The government also said that the ACCC will be responsible for determining the detail of phasing, and will have flexibility to adjust the timing for implementation where necessary.[25]

The ACCC proposes to make rules to give effect to the phased implementation of Open Banking as outlined by the government. In doing so the ACCC proposes to make rules to the effect that the 'four major banks' within scope of the initial phase are:

---

22 Banking Act, section 9(3). "Banking business" is defined in section 5 of the Banking Act to mean:
(a) a business that consists of banking within the meaning of paragraph 51(xiii) of the Constitution; [which itself refers to 'banking, other than State banking; also State banking extending beyond the limits of the State concerned, the incorporation of banks, and the issue of paper money]; or
(b) a business that is carried on by a corporation to which paragraph 51(xx) of the Constitution applies and that consists, to any extent, of:
(i) both taking money on deposit (otherwise than as part-payment for identified goods or services) and making advances of money; or
(ii) other financial activities prescribed by the regulations for the purposes of this definition.

23 Available at https://www.apra.gov.au/register-authorised-deposit-taking-institutions.

24 Consumer Data Right Booklet, page 8.

25 Consumer Data Right Booklet, page 8.

- Australia and New Zealand Banking Group Limited
- Commonwealth Bank of Australia
- National Australia Bank Limited
- Westpac Banking Corporation.

Related brands of the four major banks will not fall within the first version of the rules (for example: Bank West, UBank, St George, Bank of Melbourne, etc.). Instead, the ACCC proposes to make rules to the effect that these entities participate 12 months later, in line with other ADIs.

4.3. Data held by or on behalf of a data holder

For completeness, the ACCC notes that the definition of a 'data holder' in the draft legislation provides that a person is a data holder where they are designated as such by the designation instrument, and where the designated data is held *by or on behalf of that* person.[26] This means that an ADI will be a data holder where data is held on their behalf by, for instance, an agent, contractor or other third party and the ADI cannot by that reason avoid their obligations under the CDR.

4.4. Exemptions

The ACCC recognises that with the subsequent phases of Open Banking there may be a need to exempt certain entities from some or all obligations. Exemptions could be granted via the rules, and the ACCC proposes to make rules that acknowledge that exemptions may be granted in certain cases.

5. Data sets – what data is within scope?

Summary of proposed rules

The ACCC proposes to make rules to specify minimum inclusions for 'customer data'. In relation to customer data, the ACCC also proposes:

- to make a rule to the effect that the obligation to share customer data will only apply to this information where it is kept in a digital form.
- to make a rule to the effect that product data which relates to an account that a customer holds is within scope.
- to not include identity verification assessments within the scope of customer data in the first version of the rules.
- to not include data relating to authorisations to share data given under the CDR within the scope of customer data in the first version of the rules.

The ACCC proposes to make rules to specify minimum inclusions for 'transaction data'.

The ACCC welcomes submissions from stakeholders on what transaction metadata could be within scope; what benefits to consumers it could deliver; and what risks would arise.

The ACCC proposes to make rules to specify minimum inclusions for 'product data'.

The ACCC proposes to make rules to the effect that data holders will be obliged to make 'generic' product data publicly available (see section 11 below).

The ACCC proposes to make rules which specify that the standards will include further detail with respect to the relevant data sets, including specific fields and formats and a detailed product data taxonomy. The ACCC proposes to make a rule to the effect that data should be shared in the format as determined by the standards.

26 Draft legislation, section 56AG(1).

The Open Banking review made recommendations on the data that should be within scope of Open Banking, identifying a number of data sets under the headings of customer-provided data, transaction data and product data. [27]

5.1. Draft legislation and designation instrument

The draft legislation provides that, in effect, 'CDR data' is information that is specified in, or is within a class of information specified in, a designation instrument.[28]

The ACCC understands that the designation instrument will specify that data in relation to certain 'deposit products' and 'advances' (that is, lending products) is 'CDR data'. These concepts may be cross-referenced to the *Banking Regulation 2016* (Banking Regulation), which specifies particular types of account that are subject to the government banking guarantee. The designation instrument may also specify that the relevant data sets for those defined products encompass customer data, transaction data and product data. It may also specify that data sets relate to products that are currently on offer or which have current customers. Depending on the degree of generality at which these data sets are stated in the designation instrument, the ACCC will add specificity via the rules.

As noted earlier, the Open Banking review considered that data should be available in relation to the relevant products that are 'widely available to the general public'. The ACCC understands that the designation instrument will not specify this condition, and it consequently may be appropriate to do so in the rules.

5.2. Derived data

The Open Banking review recommended that data that results from 'material enhancement by the application of insights, analysis or transformation by the data holder' should not be within scope of Open Banking.[29]

The draft legislation provides that 'CDR data' can include data that is 'directly or indirectly derived' from underlying CDR data. The ACCC understands that the purpose of this inclusion is twofold:

- to ensure that the privacy safeguards and other protections continue to apply to data that has been derived from the 'underlying' CDR data, and
- to provide scope for transformed or value-added data to fall within the CDR regime.

The ACCC accepts that the terms 'transformed' or 'value-added' can encompass a spectrum of activities, from simple transformation of data (for instance, simple arithmetic or collation) through to sophisticated analysis. The proposed rules relating to data sets set out in the following sections seek to ensure that the data sets recommended by the Open Banking review are within scope, recognising that these data sets may include derived data, though not data that results from 'material enhancement' as contemplated by the Open Banking review.

5.3. Data sets

On the assumption that the CDR rules will be required to further delineate the relevant data sets identified in the designation instrument, the ACCC proposes to make rules specifying the data sets identified below. The ACCC acknowledges that consultation on this rules framework will further refine how these data sets are defined.

27 Open Banking review, recommendations 3.1, 3.2 and 3.6.
28 Draft legislation, section 56AF(1).
29 Open Banking review, recommendation 3.3.

The ACCC also notes that it is expected that the designation instrument will place a temporal limit on data sets that can be within scope, stipulating that data generated or collected prior to 1 January 2017 is outside of scope.[30]

5.3.1. Customer data

The Open Banking review recommended that a data holder should be obliged, at a customer's direction, to share all information that has been provided to them by the customer (or a former customer – though see the discussion above at 3.1). The Open Banking review also recommended that the obligation should only apply where the data holder keeps that information in a digital form. Also, the obligation would not extend to information supporting an identity verification assessment. Data holders would only be obliged to share such information with the customer directly, not with a data recipient.[31]

The ACCC proposes to make rules to the effect that customer data will include, at a minimum:

- the customer's name
- the customer's contact details
- the customer's account number(s)
- payee lists/direct debit authorisations on the account(s)
- account-level information, such as authorisations on the account and account-level contact details
- any unique identifiers associated with the listed items.

The ACCC proposes to make rules that the obligation will only apply to this information where it is kept in a digital form.

The ACCC also proposes to make rules to the effect that the product data specified in section 5.3.3, as it relates to an account or accounts that a customer holds, is within scope. This will ensure that the features of the account that the individual customer holds, such as the applicable fees, charges or interest rates on that account, can be shared.

In relation to identity verification assessments, the Open Banking review recommended that the outcome of these assessments be within scope of Open Banking, subject to reforms to anti-money laundering laws that would allow data recipients to rely on the outcome of that assessment.[32] As these reforms have not yet occurred, the ACCC does not propose to include identity verification assessments within the first version of the rules.

A subsequent version of the rules may require the sharing of authorisations given under the Open Banking regime; that is, it will be for consumers to share the authorisations they have given to share their data. The ACCC does not consider it to be essential that this data set is included in the first version of the rules.

5.3.2. Transaction data

The Open Banking review recommended that data holders be obliged, at a customer's direction, to share the customer's transaction data in a form that facilitates its transfer and use.[33] The ACCC proposes to make rules to the effect that transaction data include, at a minimum:

30 Draft explanatory materials, paragraph 1.41.
31 Open Banking review, recommendation 3.1.
32 Open Banking review, recommendation 3.4.
33 Open Banking review, recommendation 3.2.

- the opening and closing balance of an account for the period specified
- the date on which a transaction was made
- the relevant identifier for the counter-party to a transaction
- the amount debited or credited pursuant to the transaction
- the balance on the account prior to and following a transaction
- any description in relation to the transaction, whether entered by the consumer or the data holder
- any identifier or categorisation of the transaction by the data holder (that is, debit, credit, fee, interest, etc.).

A principle underlying the specification of transaction data is that data relating to transactions made by the CDR consumer in relation to the relevant products will be within scope. This creates a nexus between the CDR consumer and their data set, and means the transaction data is data that relates to an identifiable or reasonably identifiable CDR consumer, and is therefore protected by the privacy safeguards. A further principle is that transaction data should include, at a minimum, data that is available on a consumer's bank statement.

The ACCC is considering whether the metadata associated with each transaction should be included as part of the transaction data to be shared in the first version of the rules. 'Metadata' is data about data, and in relation to transactions could include information such as geolocation data on where a transaction occurred, or the time when a transaction took place. The ACCC welcomes submissions from stakeholders on what metadata could be within scope, what benefits to consumers it could deliver if it was in scope and what risks would arise and need to be managed.

5.3.3. Product data

The Open Banking review recommended that if data holders are under an existing obligation to disclose information on their products and services (such as information on their price, fees and other charges), that information should be made publicly available under Open Banking.[34]

The ACCC proposes to make rules to the effect that this product data will include, at a minimum:

- product type
- product name
- product prices
- all fees and charges, including interest rates, associated with the product, and the circumstances in which these apply
- features and benefits
- terms and conditions
- customer eligibility criteria.

Product data that does not relate to an identifiable or reasonably identifiable person may be described as 'generic' or 'reference' data. Data holders will be obliged to make this data publicly available (see section 11). The ACCC understands that the standards process will develop a taxonomy to assist with like-for-like comparisons of generic product data from different institutions. This generic product data will not be subject to the privacy safeguards.

34 Open Banking review, recommendation 3.6.

Product data may relate to an identifiable or reasonably identifiable person where *it relates to an account or accounts that a customer holds*. As noted in section 5.3.1, including this data will ensure that the features of the account that the individual customer holds, such as the applicable fees, charges or interest rates on that account, can be shared. This data will be subject to the privacy safeguards.

5.3.4. Interaction with data standards

The ACCC will make rules to specify that the standards will include further detail with respect to the relevant data sets, including:

- the specific fields and formats for customer, product and transaction data, and
- a detailed product data taxonomy for 'generic' or 'product reference data'.

The ACCC also proposes to make a rule to the effect that the data should be shared in the format as determined by the standards.

5.4. Reciprocity

The Open Banking review supported in principle the concept that an accredited data recipient should be obliged to provide equivalent data in response to a direction of a consumer, but left complex issues for further consideration by the ACCC.[35] The Open Banking review provided views on what 'equivalent data' would consist of, and suggested that the ACCC determine what constitutes equivalent data for Open Banking as part of the accreditation process for accredited data recipients that do not operate in the banking sector.[36] However, this was not a condition of the data sharing obligation that was recommended, and not reflected in the formal recommendations. Recommendation 3.9 stated that:

> *Entities participating in Open Banking as data recipients should be obliged to comply with a customer's direction to share any data provided to them under Open Banking, plus any data held by them that is transaction data or that is the equivalent of transaction data.*

The Consumer Data Right Booklet endorsed reciprocity as a principle, noting that the exact detail of reciprocity is yet to be settled and will be subject to further consultation.[37] The Consumer Data Right Booklet also noted that the enabling legislation would incorporate a principle of reciprocity, allowing the ACCC to make rules regarding implementation, including rules regarding the timing of when accredited data recipients would become subject to reciprocity requirements.[38]

A number of stakeholders have argued for the concept of reciprocity to be introduced into the CDR regime and Open Banking; that is, the concept of extending the CDR obligations for equivalent data sets to data recipients, making them in effect data holders.

The ACCC does not understand the principle of reciprocity to mean that a data holder is entitled to request or obtain data from an accredited data recipient before sharing data it has been directed to share by a CDR consumer. Reciprocity is not a 'quid pro quo' arrangement between data holders and accredited data recipients. The CDR regime is consumer focused, and any approach to reciprocity would need to be based on a consumer directing and consenting to an accredited data recipient sharing their data.

35 Open Banking review, page 44.
36 Open Banking review, page 44.
37 Consumer Data Right Booklet, page 4.
38 Consumer Data Right Booklet, pages 4-5.

In the ACCC's view the concept of reciprocity raises complex issues requiring further consideration. The ACCC therefore does not propose to make any rules regarding reciprocity in the first version of the rules.

6. Accreditation

Summary of proposed rules

The ACCC proposes to provide for a single general tier of accreditation in the first version of the rules.

The ACCC also supports the development of lower tiers of accreditation, and welcomes the views of stakeholders about the tiers that it would be practical to implement and the basis for any reduced accreditation requirements.

The ACCC proposes to make rules that the Data Recipient Accreditor grant accreditation to an applicant if it is satisfied that:

- the applicant is a 'fit and proper' person to receive CDR data
- the applicant has appropriate and proportionate systems, resources and procedures in place to comply with the legislation, the rules and the standards including in relation to information security
- the applicant's internal dispute resolution processes meet the requirements specified in the rules and the applicant is a member of an external dispute resolution body recognised by the ACCC
- the applicant holds appropriate insurance. The ACCC welcomes views about appropriate insurance cover, current availability and cost.

The ACCC proposes to make rules that will specify the manner in which accredited data recipients are permitted to describe their accredited status.

The ACCC proposes to make rules to provide a streamlined accreditation process for ADIs (other than restricted ADIs or providers of purchased payment services).

The ACCC does not propose to provide for recognition of accreditation in other jurisdictions in the first version of the rules.

The ACCC proposes to make rules that will require any foreign entity that is granted accreditation to appoint a local agent that will be responsible for any obligations of the foreign entity under the CDR regime.

The ACCC proposes to make rules specifying the powers and obligations of the Data Recipient Accreditor, including rules:

- allowing the Data Recipient Accreditor to suspend or revoke an accredited data recipient's accreditation on grounds relating to the criteria for accreditation and to protect the security or integrity of the CDR regime
- providing for the revocation of accreditation where this is requested by an accredited data recipient.

The ACCC proposes to make rules that will specify what happens in relation to a data recipient's CDR obligations when a decision is made to suspend or revoke its accreditation.

The ACCC proposes to make rules that will require an accredited data recipient that enters into an outsourcing arrangement involving the disclosure of CDR data to ensure it has appropriate plans and processes in place for managing risk.

The ACCC proposes to make rules that specify the steps an accredited data recipient must take to protect CDR data from misuse, interference, loss or unauthorised access, modification and disclosure. The ACCC welcomes views from stakeholders about appropriate industry standards that may be recognised under the rules for compliance with this obligation.

6.1. Background

6.1.1. Open Banking review

The Open Banking review recommended that only accredited parties should be able to receive CDR data and that the ACCC should determine the criteria for, and the method of, accreditation.[39] In determining the accreditation criteria as part of the rule setting process, the Open Banking review noted that the ACCC should consult with relevant sectors to ensure that accreditation is based on objectively determined standards.[40]

The Open Banking review recognised that not all entities will pose the same risk to the regime and that a balance needs to be struck 'between the safeguards needed to promote confidence and a sustainable Open Banking system, and avoiding unnecessary barriers to entry and innovation' in setting the accreditation criteria.[41] The Open Banking review notes that the experiences in other jurisdictions provide some indication of issues that might be considered in Australia in determining the accreditation criteria,[42] specifically citing requirements under the European Union's revised Payment Services Directive (PSD2) and the UK's *Payment Services Regulations 2017* (PSR).

The Open Banking review also provided examples of the type of criteria that may influence a finding that a party has sufficient systems and resources in place to control and mitigate material risks in order to become accredited, including whether the party can provide evidence of risk management processes and measures including in regard to their outsourcing arrangements, whether they have the technical capabilities to meet the standards, and whether they have a history of data breach or misuse, or of disregard for the law.[43]

The Open Banking review also recommended that accreditation be 'tiered', in accordance with risk-based accreditation standards. The Open Banking review envisaged that the tiers would be based on an assessment of the harm that could arise from unauthorised disclosure of particular types of CDR data, as well as risks related to the party seeking accreditation.[44] Parties accredited to receive lower risk data sets would not be able to receive higher risk data sets (and accreditation at this level could be akin to a registration process), and parties accredited to receive higher level data sets could receive both high and low risk data.[45]

The Open Banking review recommended that ADIs be automatically accredited as data recipients.[46]

The Open Banking review recognised that several other jurisdictions are in the process of implementing open data regimes and identified that mutual recognition of accredited parties from those jurisdictions ('passporting') may amplify the benefits of Open Banking.[47] However, the Open Banking review noted that passported entities must be subject to Australian laws,[48] and that the ACCC would need to consider what would be required to passport accredited entities from other jurisdictions into Australia's Open Banking regime.[49]

39 Open Banking review, recommendation 2.7.
40 Open Banking review, page 26.
41 Open Banking review, page 23.
42 Open Banking review, page 24.
43 Open Banking review, page 26.
44 Open Banking review, page 25.
45 Open Banking review, page 25.
46 Open Banking review, recommendation 3.10.
47 Open Banking review, page 26.
48 Open Banking review, page 26.
49 Open Banking review, page 27.

6.1.2. Draft legislation

The draft legislation provides a general power for the ACCC to make rules in relation to accreditation of data recipients.[50] The rule-making power in relation to accreditation is broad in nature, reflecting that sector-specific rules for accreditation may be required.

The rule-making power also includes the ability to make rules governing the Data Recipient Accreditor, who is appointed by the Minister.[51] The Data Recipient Accreditor has the function and power to accredit persons as data recipients if the criteria specified in the rules are satisfied.[52] The draft legislation states that there is no requirement that an applicant is registered as a corporation under the *Corporations Act 2001* (Cth) (Corporations Act), or is either an Australian citizen or a permanent resident.[53] Initially, the ACCC will perform the role of Data Recipient Accreditor.[54]

The draft legislation provides for review in the Administrative Appeals Tribunal (AAT) of a decision refusing accreditation.[55]

6.1.3. Accreditation in the UK

Under the UK's Open Banking regime, the nine largest UK banks are required to share data with trusted third parties using secure open APIs at the customer's direction. All third parties (i.e. data recipients) must be accredited and regulated by the Financial Conduct Authority (FCA). Data recipients may be accredited as either account information service providers (AISPs), or payment initiation service providers (PISPs), or both. PISPs initiate payments from a customer's payment account at the customer's request. ASIPs provide online information services that consolidate information from a customer's payment accounts.[56]

The two categories of data recipients are differentiated by whether they have authority to 'read' or 'write' data. PISPs have 'write' privileges, giving them access to data which can be 'written to', in other words, modified (therefore enabling the making of payments). ASIPs only have 'read' privileges, which means they can only access data capable of being displayed, they cannot change that data.

Given the different levels of risk posed by PISPs and ASIPs, they are subject to slightly different processes in applying to participate in Open Banking; PISPs apply for authorisation,[57] while AISPs apply for registration, which has different requirements.[58]

Given the similarities between AISPs in the UK, and the way in which accredited data recipients will be able to access data under the CDR regime, the ACCC has had particular regard to the criteria that apply to the registration of AISPs in considering the criteria for accreditation that should be provided for by the rules.

6.2. Proposed rules for accreditation model and criteria

In the first version of the rules, the ACCC proposes to provide for a general tier of accreditation that will entitle an accredited data recipient to receive and hold any type of CDR data in scope for Open Banking, subject to compliance with the draft legislation, the rules, and the standards. The accreditation criteria relating to this general tier of

50 Draft legislation, section 56BA and section 56BB(1)(c).
51 Draft legislation, section 56BB(e) and section 56CA.
52 Draft legislation, section 56CB and section 56CE(1).
53 Draft legislation, section 56CE(2).
54 Draft explanatory materials, paragraph 1.43.
55 Draft legislation, section 56CF.
56 OBIE, *Open Banking Guidelines for Read/Write Participants*, May 2018 (version 3.2), part 2.1, available at https://www.openbanking.org.uk/wp-content/uploads/Guidelines-for-Read-Write-Participants.pdf.
57 PSR, regulation 5.
58 PSR, regulation 17.

accreditation, and the ongoing obligations of accredited recipients, are discussed in the sections below.

The ACCC also supports the development of lower tiers of accreditation in the first version of the rules, to the extent that this can be implemented from 1 July 2019. Lower tiers of accreditation may limit access to particular types of CDR data (or have other restrictions) and have reduced requirements for accreditation. For example, the intermediary model (see 12.1.3) is a scenario where it may be appropriate for the rules to provide for a lower level of accreditation for entities that will not collect CDR data but will be able to access and use subsets of CDR data or insights from CDR data collected by an intermediary to provide services to consumers. The ACCC welcomes the views of stakeholders about this issue and the types of lower tiers that would be useful and practical to implement, having regard to existing business models and likely use cases for CDR data. The ACCC seeks views about the basis on which lower tiers could be restricted and the way in which these limitations would reduce risks relating to the collection, storage or use of CDR data and therefore provide a basis for reduced accreditation requirements.

6.2.1. Criteria for general level of accreditation

The ACCC considers that the criteria for accreditation should be objective, to the extent possible, related to the security and integrity of the CDR regime and primarily directed towards ensuring that applicants demonstrate their capacity to manage CDR data in accordance with the privacy safeguards. In developing the proposed criteria for accreditation, as noted above, the ACCC has had particular regard to the requirements for registration as an AISP in the UK, and the requirements to be met by ADIs, in relation to risk management and the applicant's history of compliance with relevant laws. The ACCC also recognises that an objective of the CDR regime is to encourage data-driven innovation and that an appropriate balance needs to be struck to ensure that the criteria for accreditation do not impose unnecessary barriers to entry. The ACCC seeks the views about the practical implications of the proposed criteria for general accreditation in this context.

The proposed criteria for accreditation assume that in most cases an applicant will be a corporation. However, the ACCC acknowledges that individuals and other legal entities may apply for accreditation and proposes to accommodate this in the first version of the rules.

The ACCC proposes to make rules that the Data Recipient Accreditor grant accreditation to an applicant to be a 'data recipient' of CDR data if the Data Recipient Accreditor is satisfied that:

1. The applicant is a 'fit and proper' person to receive CDR data. Relevant information that will need to be provided with an application, and which may be taken into account by the Data Recipient Accreditor for the purposes of this assessment, is expected to include:
    - whether the applicant (or its directors) has been charged with or convicted of a serious criminal offence, or an offence of dishonesty, against a law of the Commonwealth or of a State or Territory
    - whether the applicant (or its directors) has been found to have contravened, or civil proceedings have been commenced against the applicant alleging contravention of, a law relevant to the management of CDR data including the *Competition and Consumer Act 2010* (Cth) (CCA) (including the Australian Consumer Law), the *Australian Securities and Investment Commission Act 2001* (Cth) (ASIC Act) and the *Privacy Act 1998* (Cth) (Privacy Act)
    - whether any directors of the applicant have been disqualified from managing corporations
    - whether the applicant or its directors has a history of bankruptcy or insolvency

- any other relevant matter.

2. The applicant has appropriate and proportionate systems, resources and procedures in place to comply with the legislation, the rules and the standards, including in relation to the management of risks relating to CDR data in compliance with the privacy safeguards. As noted at section 6.9, the ACCC seeks stakeholder views on certification against industry standards that may be appropriate to recognise in the rules as evidence of this criterion in the accreditation process. The applicant will need to provide:
    - a business plan, including a detailed description of the services the applicant intends to provide to consumers using CDR data and examples of the relevant consent screens
    - evidence of the applicant's internal control mechanisms, including:
        - if applicable, the details of outsourced activities relating to CDR data (see section 6.8 below) and of the policies and procedures in place to manage those arrangements
        - information about business continuity arrangements, including clear identification of critical operations, effective contingency plans, and procedures for testing and reviewing of the adequacy of such plans
    - evidence of the applicant's risk management processes, including:
        - effective procedures to identify, manage and monitor any risks to which it might be exposed with respect to CDR data
        - adequate procedures and processes to comply with the privacy safeguards including a copy of the policy about the management of CDR data required by privacy safeguard 1
        - the applicant's procedures for monitoring, handling, and following up security incidents and security-related customer complaints
        - the applicant's measures and tools for the prevention of fraud and illegal use of CDR data
        - descriptions of security control and mitigation measures and procedures for the mandatory reporting of incidents, and notification processes to consumers in the event of a security incident.
3. The applicant's internal dispute resolution processes meet the requirements specified in the rules and the applicant is a member of an external dispute resolution body recognised by the ACCC (see section 15).
4. The applicant holds appropriate insurance, relevant to the nature and extent of the applicant's management of CDR data.

In relation to the insurance requirement, insurance (or other comparable guarantee) is required for registration as an AISP in the UK and is determined by reference to formulae specified in guidelines issued by the European Banking Authority.[59] The ACCC sees the benefit of insurance as twofold; first, to cover potential claims for loss or damage by consumers or other CDR participants arising from misuse or loss of CDR data, and second, to cover access to services to assist recovery of security or other business systems after a security incident. The ACCC welcomes views about the appropriate types of cover,[60]current availability and cost of insurance that would meet a requirement of this kind.

59 Available at https://www.eba.europa.eu/documents/10180/1901998/Final+Guidelines+on+PII+under+PSD2+%28EBA-GL-2017-08%29.pdf.
60 For example, professional indemnity, cyber-attack, third party liability.

6.2.2. Accreditation status disclosure

In the UK, the FCA does not allow any firm to use the FCA logo in any circumstances.[61] However, this does not prevent firms from making factual statements about their regulatory status. The FCA publishes example statements for firms and notes that while it is not mandatory to use the exact wording of those statements, it is important that consumers are made aware of the firm's accredited status. For example, the wording the FCA suggests for registered AISPs is: '*[Name] is registered with the Financial Conduct Authority under the Payment Services Regulations 2017 [register reference] for the provision of payment services'*.[62]

The ACCC proposes to make similar rules that will specify the manner in which accredited data recipients are permitted to describe their accredited status, and will prohibit the use of the ACCC's logo in connection with such statements. The ACCC expects that the approved wording will be similar in form to the approved wording permitted by the FCA and will refer only to the fact that the entity is registered with the ACCC as an accredited data recipient and will include any reference details from the Register of Accredited Data Recipients (Register) (see section 7 below).

6.3. ADI accreditation

The ACCC proposes to make rules to provide a streamlined accreditation process for ADIs that are specified by the rules to be data holders, and that wish to be registered as accredited data recipients on the Register. However, this streamlined process will not apply to restricted ADIs or providers of purchased payment facilities.

The ACCC envisages that the streamlined application process will involve confirmation of a registrant's status as an ADI within the scope of the rules and provision of additional information relating to ongoing obligations as an accredited data recipient under the rules (for example, the applicant's CDR data management plan and details of appropriate insurance).

The rules will apply to ADIs that are registered as accredited data recipients through this process in the same way they will apply to all other accredited entities. For example, accredited ADIs will be included on the Register, will need to comply with the obligations of accredited data recipients under the draft legislation and the rules, and will be subject to the rules relating to suspension or cancellation of accreditation.

6.4. Recognition of participants of other Open Banking regimes

The ACCC does not propose to provide for recognition of accreditation in other jurisdictions (for example, entities that are registered as AISPs in the UK) in the first version of the rules. The ACCC considers that this issue requires further consideration and consultation with relevant authorities in other jurisdictions. The ACCC anticipates that recognition of entities participating in other similar regimes will be included in a later version of the rules and ideally on the basis of mutual recognition of accreditation so that entities that have been accredited in Australia will have the benefit of reciprocal rights in other jurisdictions.

6.5. Accreditation of foreign entities

The draft legislation allows foreign entities to apply for accreditation under the CDR regime.[63] Once accredited, those entities will be subject to the same obligations as other accredited entities.

---

61 FCA, *Payment Services and Electronic Money – Our Approach*, July 2018 (version 2), part 7.2, available at https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf.
62 FCA, *Payment Services and Electronic Money – Our Approach*, annex 3.
63 Draft legislation, section 56CE(2).

As contemplated by the draft explanatory materials,[64] the ACCC proposes to make rules to ensure that where a foreign entity is granted accreditation, the obligations applying to the foreign entity under the draft legislation and the rules as an accredited data recipient can be effectively investigated and enforced by the ACCC, the Office of the Australian Information Commissioner (OAIC), CDR participants and consumers. Specifically, the ACCC proposes to make rules that will require a foreign entity to appoint a local agent that will be responsible for any obligations of the foreign entity under the CDR regime and may be liable for any breaches or penalties. The effect of the proposed rules will be similar to the requirement for a foreign company registered under the Corporations Act to appoint a local agent and that the local agent be authorised to accept service of process and notices on behalf of the foreign entity. If accredited, a foreign entity would have the obligation under the rules to always maintain a local agent and to notify the ACCC of any change in appointment of a local agent. Failure to comply with this obligation will be a ground for suspension or revocation of accreditation.

6.6. Data Recipient Accreditor's powers

The ACCC proposes to make rules that give the Data Recipient Accreditor the power to:

- require that an application be made in a specified form
- not consider an incomplete application
- require further information from an applicant in order to assess an application
- grant accreditation subject to conditions, which may be imposed as part of the decision to accredit, or imposed after accreditation has been granted
- conduct interviews with the applicant in order to assess an application
- have qualified 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
- suspend or revoke accreditations
- vary conditions applying to an entity's accreditation or impose conditions on an entity's accreditation.

The ACCC anticipates that the rules will provide for the payment of application fees as part of the accreditation process. The amount of the fees will be considered as part of the development of the rules and will reflect the administrative costs of assessing applications.[65]

6.7. Revocation or suspension of accreditation

The ACCC proposes to make a rule that provides that the Data Recipient Accreditor may suspend or revoke an accredited data recipient's accreditation where:

- the accredited data recipient obtained its accreditation through false statements or other irregular means
- the Data Recipient Accreditor believes, on reasonable grounds, that the accredited data recipient has contravened a civil penalty provision of the draft legislation, including the privacy safeguards, the rules, the standards or a condition of its accreditation (where applicable)
- civil or criminal proceedings are commenced against the accredited data recipient, or a director of the accredited data recipient, by a public agency in Australia alleging a contravention of the CCA (including the Australian Consumer Law), the ASIC Act, the

64 Draft explanatory materials, paragraph 1.67.
65 Draft explanatory materials, paragraph 1.73.

Privacy Act or a serious offence or an offence of dishonesty. This provision would also be extended for foreign entities to capture similar proceedings commenced by a public authority in other jurisdictions

- the accredited data recipient becomes insolvent (in the case of an individual, the individual becomes bankrupt or enters into a personal insolvency agreement; in the case of a company, the company enters into liquidation, administration, or receivership)
- the Data Recipient Accreditor considers it necessary for the protection of consumers, or to protect the security, integrity, stability of, or trust in, the CDR regime
- in the case of ADIs that have been registered as accredited data recipients, the ADI has its ADI status suspended or revoked.

The rules will set out the process for the making of a decision by the Data Recipient Accreditor to suspend, vary or revoke an accredited data recipient's accreditation, requiring the Data Recipient Accreditor to provide written notice of the proposed decision and reasons to the accredited data recipient in advance and provide an opportunity for the accredited data recipient to respond. However, this process will not apply where a decision to suspend, vary or revoke accreditation is made on the grounds that it is necessary for the security or integrity of the CDR regime.

The rules will also make provision for the revocation of accreditation where this is requested by an accredited data recipient.

6.7.1. Consequences of revocation or suspension of accreditation

The ACCC proposes to make rules that will specify what happens when a decision is made to suspend an accredited data recipient's accreditation. Specifically, the rules will prevent the suspended accredited data recipient from collecting further CDR data and will require the (temporary) de-activation of the entity's registration in the Register. However, the suspended accredited data recipient's obligations in relation to CDR data will continue to apply. The proposed rules will also require the accredited data recipient to notify CDR consumers of the suspension.

Where a decision is made to revoke accreditation, the ACCC proposes to make rules that will require the data recipient to delete or de-identify the CDR data, consistent with the rules made for the purposes of privacy safeguard 11 (see section 13). The ACCC proposes to make transitional rules to ensure that this obligation will continue to apply and can be enforced, notwithstanding the revocation of accreditation.

6.7.2. AAT review of decisions to suspend, revoke or vary accreditation

The draft legislation expressly provides for the rules to provide for the making of applications for AAT review of decisions of a person or body under the rules.[66] The ACCC acknowledges that AAT review of decisions to suspend, revoke or vary accreditation may be provided for in the final version of the legislation. To the extent that this does not occur, the ACCC proposes to make rules that will provide for review by the AAT of a decision to suspend or revoke an entity's accreditation, or to impose or vary a condition on an entity's accreditation.

The ability to seek AAT review will not apply to a decision of the Data Recipient Accreditor to revoke accreditation which is made at the request of an accredited data recipient.

66 Draft legislation, section 56BH(d).

6.8. Accreditation and outsourcing

The ACCC proposes to make rules that will require an accredited data recipient that enters into an outsourcing arrangement with a service provider that involves the disclosure of CDR data to ensure that it has in place appropriate risk management plans and processes and to ensure that it is able to meet its obligations under the CDR regime. The accredited data recipient will remain responsible and liable for compliance with all obligations under the legislation, rules and standards, notwithstanding any outsourcing arrangements.

The ACCC proposes to make rules relating to outsourcing which will require an accredited data recipient to:

- maintain a risk management policy relating to outsourcing arrangements that involve the disclosure of CDR data
- have legally binding agreements with any outsourced service provider that mirror the obligations of the accredited data recipient in relation to security and management of CDR data
- have monitoring processes in place in relation to outsourcing arrangements that involve disclosure of CDR data.

As noted in section 8, the ACCC proposes to make rules about obtaining consumer consent where an accredited data recipient discloses CDR data under an outsourcing arrangement and where CDR data will be transferred overseas (see section 8). The accredited data recipient will also be required to maintain a list of outsourced service providers in the policy about the management of CDR data to be prepared and maintained for the purposes of privacy safeguard 1.

6.9. Ongoing information security obligations

In accordance with privacy safeguard 11, the ACCC proposes to make rules that specify the steps accredited data recipients must take to protect CDR data from misuse, interference, loss or unauthorised access, modification and disclosure.

In the UK, AISPs are obliged to ensure information security, but there is no mandated method for compliance. Instead, the Open Banking Implementation Entity (OBIE) has released guidance on best practice security approaches for Open Banking participants which recommends that participants adopt the information security standard 'ISO27001:2013', or, for smaller organisations, 'Information Assurance for Small, Medium Enterprises'.[67]

APRA takes a similar approach in its draft Information Security Prudential Standard, expected to commence on 1 July 2019.[68] Under the standard, ADIs are obliged to establish and actively maintain effective information security controls, however, they are not required to comply with strict technical standards.

Under the Privacy Act, entities are required to take reasonable steps to protect the personal information that they hold, and the OAIC has published guidance on information security for this purpose.[69]

The ACCC envisages that the rules that will specify the steps to be taken to protect CDR data will broadly reflect the OAIC's information security guidelines, including by requiring appropriate systems and procedures in relation to information security, data breaches, physical security, workplace policies, and regular monitoring and review. Consistent with the

67 OBIE, *Open Banking Guidelines for Read/Write Participants*.
68 Draft Prudential Standard CPS 234 Information Security, March 2018, available at https://www.apra.gov.au/file/3531.
69 OAIC, *Guide to securing personal information: 'reasonable steps' to protect personal information*, June 2018, available at https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information.

approach taken in other regulatory regimes, the ACCC does not propose to make rules that will require compliance with a particular information security standard. However, the ACCC welcomes stakeholder views about information security standards (particularly sector specific standards), compliance with which would demonstrate that an entity has in place adequate policies and systems in relation to risk management and security in relation to management of CDR data. The ACCC will give consideration to recognising such standards in the rules for the purposes of compliance with this ongoing obligation and as part of the accreditation process. The ACCC expects that best practice information security guidelines will be published at an appropriate time, and that these guidelines will be prepared in consultation with the OAIC and the Data Standards Body.

7. The Register

Summary of proposed rules

The ACCC proposes to make rules relating to the Register, including in relation to the information required to be made publically available online and the powers and obligations of the Accreditation Registrar.

The Open Banking review states that the ACCC should have responsibility for ensuring there is a public address book of accredited parties.[70] The Open Banking review considered that the address book should be live, robust, and ideally decentralised,[71] as well as secure, transparent and include a method of tracing all changes made. [72]

The draft legislation provides for the Register. The draft explanatory materials notes that the Register will be maintained by the Accreditation Registrar, which will initially be the ACCC.[73] The Register must be available in electronic format.[74] Matters relating to the inclusion of entries on the Register, ongoing maintenance of the Register, correction of errors, and publication of all or part of the Register, will be covered by the rules.[75]

The ACCC proposes to make rules that:

- require information in the Register about the entities that are accredited, and where relevant the level of accreditation, to be made publically available online. This will enable consumers to check whether an entity is accredited
- the Accreditation Registrar may keep the Register in any electronic format and the Register may contain such information as the Registrar considers appropriate, provided that the Register identifies all entities that hold accreditation under section 56CE(1) of the draft legislation and, where different levels of accreditation exist, the person's level of accreditation
- the Accreditation Registrar may make corrections to the Register to ensure its accuracy
- the Register be updated as soon as practicable to reflect new accreditations and accreditations which have been revoked, suspended, or varied. The rules will also require the Accreditation Registrar to notify data holders when changes have been made to the Register.

70 Open Banking review, recommendation 2.9.
71 Open Banking review, page 28.
72 Open Banking review, page 28.
73 Draft explanatory materials, paragraph 1.58.
74 Draft legislation, section 56CK(2).
75 Draft legislation, section 56CK(4) and draft explanatory materials, paragraph 1.62.

8. Consent

Summary of proposed rules

The ACCC proposes to make rules to the effect that where consumers with a joint account hold individual authority to transact on that account they will each be able to give individual consent to share their joint data under the CDR regime. The rules may require that each joint account holder be notified of any data sharing arrangements and given the ability to terminate them should they wish.

The ACCC also wishes to better understand the complexities of the issue of consent in relation to complex accounts and any other relevant scenarios and seeks stakeholder views on this.

The ACCC does not propose to make rules that would seek to treat minors differently from any other consumer who may take advantage of the CDR.

The ACCC proposes to make rules to the effect that an accredited data recipient must obtain a consumer's consent to both collecting, and using, specified data for specified purposes and for a specified time.

The ACCC proposes to make rules requiring consumer consent to be freely and voluntarily given, express, informed, specific as to purpose, time limited and easily withdrawn. In particular, the ACCC proposes to make rules to the effect that:

- accredited data recipients cannot make consent to share data a precondition to obtaining other services not related to, or dependant on, the sharing of CDR data.
- consent must be unbundled with other directions, permissions, consents or agreements, and must not rely on default settings, pre-selected options, inactivity or silence.
- accredited data recipients must provide specified information to consumers as part of the consent process.
- consent be obtained using language and/or visual aids and a process that is concise and easy for consumers to understand, and that, as part of the standards-setting process, the consent process should be tested for consumer comprehension. Accordingly, the ACCC does not propose to make a rule requiring all information to be displayed on a single screen.
- accredited data recipients must disclose, in an unambiguous way at the time of seeking the consumer's consent, the uses to which data will be put. Accredited data recipients may only use data in line with the uses to which the consumer has consented, and should only seek consent to access the minimum data necessary for the uses agreed to.
- the ACCC proposes to make a range of rules which will help provide consumers with a straightforward withdrawal process.

The ACCC welcomes stakeholder views regarding the extent to which a consumer should be able to decide whether their redundant data is de-identified or destroyed.

The ACCC proposes to makes rules that will require accredited data recipients to have a system in place which allows consumers to manage their consents easily.

In relation to on-selling of data and use of CDR data for direct marketing, the ACCC's current position is that it proposes to make rules that will prohibit the use of CDR data for these purposes. The ACCC welcomes stakeholder views on this proposal.

The rules around consent are designed to ensure that consumers are properly aware of and understand what they are consenting to, but are not intended to discourage participation in the CDR regime.[76] The ACCC recognises there is a balance between ensuring consumers are appropriately in control of their CDR data, and ensuring that the CDR regime is useful and provides a positive user experience. Stakeholders may have alternative views on where this balance should be struck.

In formulating these proposed rules the ACCC has taken account of consent conditions in Open Banking in the UK, particularly the principles set out in the OBIE's Consent Model How to Guides.

76 Draft explanatory materials, paragraph 21.

8.1. Who can provide consent?

In simple terms, persons who can provide consent are those persons with the ability to exercise the CDR. The ACCC proposes that the rules provide specifically for how consent is provided in certain circumstances as set out below.

8.1.1. Joint accounts and complex authorisations

The Open Banking review considered joint accounts, where more than one person is the relevant CDR consumer. The Open Banking review recommended that authorisation for transfers of data relating to a joint account should reflect the authorisations for transfers of money from that account.[77]

The ACCC notes that while this proposal may address issues with simple joint accounts, it may not necessarily resolve all issues for accounts that allow multiple parties to view and/or transact on the account, or that otherwise entail complex account arrangements.

Further, the ACCC is conscious of particular risks that can arise in relation to vulnerable consumers, including those at risk of financial or other exploitation by other account holders.

The ACCC proposes to make rules to the effect that where consumers with a joint account hold individual authority to transact on that account (that is, they do not require the consent of the other joint account holder(s) to transact), they will be able to apply for the CDR data in their joint accounts.

The rules may require that each joint account holder be notified of any data transfer arrangements initiated on their accounts, consistent with privacy safeguard 5 (see section 13), and given the ability to readily terminate any data sharing arrangements initiated by any other joint account holders.

The ACCC seeks comments on how the rules should address alternative scenarios; that is, whether specific rules are needed relating to bringing data from complex accounts within the CDR. For instance rules may specify that only individuals with certain permissions can authorise sharing. Alternatively, they may delay sharing in relation to such accounts for a certain period to allow consumers and banks to put relevant specific authorities in place.

The ACCC wishes to better understand the complexities of this issue and seeks stakeholder views on how the rules should deal with consent in relation to complex accounts and any other relevant issues.

8.1.2. Minors

The Open Banking review did not make specific recommendations on whether consumers who are minors should be able to consent to sharing their data, although the ACCC understands the issue has been raised in consultations.

The ACCC notes that there are many banking products which are either promoted for minors or available to minors. Minors over a certain age (often 12 or 14) are able to transact on an account without the consent of a parent or guardian, although the parent/guardian may be able to limit the level of funds at their disposal. Additionally, the Privacy Act does not set out a specific age at which minors can consent to share their personal information. Guidelines on the Australian Privacy Principles (APPs) suggest though that by the age of 15 a minor would have sufficient understanding and maturity to do this.[78]

77 Open Banking review, recommendation 4.7.
78 OAIC, APP Guidelines, available at https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/.

The ACCC does not propose to make rules that will treat minors differently to any other consumer who may take advantage of the CDR.

8.2. What does the consumer consent to?

As outlined in the process flow diagram earlier, the consent process will typically be initiated through a service request by the accredited data recipient to the consumer. Consumer preferences as to the scope of data involved, the uses to which the data is put, and the time over which the data is made available will be settled in the consent provided to the accredited data recipient.

Following this, a data holder must obtain a consumer's authorisation to *disclose* to the accredited data recipient the specified data in accordance with the consumer's request. The authorisation provided to the data holder should reflect the scope of data consented to by the consumer in their interactions with the third party accredited data recipient, although will not include information as to the intended use of that data or purpose (see section 9 below).

8.3. Consent provided to accredited data recipients

The ACCC proposes to make rules to the effect that an accredited data recipient must obtain a consumer's consent to *collecting* and *making use of* specified *data*, for specified *purposes* and for a specified *time.* A consumer will be able to specify and/or limit their consent to the scope of the data provided (including the types of data and the period of time covered by the data), the uses to which the data is put, and the duration of time over which the data is made available and held.

8.3.1. Nature of the consent to be provided

The Open Banking review recommended that a consumer's consent must be explicit, fully informed and able to be permitted or constrained according to the consumer's instructions.[79] The Open Banking review found that consumers need to be confident that the CDR is focused on giving them control of their data, as without this confidence, consumer take-up of the CDR will be limited and the initiative may not achieve its policy objectives.[80]

The government reiterated the importance of genuine consent for the CDR regime, stating that consumers should be able to understand what they are consenting to, and that consents should be clear and unambiguous, and not open ended.[81] While the Open Banking review specifically recommended that consent be explicit, fully informed and able to be permitted or constrained according to the consumer's instructions, it also supported an expanded list of features, which were called for by a wide range of stakeholders:[82]

- consent should be freely given by the consumer
- a consumer's consent should be express
- consumer consent should be informed
- the consent obtained should be specific as to the purpose of sharing data, that is, the uses to which the data will be put
- consent should be time limited
- consent should be able to be easily withdrawn with near immediate effect.

The ACCC proposes to make rules to give effect to the above principles, as outlined below.

79 Open Banking review, recommendation 4.5.
80 Open Banking review, page 49.
81 Consumer Data Right Booklet, page 5.
82 Open Banking review, recommendation 4.5.

Consent should be freely given by the consumer

The ACCC proposes to make a rule that accredited data recipients cannot make consent to share data a precondition to obtaining other services not related to, or dependant on, the sharing of CDR data. This will help ensure that consent is freely given.

In this sense, the ACCC contemplates that 'freely given' consent requires a higher standard than where consent is 'voluntary'. The OAIC's Australian Privacy Principles (APP) guidelines state that consent is voluntary if an individual has a genuine opportunity to provide or withhold consent. Consent is not voluntary where there is duress, coercion or pressure that could overpower the person's will. 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 if an individual refuses to consent
- any adverse consequences for family members or associates of the individual if the individual refuses to consent.[83]

The ACCC proposes to make rules to the effect that consent should be voluntary in the sense described by the OAIC's APP guidelines, and must also be freely given in the sense outlined above.

The ACCC also proposes to make a rule stating that consent should be unbundled from other directions, permissions, consents or agreements.[84] Bundled consent refers to the practice of 'bundling' together multiple requests for an individual's consent to a range of collections, uses and disclosures of information, without giving the individual the opportunity to choose which collections, uses and disclosures they agree to and which they do not.[85] This proposed rule would mean that consent to collect and use the data should not be bundled with other directions, permissions, consents or agreements, for example with other content such as general terms and conditions or privacy notices. This will help ensure that consent is freely given as well as specific as to purpose.

Consent should be express

The ACCC proposes to make a rule that a consumer's consent to the collection and use of CDR data is express. This will require accredited data recipients to ensure consumers make an affirmative action when consenting to the collection and use of data. Such consent should allow consumers to opt in and must therefore not rely on default settings, pre-selected ('pre-ticked' or 'pre-checked') options, inactivity or silence. Implied consent will not be permitted and will not satisfy an accredited data recipient's obligations under the rules.[86]

These requirements will help ensure that consumers make an active decision to opt in to the services they have chosen, rather than having to opt out of options they do not want. The proposed rule requiring accredited data recipients to provide specified information to consumers as part of the consent process (outlined below) will also assist to ensure that consumers' consent is express.

83 APP guidelines, at B.43 and B.44.
84 Open Banking review, page 133.
85 APP Guidelines.
86 Consumer Data Right Booklet, page 5.

Consent should be informed

Specified information to be provided

The ACCC proposes to make a rule that requires accredited data recipients to provide specified information to consumers as part of the consent process. This will help ensure that consent is express and informed. The ACCC proposes to make rules to the effect that the consent request from the accredited data recipient include:

- the name of the accredited data recipient requesting the information
- if the accredited data recipient is to collect the data via an intermediary, the name of the intermediary the accredited data recipient proposes to use
- if the accredited data recipient uses or proposes to use any outsourced service providers to assist in providing the service to the consumer, the name of those third party service providers
- the data that has been requested, including the type of data, and where relevant, the period of time covered by the data
- the purpose of the data request and the uses to which the data will be put, including specifying in detail the role of any accredited intermediary or third party provider the accredited data recipient will use to provide the service to the consumer
- the period for which any transaction data has been requested
- when the accredited data recipient's access to the data will expire
- the period for which the accredited data recipient will hold the data
- whether the request is one-off or recurring and, if recurring, how frequently data will be shared/accessed
- if any third party service providers are located overseas, the name of the entity and their location
- a statement that the consumer can withdraw consent at any time, and terminate the sharing of data.

The consent should not cross-reference other documents, for example by requiring consumers to click on a link to be taken to a further statement that outlines the nature of their consent.

Easy to understand

While providing information is a necessary and important part of ensuring that consumers are informed, it is often not, on its own, adequate in promoting quality consumer decision-making. The ACCC therefore proposes to makes rules requiring that consent be obtained using language and/or visual aids and a process that is concise and easy for consumers to understand. The ACCC also proposes to make rules that require, as part of the standards-setting process, consumer comprehension testing of the consent process.

Presentation

The Open Banking review recommended requiring accredited data recipients (and data holders) to display all the required information on a single screen.[87] This was to help prevent consumers from becoming disengaged or overwhelmed by the consent process. The Open Banking review found that limiting consent to one page should encourage consumers to

87 Open Banking review, recommendation 4.6.

actively participate in making decisions about the use of their data so that consent is informed and meaningful.[88]

Although recommended by the Open Banking review, the ACCC does not propose to make a rule requiring all information to be displayed on a single screen. The ACCC is not convinced presentation on a single screen will necessarily promote informed consent and meaningful engagement by consumers in and of itself. For example, there is some evidence that spreading information across multiple screens can in fact promote consumer understanding and engagement.[89] The ACCC will instead, as outlined above, make a rule requiring consent to be presented visually in accordance with design best practices, in line with guidelines established by the Data Standards Body. As noted above, consumer comprehension testing will be required as part of the standards-setting process. This will allow the development of an appropriate and targeted consent process.

Consent should be specific as to use

As outlined above, the ACCC proposes to make rules to require that an accredited data recipient must disclose, at the time of seeking the consumer's consent, the uses to which the data will be put. Uses must also be stated unambiguously, such that consumers are aware of the actual uses to which the data will be put; statements such as 'data may be used for research purposes' will not be sufficient.

The ACCC proposes to make a rule to the effect that an accredited data recipient may only use data in line with the uses to which the consumer has consented, and that if an accredited data recipient wishes to use data that it has received from a consumer for a use that was not covered in the original consent, it will be required to seek new consent. This will help ensure consent is specific as to purpose.

In addition, the ACCC proposes to make a rule that accredited data recipients should only seek consent to access the minimum data necessary for the uses agreed to. This will help ensure consent is specific as to purpose, and that consent is express and informed.

Consent should be time limited

There are two distinct issues discussed in this section. First, where an accredited data recipient obtains consent to use a consumer's data for a particular purpose, is there a limit to how long that data can be held and used by the accredited data recipient? Secondly, should there be a limit to how long a consumer's consent allowing the accredited data recipient to receive that consumer's data from the data holder should remain valid?

In relation to the first issue, privacy safeguard 11 provides that once data is no longer needed for the purposes permitted under the rules (and is not required to be kept under another law or by a court or tribunal), it is 'redundant data'. This means that once an accredited data recipient has provided the service as agreed in the consumer's consent it has no further use for the data and it becomes redundant. The ACCC is considering its approach to this issue, and welcomes stakeholder views regarding the extent to which a consumer should be able to decide whether their redundant data is de-identified or destroyed: see discussion below and section 13.

In relation to the second issue, the ACCC proposes to make a rule that would limit the period of authorisation provided to data holders to 90 days (see section 9.5 below). This is separate to the issue of how redundant data should be treated, and relates instead to placing a time limit on an accredited data recipient's ability to seek continuing access to a consumer's data (rather than one off access). This means that the consent provided to accredited data

88 Open Banking review, page 61.
89 OBIE, *How to Guide: Consent Model – Part 2: User Experience*, December 2017 (version 1.1), page 32, available at https://www.openbanking.org.uk/wp-content/uploads/Consent-Model-Part-2-User-Experience-Guide.pdf.

recipients cannot provide for a persisting right to access data from the data holder for longer than 90 days, as the accredited data recipient's right of access will automatically end at this time. This rule will help ensure that consent is time limited, and that consumers will not build up continuing consents that they no longer require.

Consent should be able to be easily withdrawn with near immediate effect

Central to providing consumers with control over their CDR data is the capacity for consumers to withdraw consent. The ACCC proposes to make a range of rules which will help provide consumers with a straightforward withdrawal process. The proposed rules include:

- a consumer may withdraw consent at any time without detriment
- the ability to withdraw consent will be no more complex than giving consent in the first place
- accredited data recipients must inform consumers how they can withdraw consent
- withdrawal of consent must be able to be effected via both the accredited data recipient and the data holder (where it is withdrawal of authorisation; see section 9.9)[90]
- if a consumer withdraws consent through the accredited data recipient, the accredited data recipient must notify the data holder and any intermediary. Similarly, if consent is withdrawn via an intermediary, it must notify the data holder and the accredited data recipient
- if a consumer withdraws consent, the consumer's data becomes redundant, whether it is held directly by the data recipient or is being stored by a contractor, see discussion above and section 13.

8.3.2. Consumer dashboard

The Open Banking review recommended that consumers be provided with the ability to access a record of their data usage history.[91]

The Government confirmed consumers should be able to keep track of their authorisations and that these records will themselves be designated data sets under the CDR.[92] The draft explanatory materials envisages that:

> *'The consumer data rules require all banks to provide convenient online access to a dashboard displaying all of the permissions the CDR consumer has granted.'*[93]

The ACCC proposes to makes rules that will require all accredited data recipients to have a system in place which allows consumers to readily manage their consents. This should allow consumers to view what they have consented to and to readily withdraw those consents if they choose.

Specifically, accredited data recipients will be required to provide a consumer facing online interface or dashboard that shows the consumer's current and historic consents provided to accredited data recipients, including:

- which datasets the consumer has provided consent to be collected and used
- when consent was obtained

90 Open Banking review, page 134.
91 Open Banking review, recommendation 5.11.
92 Consumer Data Right Booklet, p.5.
93 Draft explanatory materials, example 1.11 at paragraph 1.102.

- the period for which data was requested
- the purposes or uses for which consent was obtained
- the name of any intermediary
- when the accredited data recipient's access to the data will expire and the period for which the accredited data recipient will hold the data
- whether any consents have been revoked and, if so, when.

Data holders will be required to provide a similar consumer dashboard in relation to authorisations; see section 9.8.

8.3.3. Particular uses noted in the Open Banking review

The Open Banking review identified a range of uses of data that may require a strengthened approach to consent:

- transfer of data outside of the CDR regime
- transfer of data overseas
- on-selling of data
- direct marketing.[94]

In relation to transfer of data outside the CDR regime and transfer of data overseas, the ACCC recognises the potential risks with these uses but given the stringent rules the ACCC proposes in relation to consent under the CDR regime generally (where all uses are required to be disclosed), the ACCC considers that additional requirements will not be needed in the rules.

In relation to on-selling of data and use of CDR data for direct marketing, the ACCC's current position is that it proposes to make rules that will prohibit the use of CDR data for these purposes. The ACCC welcomes stakeholder views on this proposal.

Further requirements in relation to disclosure of data to a non-accredited recipient are discussed at section 12.1.

9. Authorisation and authentication process

Summary of proposed rules

The ACCC proposes to make rules to the effect that:

- the standards must include standards in relation to authorisation, and that authorisation processes for CDR data must occur in accordance with the standards.
- data holders must clearly communicate to consumers what they are authorising the data holder to do, and provide specified information to consumers as part of the authorisation process.
- authorisation standards must:
  - be subject to consumer testing, consideration by the Data Standards Body's user experience consultative group, and meet certain service level requirements.
  - provide for multi-factor authentication requirements consistent with the requirement for strong customer authentication under PSD2 and the European regulatory technical standard for strong consumer authentication under PSD2 (RTS).
  - provide for the ability for a consumer to grant authorisation for a specific, once-off request,

94 Open Banking review, page 60.

or authorisation that persists over time. In terms of persisting authorisations, the ACCC proposes to make a rule that will limit the period of authorisations to 90 days. The ACCC proposes to make a rule that re-authorisation will then be required if the accredited data recipient seeks continuing access to the consumer's data, though this may be via a simplified process.

    - specify permissions for applications to access data. The ACCC does not propose to specify the nature or level of 'granularity' of those permissions in the first version of the rules. However, the ACCC proposes to make a rule that the Data Standards Body continue to pursue delivery of more finely-grained authorisations.

- data holders should not add requirements to authorisation processes beyond those specified in the standards, or offer additional or alternative services to the consumer or request additional information beyond that described in the standards during and as part of the authorisation process.
- data holders must collect and maintain records and report on API performance, including response times against minimum service level benchmarks set out in the standards.
- data holders must have a system in place which allows consumers to readily manage their authorisations and consumers should be able to withdraw authorisations at any time.

The ACCC is also considering whether the rules should specify certain service level standards for the authorisation and authentication processes, or whether this is best addressed by the technical standards, and welcomes submissions on this issue.

Once consent has been granted by the consumer to the accredited data recipient – depending on authorisation models put forward by the Data Standards Body – the consumer will typically be directed to initiate an interaction with their data holder, to facilitate the sharing of data. The consumer will be asked to authenticate their identity, and to authorise the data holder to disclose data to the accredited data recipient.

Authorisation and authentication are important steps in the data sharing process. Authorisation is the process by which the consumer authorises the data holder to share data with the accredited data recipient. This authorisation should reflect the consent previously provided to the accredited data recipient by the consumer, and outline the scope of data involved and the time during which the data should be shared. Authentication is the process by which the data holder verifies the identity of the consumer directing the sharing of their data, and the identity of the accredited data recipient seeking to collect the consumer's data.

9.1.1. UK approach and Open Banking review

Appropriate authorisation and authentication processes contribute to the security of the data sharing process. The UK's Competition and Markets Authority (CMA) Retail Banking Market Investigation Order 2017 (CMA Order) specified that the Read/Write and Read-only Data Standards include provisions relating to security standards, including authorisation and authentication standards (for confidential data).[95] These are set out in the UK's Open Banking Security Standard, which uses the OAuth 2.0 authorisation framework.

The Open Banking review made a number of recommendations in relation to the authorisation and authentication aspects of the data sharing process under the Australian Open Banking model. Specifically, the Open Banking review recommended that:

- the re-direct based authorisation and authentication flow detail in the UK Open Banking technical standard should be the starting point for authorisation and authentication under the Australian model. Consideration should be given to the merits of a decoupled approach provided it minimises customer friction[96]

95 CMA Order, Article 10.2.3.
96 Open Banking review, recommendation 5.4.

- data holders may not add authorisation requirements beyond those included in the standards. Requiring multifactor authentication is a reasonable additional security measure, but it must be consistent with the authentication requirements applied in direct interactions between the data holder and its customers[97]
- customers should be able to grant persistent authorisation. They should also be able to limit the authorisation period at their discretion, revoke authorisation through the third-party service or via the data holder, and be notified periodically by the data holder that their data is being shared. All authorisations should expire after a set period[98]
- customers should be able to authorise access to transaction data in full. Accredited data recipients should not be limited to accessing pre-set functions or sending blocks of their own code to run on the system of the bank or its partner or prevented from caching data. However, participants should be free to offer services that provide more limited data to accredited data recipients who have lower levels of accreditation[99]
- data holders should, as part of the authorisation process, notify consumers that their relationship with the accredited data recipient does not involve the data holder and the sharing of data is at the consumer's own risk.[100]

Related recommendations included that:

- the Data Standards Body should determine how to limit the number of data requests that can be made[101]
- consumers should be able to access a record of their usage history and data holders should keep records of the performance of their API that can be supplied to the regulator as needed.[102]

9.2. ACCC approach to rule-making on these topics

The ACCC proposes to make rules in relation to aspects of the authorisation and authentication processes, including to give effect to recommendations from the Open Banking review. This is because the ACCC recognises the importance of these processes to the overall CDR regime, both in the sense of ensuring the security of data sharing, and in ensuring a satisfactory consumer experience. Further, there is a tension between these considerations, such that high level authorisation/authentication requirements that ensure security may add friction to the user experience, and vice versa. The rules are therefore a means by which direction can be given on where to strike the balance. The ACCC is also concerned to ensure that authorisation and/or authentication processes are not used by data holders to deliberately obstruct or frustrate the ability of consumers to make use of the CDR.

The ACCC recognises that many aspects of the authorisation and authentication processes will be appropriately addressed by the technical standards. Further, this is an area of the standards that is likely to develop over time. As a result, the ACCC is conscious of not making rules that are counter-productive to the standards development process, or that may impede technological developments that deliver good outcomes for consumers.

In setting parameters the ACCC nonetheless considers that the balance should be weighted towards ensuring a high degree of security for the CDR regime. The ACCC accepts that

97 Open Banking review, recommendation 5.5. The ACCC interprets this recommendation to mean that multi-factor authentication could be permitted in the standards.
98 Open Banking review, recommendation 5.6.
99 Open Banking review, recommendation 5.7.
100 Open Banking review, recommendation 4.6.
101 Open Banking review, recommendation 5.10.
102 Open Banking review, recommendation 5.11.

taking this approach will add friction to the user experience, but considers this friction should be within acceptable bounds.

9.3. General obligations

The role of data holders in the authorisation process is to ensure the content of the authorisation reflects the scope of the consent previously provided to the accredited data recipient by the consumer, to uphold that consent (by not challenging it or seeking to amend it), and to allow consumers to deny authorisation.

9.3.1. Authorisation in accordance with technical standards

The ACCC proposes to make rules that the technical standards must include standards in relation to authorisation, and that authorisation processes for CDR data must occur in accordance with the standards. Relatedly, the ACCC proposes to make a rule that data holders must not add requirements to authorisation processes beyond those specified in the standards. These rules will contribute to ensuring a consistent approach to authorisation in the CDR regime, and a consistent experience for consumers. In particular, the rule that data holders must not add additional requirements for authorisation is intended to protect against attempts to discourage consumers from using the CDR by means of obstructive or 'user unfriendly' processes.

9.3.2. Notification to the consumer

The ACCC proposes to make rules to the effect that data holders must clearly communicate to consumers what they are authorising the data holder to do. For example, the ACCC proposes to make a rule that requires data holders to provide specified information to consumers as part of the authorisation process. This will help ensure that authorisation is express and informed.

The authorisation request from the data holder may be required to include information such as:

- the name of the accredited data recipient that requested the data and, if relevant, the name of the accredited intermediary to which the data will be transferred, in line with the consent provided to the accredited data recipient by the consumer
- the data that has been requested
- the period over which the transaction data has been requested
- when the accredited data recipient's, and, where applicable, an accredited intermediary's, access to the data will expire
- the details of the account(s) to which access will be authorised
- for transaction data, the period over which the transaction history has been requested.

9.3.3. Consumer testing

The ACCC also proposes to make rules that the authorisation standards are subject to consumer testing, consideration by the Data Standards Body's user experience consultative group, and meet certain service level requirements/non-functional requirements. These rules are intended to ensure that the authorisation standards support appropriate consumer outcomes and experiences.

9.4. Authorisation and authentication model

The ACCC understands that there are different authorisation models, and that during the Open Banking review, submissions were made regarding the attributes and appropriateness of these models for Open Banking and the CDR. The UK Open Banking framework uses a re-direct model based on the OAuth 2.0 framework, which itself is widely used by applications. The Open Banking review ultimately recommended that the re-direct based authorisation and authentication flow in the UK Open Banking technical standard be the starting point for authorisation and authentication under the Australian model. The recommendation also stated that consideration should be given to the merits of a decoupled approach provided it minimises customer friction.[103]

In the UK, the CMA Order requires that the security standards include standards on authentication, but does not mandate a method of authentication. Under PSD2 there is a requirement that a payment service provider applies 'strong customer authentication' where a payer accesses a payment account online; initiates an electronic payment transaction; or carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.[104] The RTS developed by the European Commission are due to take effect in September 2019.

The ACCC proposes to make a rule that requires an authorisation flow that meets the requirements of strong customer authentication under the PSD2 and the RTS. This could take the form of a re-direct flow with multi-factor authentication. While this goes beyond the recommendation of the Open Banking review, the ACCC is concerned to ensure that the CDR regime is trusted and secure, and therefore considers that a higher degree of security is required than can be provided under a simple re-direct model. The ACCC understands that the RTS allow for further development and innovation to protect against emerging security risks, and therefore does not consider that adopting those standards would unacceptably constrain the development of technical standards for Open Banking or the CDR.

The ACCC does not consider it necessary at this point to otherwise mandate a particular authorisation model, recognising that it is preferable for the standards development process to consider authorisation models, and how those models manage security risks and impact on consumer experience. Taking this approach is also consistent with recommendation 5.4 of the Open Banking review. The proposed rules around consumer testing, consideration by a user experience consultative group, and the need to meet service level standards, should help to ensure that any alternative models also deliver good outcomes for consumers.

9.5. Duration of authorisation

The ACCC proposes to make rules to the effect that consumers may grant authorisation for a specific, one-off request, or may grant authorisation that persists over time. In terms of persisting authorisations, the ACCC proposes to make a rule that will limit the period of authorisations to 90 days, consistent with EU requirements under the PSD2 that also limit the period of authorisation to 90 days.

The ACCC proposes to make a rule that re-authorisation will then be required if the accredited data recipient seeks continuing access to the consumer's data. The re-authorisation may be a simplified version of the process initially undertaken to authorise the data holder to share the data (while still requiring strong consumer authentication). Again, the ACCC's expectation is that the re-authorisation process should not add undue friction to the user experience. Re-authorisation processes should therefore be included in the

103 Open Banking review, recommendation 5.4.
104 PSD2, article 97(1).

authorisation standards, which participants must comply with. Those standards would also be subject to user-testing as outlined previously.

9.6. Granularity of authorisation

The ACCC proposes to make a rule to the effect that the authorisation standards specify permissions for applications to access data. This will allow consumers more control over exactly what data they consent to share. It will also ensure that the data that the consumer has consented to the data recipient obtaining is the same data that the data holder provides to the data recipient. The specification of the permissions, and their relevant descriptions, should be undertaken by the Data Standards Body. Data holders and data recipients would be required to comply with this specification per the general rule to comply with the standards.

A related issue is the degree of 'granularity' of the authorisation. Recognising that these terms have technical meanings, the ACCC understands that 'coarse-grained' authorisation connotes granting access to a broad data set, whereas 'fine-grained' authorisation connotes granting access to a more limited or filtered data set. An example of a coarse-grained authorisation would be granting access to transactions within a specified date range. An example of a fine-grained authorisation may be granting access to transactions within a specified date range, above a specified value, and with a specified counter-party.

Fine-grained authorisations may enable more nuanced services to be provided to consumers. More fine-grained authorisations would also be consistent with a data minimisation principle, helping to ensure that only the most relevant data is shared with an accredited data recipient. However, the ACCC understands that there may be technical challenges associated with delivering 'fine-grained' authorisations, at least for the time being. It is therefore appropriate that the level of granularity of authorisation be addressed through the standards development process.

The ACCC consequently proposes to make a rule that the Data Standards Body, as part of the standards development process, continue to pursue delivery of more finely-grained authorisations. The initial degree of granularity of authorisation in the technical standards is thus a matter for the Data Standards Body, but with an expectation that more finely-grained authorisation will be developed over time. It may also be the case that in the short-term some service providers offer 'intermediary' services where they collect data pursuant to a coarse-grained authorisation, and then provide data to another accredited data recipient at a finer degree of granularity.

The ACCC also intends to ensure that the data that the consumer has consented to share with the accredited data recipient, is the same data that the data holder provides to the accredited data recipient. The specification of the permissions, and their relevant descriptions, should be undertaken by the Data Standards Body.

9.7. Minimising friction in the authorisation process

The ACCC also proposes to make rules which will help to ensure minimal consumer friction in the authorisation process.

Some degree of friction is inevitable to ensure that the consumer is fully informed of their choices. However, the purpose of requiring the data holder to notify and obtain authorisation to share data is to maintain consumer control, not provide an opportunity for the data holder to potentially discourage the consumer from using the accredited data recipient's services.

Proposed rules include:

- data holders must not add requirements to authorisation processes beyond those specified in the standards, including:
    - data holders should not offer additional or alternative services to the consumer during and as part of the authorisation process
    - data holders must not request additional information beyond what is described in the rules or standards as necessary to authenticate the consumer and the consent they have agreed with the accredited data recipient. For example, it is unnecessary for data holders to request information about the arrangements with the accredited data recipient or the purpose for which the data can be used.

The ACCC also proposes to make rules which require data holders to collect and maintain records and report on API performance, including response times against minimum service level benchmarks set out in the standards. See further discussion of record keeping obligations on data holders below in section 14.2. The ACCC is also considering whether the rules should specify certain service level standards for the authorisation and authentication processes, or whether this is best addressed by the technical standards. The ACCC welcomes submissions on appropriate service level standards for inclusion, and whether they should be specified in the rules.

9.8. Consumer dashboard

The ACCC proposes to make rules that will require all data holders, like accredited data recipients (see 8.3.2 above) to have a system in place which allows consumers to readily manage their authorisations easily. This should allow consumers to view what they have provided authorisation to and to easily withdraw authorisation if they choose. This could be done via a consumer's online banking portal.

Specifically, data holders will be required to provide a consumer facing online interface or dashboard that shows the consumer's current and historic authorisations to share their data, provided to the data holder, which shows:

- which datasets the consumer has authorised be shared
- when authorisation was given
- who authorisation was given to, including any intermediary
- how long authorisation was provided for
- whether any authorisations have been revoked and, if so, when.

The consumer dashboard could also be used as the facility provided for consumers to revoke authorisations (see section 9.9).

9.9. Revocation of authorisation

The ACCC proposes to make a range of rules to help provide consumers with a straightforward process for withdrawing consents provided to accredited data recipients (see section 8.3.1) and/or for revoking corresponding authorisations provided to data holders. Consumers will be able to end a data sharing arrangement through either the data holder or accredited data recipient.

The ACCC proposes to make a rule that a data holder must remove an authorisation if requested by the consumer, and a consumer can do so at any time.

Other proposed rules in relation to the revocation of authorisations provided to data holders include:

- if a consumer revokes an authorisation via the data holder, the data holder must notify the accredited data recipient and any intermediary
- data holders must have a system in place which allows consumers to readily revoke their authorisations, for example via a consumer dashboard (see further discussion of the consumer dashboard above in section 9.8)
- the ability to revoke authorisation should be as simple as giving authorisation in the first place.

10. Providing consumer data to consumers

Summary of proposed rules

The ACCC proposes to make rules that require data holders to:

- provide consumers with the ability to make requests for direct disclosure of their CDR data in a manner that is timely, efficient and convenient.
- allow consumers to nominate specific CDR data as part of their request, consistent with the data standards that will specify the product descriptions and information taxonomy.
- disclose the requested CDR data to the consumer in a variety of electronic formats, as provided for by the Data Standards Body, potentially at the election of the consumer.

The ACCC welcomes views about the specific rights and obligations that should be imposed to give effect to the right for a consumer to directly access their CDR data from a data holder.

One of the objects of the CDR regime, and a core right given to consumers in the draft legislation,[105] is to enable a consumer to require a company holding designated data relating to that consumer to provide that data direct to the consumer. This is complementary to the object of enabling consumers to require that this kind of information be transferred to accredited data recipients. The draft explanatory materials envisages that the manner in which the data is made available to the consumer directly, as well as to accredited data recipients, will be established by the rules and the standards.[106]

The ACCC proposes to make rules specifying the key requirements for consumers to make valid requests for direct access to their CDR data and the obligations of data holders in responding to such requests. Providing CDR data direct to a consumer should be less complex for data holders than transferring it to an accredited data recipient. It is important that it is easy for a consumer to initiate such a request, that data be shared in a timely way, and that data be shared in formats that are readily useable by consumers. The ACCC envisages that the rules will permit flexibility in the manner in which direct access to the CDR data is to be provided. It is also likely to be appropriate to allow for the CDR data to be provided in a variety of formats; potentially at the election of the consumer. The detail of these obligations will be set out between the rules and the standards, and the ACCC expects that the Data Standards Body will develop mechanisms that facilitate direct consumer access

The ACCC seeks views about the specific rights and obligations that should be imposed in the rules and standards to give effect to the core right for a consumer to directly access their CDR data from a data holder.

At a high level, the ACCC proposes to make rules that would require data holders to:

- provide consumers with the ability to make requests for direct disclosure of their CDR data in a manner that is timely, efficient and convenient. Likely minimum requirements are that:

105 Draft legislation, section 56AA(a)(i).
106 Draft explanatory materials, paragraph 1.25.

a) if the data holder provides an online mechanism (whether web or application based) to allow customers to perform actions on an account, the data holder must allow customers to make requests for access to their CDR data via that mechanism

b) the data holder must also allow consumers to access CDR data via an open API

- allow consumers to nominate specific CDR data as part of their request, consistent with the data standards to be made by the Data Standards Body that will specify the product descriptions and information taxonomy
- disclose the requested CDR data to the consumer in an electronic format. As noted above, the ACCC expects that the Data Standards Body will develop mechanisms that facilitate direct access to CDR data by consumers, including the formats in which data may be provided.

11. Making generic product data generally available

Summary of proposed rules

The ACCC proposes to make rules that will require data holders to make generic product data available via an API in accordance with standards made by the Data Standards Body.

The Open Banking review recommended that where banks are under an existing obligation to disclose information on their products and services (such as information on their price, fees and other charges), that information should be made publicly available under Open Banking.[107] The government contemplated that this information would be made available in machine-readable form, and that this would support comparison services.[108] In the UK, access to this kind of information is required via open APIs.[109]

The draft legislation provides for the rules to specify various requirements in relation to CDR data for which there are no CDR consumers, including requirements on a CDR participant in relation to disclosure of all or part of this type of data upon receiving a valid request from a person seeking to access this kind of data and how a valid request can be made.[110] The data that will be subject to this obligation in the first version of the rules is discussed at paragraph 5.3.3 above.

The ACCC proposes to make rules that will require data holders to make this data available via an API in accordance with standards made by the Data Standards Body. The standards will determine the format in which this information is to be made available, and the related data taxonomies, to ensure a standardised approach. Third parties will not need to be accredited to receive this information and as such there will be no requirement for data holders to verify the identity of the third party as part of the disclosure process.

12. Use of data

Summary of proposed rules

The ACCC proposes to make a rule requiring accredited data recipients to identify to a consumer the uses to which the consumer's CDR data can be put, and obtain express consent to specific uses according to the consumer's wishes.

The ACCC proposes to make a rule requiring that CDR data can only be used in accordance with the consumer's express wishes, as governed by the consent process.

The ACCC proposes to make rules requiring accredited data recipients to transfer data to a non-

107 Open Banking review, recommendation 3.6.
108 Consumer Data Right Booklet, page 4.
109 CMA Order, Articles 10.2 and 12.
110 Draft legislation, section 56BD.

accredited entity if directed by a consumer and with their specific express consent, after notifying the consumer that the entity is not accredited and disclosure is outside the protections of the CDR system.

The ACCC proposes to make rules which would allow an accredited data recipient to disclose data to an outsourced service provider, provided the outsourcing arrangement is disclosed to consumers during the consent process and other obligations relating to outsourcing are complied with. The ACCC is also considering other rules in relation to this scenario to limit the increased risk to consumers' data, and welcomes stakeholder views on this issue.

The ACCC welcomes stakeholder comment on a model based on use of an intermediary, to assist in determining to what extent the utility of the CDR would be limited without the ability to operate in this way.

The Open Banking review provided for a general freedom of use for any lawful use. The Government supported this approach, proposing to leave consumers free to determine what their data is used for, allowing for self-selection by consumers of agreed uses. It did not propose that consumers would be prohibited from granting consent to any lawful use, but acknowledged that additional use restrictions or regulation can be imposed if this becomes necessary.[111]

When initiating a CDR data sharing arrangement a consumer is in control of the uses to which their data is put. As provided for in the consent process, the ACCC proposes to make a rule requiring accredited data recipients to identify to a consumer the uses to which the consumer's CDR data can be put, and obtain express consent to specific uses according to the consumer's wishes.

Further, the ACCC proposes to make a rule requiring that CDR data, once accessed or held by an accredited data recipient (or an accredited intermediary), can only be used in accordance with the consumer's express wishes, as governed by the consent process. A consumer should never be surprised by the way in which their data has been used by an accredited data recipient (see section 8).

12.1. Disclosure of consumer data to other parties

The CDR places the value of consumer data in the hands of the consumer, providing a system in which consumers can safely and securely direct their data be disclosed to accredited data recipients for specified uses. The Open Banking review and the government's announcement of the CDR were very clear about the importance of CDR data being disclosed to trusted users that are subject to a range enhanced privacy, security and other obligations. The success of the CDR regime will depend on consumer trust in the protections provided within the system.

The proposed rules outlined throughout this rules framework focus primarily on a simplified model whereby a consumer initiates a data sharing arrangement with a single accredited data recipient, which – after the consent process – receives the consumer's CDR data for the uses specified by the consumer. This model incorporates many of the Open Banking review's numerous recommendations for ensuring a safe and secure system of data sharing to accredited data recipients.

The ACCC is aware that not all applications of the CDR will fit within this model. The ACCC understands there are circumstances in which it may be desirable for CDR data to be disclosed to a non-accredited entity, or an entity other than the accredited data recipient with which a consumer initiates a data sharing arrangement – three such scenarios are outlined below. In the first scenario the consumer's data would 'leave' the CDR system and would therefore not be covered by the protections it provides. In the second and third scenarios the

111 Consumer Data Right Booklet, page 6.

consumer data would not 'leave' the CDR system, and the protection provided for CDR data would continue to apply.

The Open Banking review and the draft legislation both contemplate an ability to disclose data to parties other than accredited data recipients, although the Open Banking review did not examine the significance or consequences of such an ability in great detail.

The ability to disclose data outside the CDR regime or to entities which are not accredited is a challenging issue. A balance must be stuck between the protections provided for within the system and its ultimate usefulness.

The ACCC appreciates the need for strong privacy and security protection of CDR data disclosures. The ACCC recognises that the risks of data breaches can increase in line with greater access to data. Consumers need to trust the CDR regime and the protections it provides, particularly those that protect the security and privacy of consumer data.

However, the ACCC also recognises that there may be legitimate reasons for data to be disclosed to non-accredited entities, and that by doing so the security, practicality and utility of the CDR to consumers may be increased. Certain applications of CDR data may depend on the ability to disclose to non-accredited entities, and if the CDR regime does not allow this to occur these applications will be unavailable to consumers, limiting the value of the CDR. A prohibition on disclosure of data to other entities is also at odds with the CDR's strong focus on consumer choice and freedom.

This is a challenging issue that impacts on several other key concepts including reciprocity, accreditation, liability, consumer consent, authorisation and authentication. It is an issue which requires further exploration and the ACCC invites stakeholder views on the possible approaches which are outlined below. These solutions are classified according to three instances identified by stakeholders as likely common scenarios.

12.1.1. To a specified entity as directed by the consumer

The ACCC recognises that there will be instances where a consumer wishes to have their CDR data disclosed to a non-accredited entity. For example, a consumer might want to have their data disclosed to their accountant to assist in the preparation of their tax return. Such instances should be facilitated by the CDR regime, recognising that consumers should be free to direct that their own data be shared with non-accredited entities for specific purposes as they wish.

The ACCC proposes to make rules requiring accredited data recipients to transfer data to a non-accredited entity if directed by a consumer and with their specific express consent. This is a situation where CDR data has been shared by a data holder with an accredited recipient, and the consumer is now directing that accredited recipient to share the data with a non-accredited recipient. The ACCC is not proposing to make rules that would permit the sharing of CDR data from a data holder to a non-accredited recipient.

As the consumer is directing that their data be disclosed to a non-accredited entity, the consumer's data will leave the CDR system and the CDR protections will no longer apply. The accredited data recipient is not liable for misuse once the data is transferred. The CDR protections will not apply, however the Privacy Act and the APPs may apply where applicable, although the Privacy Act will not apply to all third party recipients outside the CDR system.

A further rule would require that the accredited data recipient must notify the consumer that:

- the entity they are sending their data to is not accredited under the CDR and therefore the CDR protections no longer apply

- the non-accredited entity's handling of their data may be covered by the Privacy Act
- disclosure is at the consumer's own risk.

12.1.2. To an outsourced service provider of the data recipient for a specified use

The ACCC understands that the utility of the CDR may be limited without CDR data being shared with non-accredited outsourced service providers of an accredited data recipient. Such outsourced service providers may add value to the accredited data recipient's service, or may provide a part of the service which the accredited data recipient is not themselves able to perform. Outsourced service providers may include a storage provider or an advisor. While the accredited data recipient would provide the primary service to the consumer, and will be the party with which the consumer contracts, it may utilise an outsourced service provider to assist in doing so.

The ACCC proposes to allow an accredited data recipient to disclose CDR data to an outsourced service provider, even though the outsourced provider may not be accredited, with appropriate additional protections in place including the requirement that these arrangements are disclosed to consumers during the consent process and other obligations relating to outsourcing (see paragraph 6.8).

Whereas in the first scenario above in section 12.1.1, the CDR data is disclosed to a non-accredited entity of the consumer's choice, in this scenario data may be disclosed to a non-accredited outsourced provider that does not have a direct relationship with the consumer but assists the accredited data recipient in supplying services to the consumer. Also, in this scenario the consumer's CDR protections apply as normal and their data will not 'leave' the CDR system, as it will in the first scenario.

Under this scenario the accredited data recipient remains liable for all CDR obligations they owe to their consumers, including those aspects that may be undertaken by an outsourced service provider. The accredited data recipient is responsible for the actions of any outsourced service providers they use. Accredited data recipients that outsource their services to other non-accredited entities will have an obligation to ensure that they have sufficient policies and processes in place for appropriately managing all risks arising from that outsourcing arrangement and evidence of this will be required as part of the accreditation process (see section 6).

As provided for in section 8, the accredited data recipient must disclose to its consumers whether it uses or intends to use outsourced service providers and the nature of their services, including the specific reasons for which they will share consumer data with these providers. It must also maintain a list of its outsourced service providers, and the nature of their services, in its policy about the management of CDR data (see section 13).

Outsourced service providers must operate within the bounds of the consent provided by the consumer to the accredited data recipient; they will have no opportunity to use data in any way other than for the uses to which the consumer originally agreed. Accredited data recipients are responsible for ensuring outsourced service providers meet these obligations.

As outlined in section 14, accredited data recipients must maintain records of any outsourced service providers they use, the data that has been disclosed to them, and the nature of the services provided in relation to that data.

The ACCC is considering rules in relation to this scenario to limit the increased risk to consumers' data. This could include to allow data to be disclosed to an outsourced service provider once removed from the accredited data recipient but not to any further non-

accredited entity (this will prevent subcontracting arrangements involving disclosure of the CDR data by a non-accredited outsourced provider).

12.1.3. To an intermediary through whom the data passes on its way to the data recipient

The ACCC understands that one proposed alternative model for the operation of a CDR arrangement is use of an intermediary. For example, an accredited data recipient may offer its services to and directly interact with its consumers but rely on an intermediary to directly receive CDR data in the first instance, that is, the intermediary would be the entity calling the API and receiving data from the data holder.

While the second scenario above in section 12.1.2 involves an accredited data recipient directly receiving CDR data by calling the API then outsourcing parts of its service to its own outsourced providers, the intermediary model relies on an intermediary, while not necessarily interacting with the customer directly, receiving CDR data and passing it (or a subset of it) on to the accredited data recipient. This could, to the extent that a tiered system of accreditation is ultimately adopted (see section 6), allow smaller accredited data recipients to qualify for a lower level of accreditation by relying on the stronger security and privacy protections provided by an intermediary accredited to a higher level.

As an intermediary would directly participate in the disclosure process flow it would need to be accredited should this model be provided for in the rules. Without accreditation an intermediary would not be listed in the Register and would therefore not be able to access a data holder's API. These technicalities notwithstanding, the ACCC considers it appropriate that the primary collector of a consumer's CDR data be accredited in every case.

Like in scenario two, the CDR protections would continue to apply and the consumer's data will not 'leave' the CDR system, as the intermediary and the accredited data recipient would both be accredited entities subject to CDR obligations. This model may also allow for CDR data to be processed within the environment of the intermediary, and for the accredited data recipient to obtain insights from the data without ever 'seeing' or storing the data. In such a situation it may be appropriate for the accredited data recipient to hold a lower level of accreditation.

This is a complex issue which would have significant impacts on the consent, authorisation and authentication processes in particular, and would require careful development as part of the standards-setting process. The ACCC welcomes stakeholder comment on this issue, to assist in determining to what extent the utility of the CDR would be limited without the ability to operate in this way. The Open Banking review and government response both clearly emphasised that the CDR should be flexible enough to allow the development of alternative business models, and the ACCC supports this to the extent that it does not significantly impact on the security or privacy of consumers' data.

13. Rules in relation to privacy safeguards

Summary of proposed rules

A number of proposed rules in other sections of this framework will build upon and give effect to the privacy safeguards. For instance, rules in relation to consent, authorisation and use of CDR data will give effect to privacy safeguards on data collection, use and disclosure, and notification.

The ACCC also proposes:

- in relation to privacy safeguard 1, to make rules to the effect that the CDR participant must make the policy about its management of CDR data available via its website and mobile app, in a readily accessible location and provide a copy of the policy to consumers electronically or in hard copy if requested.

- in relation to privacy safeguard 2, to make rules to the effect that the use of a pseudonym by a consumer is prohibited for Open Banking.
- in relation to privacy safeguard 9, to not make rules to provide exceptions to the prohibitions relating to government related identifiers (GRI) in the initial version of the rules.
- in relation to privacy safeguard 10, to not make rules in relation to the quality and accuracy of data in the initial version of the rules.
- in relation to privacy safeguard 13, to make rules to the effect that the steps the relevant persons should take should be in accordance with the steps outlined by the OAIC in relation to APP 13.

In relation to privacy safeguard 4, the ACCC welcomes stakeholder views on scenarios that may need recognition in the rules in relation to unsolicited data.

The Open Banking review emphasised the importance of safeguards to inspire confidence in Open Banking, and recommended modifications to the APPs to provide increased protections.[112] The draft legislation includes 12 'privacy safeguards'. These safeguards are based on the APPs and seek to impose a minimum level of privacy protection for the CDR regime. They impose obligations in relation to certain CDR data and must be met by either data holders, accredited data recipients, or both. In a number of instances the safeguards contemplate that the rules will provide further detail on how the safeguard is to be given effect. The ACCC therefore proposes to make rules to give effect to the relevant safeguards.

Safeguard 1: Open and transparent management of data

This safeguard requires that a CDR participant take reasonable steps in the circumstances to implement practices, procedures and systems that:

- will ensure that the CDR participant complies with the privacy safeguards and the rules
- will enable the CDR participant to deal with inquiries or complaints from a CDR consumer for CDR data about the CDR participant's compliance with this part or the rules.

The safeguard also requires that the CDR participant have a clearly expressed and up to date policy about the CDR participant's management of CDR data, which must include at least the following specified items:[113]

- the classes of CDR data held by or on behalf of the participant
- the purpose for which the participant obtains, uses and discloses the CDR data
- how a consumer may access and correct the CDR data
- how a consumer may complain about non-compliance with the privacy safeguards or other CDR rules
- whether the participant might disclose CDR data with accredited persons overseas
- if the participant might disclose CDR data to accredited persons overseas - the countries in which they are based.

In addition to these items, the ACCC may require the policy about the CDR participants' management of CDR data to include other items, for example, a list of its outsourced service providers, the nature of their services and the data that has been disclosed to them (see sections 6.8 and 12.1.2).

112 Open Banking review, recommendation 4.2.
113 Draft legislation, section 56ED(4), (5).

The CDR participant must make the policy available free of charge and in accordance with the rules, and if a copy of the policy is requested by a CDR consumer for CDR data, the CDR participant must give a copy in accordance with the rules.

The ACCC proposes to make rules to the effect that the CDR participant must:

- make the relevant policy available on its website and mobile app, in a readily accessible location
- in response to a request from a relevant consumer, provide a copy of the policy to that consumer electronically or in hard copy.

The policy should be consumer tested for comprehension to ensure that it is easy to understand and is drafted in a way which promotes consumer engagement.

Safeguard 2: Anonymity and pseudonymity

Privacy safeguard 2 provides that a CDR participant that has been requested to disclose CDR data, or is an accredited data recipient, must give the consumer the option of anonymity, or of using a pseudonym, when dealing with the CDR participant in relation to the CDR data.[114] This requirement does not however apply in the circumstances specified in the rules.[115]

The draft explanatory materials states that it is expected that the rules in relation to Open Banking will prohibit the use of a pseudonym in this sector, and the ACCC proposes to make rules to this effect.

Safeguard 3: Collecting solicited CDR data

Privacy safeguard 3 provides that an accredited data recipient must not collect CDR data by soliciting it unless it collects the CDR data as a result of a disclosure under the rules in response to a valid request from a CDR consumer for the CDR data.[116] An exception is provided where the collection of the CDR data is required or authorised by an Australian law (other than the Privacy Act or APPs), or a court/tribunal order.[117]

The ACCC proposes to make rules to the effect that disclosure of the information discussed in section 8.3 above, which is the disclosure required at the time at which the accredited data recipient obtains the consumer's consent to collect and use the CDR data, is the relevant disclosure required for this safeguard.

Safeguard 4: Dealing with unsolicited CDR data

Privacy safeguard 4 provides that where an accredited data recipient receives but did not solicit CDR data (and is not required to retain the data by reason of an Australian law (other than the Privacy Act or APPs), or a court or tribunal order), it must destroy the CDR data as soon as practicable.

The ACCC recognises that there may be a need for rules to give further details on what constitutes 'as soon as practicable', especially for particular scenarios. For instance, under an intermediary model, it may be the case that an accredited intermediary receives data on behalf of an ultimate recipient (who would also be accredited). That intermediary recipient may not have solicited the data (the ultimate recipient would have instead solicited the data), but may need to retain the data for a period in order that the ultimate recipient can provide the relevant service to the consumer. This could be exacerbated in situations where the

114 Draft legislation, section 56EE(1),
115 Draft legislation, section 56EE(2).
116 Draft legislation, section 56EF(1).
117 Draft legislation, section 56EF(2).

accredited intermediary obtains a 'coarser grained' data set than is needed by the ultimate recipient to provide the service to the consumer. This could occur because, as discussed in section 9, it may take time to enable fine-grained authorisations, and in the interim an intermediary may wish to assume the risk of holding coarser grained data sets and provide filtered data at a finer level to other recipients who wish to assume less risk.

The ACCC welcomes stakeholder's views on these scenarios, or any others, that may need recognition in the rules in relation to this privacy safeguard.

Safeguard 5: Notifying the collection of CDR data

Privacy safeguard 5 provides that if an accredited data recipient collects solicited CDR data,[118] the person must notify each CDR consumer for the CDR data of that collection, in accordance with the rules, and ensure that the notification covers matters specified in the rules and is given at the time specified in the rules.

The ACCC proposes to make rules to the effect that the requirements of this safeguard will be met if an accredited data recipient provides the notifications discussed in section 8.3 at the time of obtaining the consumer's consent to collecting and using the data.

Safeguard 6: Use or disclosure of the CDR data

Privacy safeguard 6 imposes obligations on both data holders and accredited data recipients.

In relation to data holders, the safeguard provides that if a consumer has given a data holder a request under the rules for the CDR data to be disclosed under those rules, then the data holder must not disclose the CDR data, or any CDR data associated with it, unless:

- the disclosure is required or authorised under the rules
- the disclosure is required or authorised under Australian law (other than the Privacy Act or APPs) or court/tribunal order, and the person makes a written note of the disclosure.

The ACCC proposes to make rules to the effect that disclosure in accordance with the matters set out in sections 8 and 9 is authorised disclosure for the purposes of this safeguard. This will ensure that disclosure may only occur where it is done in accordance with the requirements around consent, authorisation and authentication as set out in the CDR rules.

The ACCC also proposes to make rules to the effect that disclosure of the CDR data by a data holder directly to the consumer, as discussed in section 10, is also authorised disclosure for the purposes of this safeguard.

The safeguard imposes similar obligations on an accredited data recipient in relation to the disclosure or use of CDR data. The safeguard provides that an accredited data recipient that collects CDR data must not use or disclose it, or any CDR data associated with it, unless:[119]

- the use or disclosure is: (a) in accordance with a valid consent received, in accordance with the rules, from a CDR consumer for CDR data; and (b) is required or authorised under the rules
- the use or disclosure is required or authorised by Australian law (except the Privacy Act or the APPs) or a court/ tribunal order, and the person makes a written note of the disclosure.[120]

118 In accordance with section 56EF of the draft legislation.
119 In accordance with section 56EF of the draft legislation.
120 This obligation does not apply for the purposes of direct marketing, which is addressed by the following safeguard.

The ACCC proposes to make rules to the effect that the use or disclosure of CDR data, by an accredited data recipient, in accordance with the matters specified in sections 8, 9 and 12 is authorised use or disclosure for the purposes of this safeguard. Similarly, valid consent will be consent that meets the requirements outlined in section 8. This will ensure that use or disclosure of the data by an accredited data recipient may only occur where it is done in accordance with the requirements around consent, authorisation, authentication and use set out in the rules.

Safeguard 7: Use or disclosure of CDR data for direct marketing

Privacy safeguard 7 in essence prohibits an accredited data recipient from using CDR data for direct marketing unless a valid consent has been obtained, in accordance with the CDR rules, and the use for direct marketing is also in accordance with the CDR rules.

The ACCC proposes to make rules prohibiting the use CDR data for direct marketing; see section 8.3.3.

Safeguard 8: Cross-border disclosure of CDR data

Privacy safeguard 8 in essence provides that if a proposed disclosure of CDR data would be to someone who is not the consumer or is not in Australia or an external territory, then the disclosure must not happen unless:

- the person to whom the data is to be disclosed is an accredited data recipient, or
- the relevant conditions in the rules are met.

As outlined in section 8 on consent, the ACCC proposes to make rules to the effect that disclosure of data overseas must be identified as a specific use of the data at the time the consumer provides their consent. The ACCC also proposes to make rules that enable an accredited data recipient to share data with an outsourced service provider, provided a range of conditions are met (see sections 6.8 and 12.1.2). In this scenario the outsourced service provider may be based overseas, which the accredited data recipient would have to disclose to the consumer and obtain the consumer's specific consent to sharing the data with that party. The ACCC proposes to make rules to ensure that these requirements are authorised for the purposes of privacy safeguard 8.

Safeguard 9: Adoption or disclosure of government related identifiers

Privacy safeguard 9 applies in relation to a data holder that has been requested via the rules to disclose data, and to an accredited data recipient, where CDR data (or data associated with the CDR data) includes a GRI within the meaning of the Privacy Act. A GRI of an individual means an identifier of the individual that has been assigned by:

- an agency
- a State or Territory authority
- an agent of an agency, or a State or Territory authority, acting in its capacity as agent
- a contracted service provider for a Commonwealth contract, or a State contract, acting in its capacity as contracted service provider for that contract.[121]

The safeguard in essence prohibits the data holder or accredited data recipient, as the case may be, from adopting the GRI as their own, or disclosing the GRI as part of the disclosure of CDR data. The safeguard recognises that the rules may provide exceptions to these prohibitions.

121 Privacy Act, section 6.

The ACCC does not propose to make rules at this stage to provide any exceptions to these prohibitions.

Safeguard 10: Quality of CDR data

Privacy safeguard 10 provides that a CDR participant for CDR data must take reasonable steps to ensure that the CDR data is, having regard to the purpose for which it is held, accurate, up-to-date and complete when the CDR participant discloses the CDR data.[122]

This safeguard also provides that if a CDR participant for CDR data discloses the CDR data[123] and later would reasonably be expected to become aware that some or all of the CDR data was incorrect because, having regard to the purpose for which it was held, it was inaccurate, out of date, incomplete or irrelevant, the CDR participant must advise each CDR consumer for the CDR data accordingly, and in writing.[124] Further, if the CDR consumer is so advised, and requests the CDR participant to disclose the corrected CDR data to the recipient of that earlier disclosure, then the CDR participant must comply.[125]

The ACCC does not propose to make any rules in relation to safeguard 10 in the first version of the rules.

Safeguard 11: Security of CDR data

Privacy safeguard 11 provides that if an accredited data recipient collects CDR data in accordance with safeguard 3 (that is, the person has solicited the CDR data), the person must take the steps specified in the rules to protect the CDR data, and any CDR data associated with the CDR data, from:

- misuse, interference and loss
- unauthorised access, modification or disclosure.[126]

The ACCC proposes to make rules to the effect that data be treated in accordance with the continuing security requirements outlined in section 6.9. The ACCC also notes that the OAIC has published guidelines on how the equivalent obligation under the APPs (APP 11) is to be met.

The safeguard also provides that if a person collects CDR data in accordance with safeguard 3, and any of the CDR data, or CDR data associated with the CDR data, is no longer needed for the purposes permitted under the rules or under the CCA, or the person is not required by or under any Australia law (except the APPs) or court/tribunal order to retain the data, the person must take the steps specified in the rules to destroy that 'redundant data' or ensure that the redundant data is de-identified.[127]

As outlined in section 8 on consent, the ACCC proposes to make rules to the effect that data should only be kept by an accredited data recipient for as long as is necessary to provide the uses consented to by the consumer.

The ACCC is considering the issue of how redundant data should be dealt with. While the Open Banking review did not recommend a right of deletion, allowing accredited data recipients the ability to retain consumers' data at their discretion, albeit de-identified, may not be consistent with the consumer-centric aims of Open Banking. The ACCC welcomes stakeholder views regarding the extent to which a consumer should be able to decide

122 Draft legislation, section 56EM(1).
123 That is, discloses it in accordance with section 56EI(1) of the draft legislation.
124 Draft legislation, section 56EM(2).
125 Draft legislation, section 56EM(3).
126 Draft legislation, section 56EN(1).
127 Draft legislation, section 56EN(2)

whether their redundant data is de-identified or destroyed, noting that safeguard 11 requires redundant data to be de-identified at a minimum.

Safeguard 12: Correction of CDR data

Privacy safeguard 12 provides that if a CDR consumer for CDR data (the "subject data") makes a request to the persons identified below to correct the subject data, then those people must respond to the request by taking such steps as specified in the rules to deal with certain specified matters. The persons are:

- a data holder who has been requested to disclose the subject data, or to disclose any CDR data associated with the subject data
- an accredited data recipient of the subject data.

The matters those persons must deal with are:

- either (a) to correct the subject data, or (b) include a statement with the subject data, to ensure that, having regard to the purpose for which the subject data is held, the subject data is accurate, up to date, complete, relevant and not misleading
- to give notice of any correction or statement, or notice of why a correction or statement is unnecessary or inappropriate.

The ACCC proposes to make rules to the effect that the specified steps the relevant persons should take are in accordance with the steps outlined by the OAIC in relation to APP 13, but in relation to the applicable CDR data rather than personal information as is the case under the APP. APP 13 outlines similar obligations in relation to personal information, and the OAIC has published extensive guidance on the application of the principle, available on the OAIC website. The ACCC may consider including more detailed requirements in a later version of the rules should the circumstances warrant.

14. Reporting and record keeping

Summary of proposed rules

The ACCC proposes to make rules requiring CDR participants to keep and maintain records relating to the participant's compliance with the privacy safeguards, the rules and the standards for a period of six years.

The ACCC also proposes to make rules requiring CDR participants to keep and maintain information about complaints for a period of six years and to provide regular reports of this information to the ACCC and the OAIC.

The ACCC also proposes to makes rules requiring accredited data recipients to notify the Data Recipient Accreditor of material changes in circumstances relevant to their accreditation.

14.1. General approach

The collection of information about the performance of the CDR will promote transparency, enable oversight of the operation of the CDR regime and provide information to enable regulators to monitor the CDR regime and to undertake compliance and enforcement action.

The Open Banking review made a number of recommendations in relation to the keeping of records and the reporting of information in the CDR regime. Specifically, the Open Banking review recommended that:

- data holders be required to keep performance records of their APIs and make these available to the regulator[128]

128 Open Banking review, recommendation 5.11.

- CDR participants be required to report to the ACCC about disputes arising under the multilateral contract relating to the standards.[129]

To facilitate this, the draft legislation provides a power for the ACCC to make rules relating to record keeping and reporting by CDR participants.[130] The draft explanatory materials to the draft legislation envisages that '*accredited data recipients will be required to provide specified reports to the ACCC or the OAIC for the purpose of those regulators enforcing compliance with all aspects of the CDR*.'[131] The ACCC intends to make rules requiring:

- all CDR participants to keep and maintain records relating to the participant's compliance with the privacy safeguards, the rules and the standards
- all CDR participants to keep and maintain information about complaints and to provide regular reports of this information to the ACCC and the OAIC
- the retention of all records for a period of six years.

The proposed record keeping and reporting rules are further detailed below. Additional requirements may be identified during the further development of the CDR regime and through stakeholder consultation.

14.2. Obligations on data holders

The ACCC proposes to make rules that will require data holders to keep and maintain:

- API performance records that would include API outage and response times, against the minimum service level benchmarks set out in the standards, the average time taken to complete the authorisation procedure across all consumers and the number of times a call is made on or to the data holder's API (to disclose a consumer's CDR data in accordance with a consumer's consent and authorisation), see sections 8 and 9
- records of any disclosures of CDR data directly to consumers including response times
- records relevant to their compliance with the privacy safeguards, in particular those demonstrating that consumer authorisations are appropriately sought and maintained
- complaint records which identify, on a quarterly basis:
    - the total number of consumer complaints received by the data holder, the average number of days taken to resolve those complaints, the outcome of the complaints and, where relevant, the number of complaints referred to external dispute resolution
    - the total number of disputes with other CDR participants, including in relation to the deemed contract between CDR participants requiring compliance with the standards,[132] and the outcome of those disputes.

A quarterly report detailing API performance information will be required to be provided to the ACCC and a quarterly report relating to complaints and disputes will be required to be provided to both the ACCC and the OAIC.

14.3. Obligations on accredited data recipients

The ACCC proposes to makes rules that will require accredited data recipients to keep and maintain:

129 Open Banking review, recommendation 2.11.
130 Draft legislation, section 56BH.
131 Draft explanatory memorandum, paragraph 1.101.
132 Draft legislation, section 56FF.

- records relevant to their compliance with the privacy safeguards, in particular those demonstrating that consumer consents are appropriately sought and maintained
- records relating to any outsourcing arrangements the accredited data recipient has in place, any transfers of consumer data outside of the CDR regime and the subsequent use of such data (see sections 6.8 and 12)
- complaints records which identify, on a quarterly basis:
    - the total number of consumer complaints received by the accredited data recipient, the average number of days taken to resolve these complaints, the outcome of the complaints, and, where relevant, the number of these complaints referred to external dispute resolution
    - the total number of disputes with other CDR participants, including in relation to the deemed contract between CDR participants requiring compliance with the standards,[133], and the outcome of those disputes.

A quarterly report detailing this complaints information will be required to be provided to both the ACCC and the OAIC.

The ACCC also proposes to make rules that will require accredited data recipients to notify the Data Recipient Accreditor as soon as practicable of any material change in circumstance relating to grounds on which accreditation may be suspended, varied or revoked, including:

- the commencement of legal proceedings of the type outlined in section 6.7
- a director of the accredited data recipient being disqualified from managing corporations
- the accredited data recipient becoming insolvent
- ceasing to be a member of the recognised external dispute resolution scheme (see section 15.3.1).

15. Dispute resolution

Summary of proposed rules

In relation to internal dispute resolution, the ACCC proposes to make a rule requiring that all CDR participants have in place internal dispute resolution procedures that comply with the requirements specified in the rules.

In relation to external dispute resolution, the ACCC proposes to make a rule requiring that all CDR participants be a member of the external dispute resolution scheme recognised by the ACCC for Open Banking. The ACCC proposes to recognise the Australian Financial Complaints Authority (AFCA).

In relation to complaints by larger businesses or disputes between CDR participants, the ACCC does not intend to make rules relating to alternative dispute resolution in these situations in the first version of the rules. However, the ACCC welcomes stakeholder views on this issue.

15.1. Background

Access to robust and timely dispute resolution options for complaints and disputes related to the CDR will enhance the effectiveness of the CDR regime. Inexpensive and informal dispute resolution will be particularly important to individual and small business consumers, who may lack the resources to pursue claims through the court system.

The Open Banking review made a number of recommendations in relation to dispute resolution. Specifically, the Open Banking review:

133 Draft legislation, section 56FF.

- recommended a tiered dispute resolution framework, involving internal and external dispute resolution processes for consumer complaints[134]
- recommended that the tiered framework include small business consumers[135]
- supported accredited parties committing to resolving disputes in relation to compliance with the standards through external dispute resolution where possible.[136]

The draft legislation provides:

- consumers with the ability to directly sue CDR participants if they suffer loss or damage as a result of a contravention of a civil penalty provision of the rules[137]
- CDR participants with the ability to enforce the standards against each other as a multilateral contract[138]
- a power for the ACCC to make rules requiring that CDR participants to have in place internal or external dispute resolution processes and enabling the ACCC to specify criteria for these processes[139]
- a power for the ACCC to recognise an external dispute resolution scheme for the resolution of disputes involving the CDR for one or more designated sectors.[140] This power is exercisable by notifiable instrument. The ACCC must consult with the OAIC before using the power.

The draft explanatory materials envisages that the AFCA will be recognised by the ACCC to undertake the external dispute resolution role in relation to Open Banking.[141]

The government confirmed that neither dispute resolution assistance from the OAIC nor external dispute resolution schemes would be available to large business consumers.[142] However, the government suggested that the ACCC may make rules to provide for other dispute resolution arrangements for these consumers.[143] The draft explanatory materials also suggests there may be a role to be played by alternative dispute resolution mechanisms, such as commercial arbitration, in relation to disputes between CDR participants.[144]

The Open Banking regime in the UK requires participants to put in place internal dispute resolution procedures that meet certain minimum requirements.[145] In addition, the UK's Financial Services Ombudsman provides external dispute resolution services in relation to consumer disputes. The UK Open Banking model does not mandate any alternative dispute resolution processes for disputes between participants.

The ACCC proposes to make rules in relation to internal and external dispute resolution processes as set out below.

134 Open Banking review, recommendation 2.10.
135 Open Banking review, recommendation 4.4.
136 Open Banking review, page.31.
137 Proposed amendment to subsection 82(1) of the CCA.
138 Draft legislation, section 56FF.
139 Draft legislation, section 56BH.
140 Draft legislation, section 56AD.
141 AFCA will replace the three existing external dispute resolution schemes of the Financial Ombudsman Service, the Credit and Investments Ombudsman and Superannuation Complaints Tribunal and will commence from 1 November 2018. Information about AFCA membership, including membership fees, is available at: https://www.afca.org.au/.
142 Consumer Data Right Booklet, page 7.
143 Consumer Data Right Booklet, page 7.
144 Draft explanatory materials, paragraph 1.151
145 PSR, regulation 101.

15.2. Internal dispute resolution

In practice, many complaints about the CDR regime will be best resolved between the affected parties. Accordingly, the ACCC proposes to make rules requiring that all CDR participants (i.e. both data holders and accredited data recipients) have in place internal dispute resolution procedures that comply with the requirements specified in the rules and which cover their activities as participants in the CDR regime. This would act as the first step in the dispute resolution process. Internal dispute resolution should be available in relation to all CDR complaints and disputes, whether the entity complaining is a consumer or another CDR participant, and whether the complaint relates to compliance with the privacy safeguards, the rules or the standards.

AFS licence holders and licensed credit providers are already required to have in place internal dispute resolution procedures that adhere to the requirements specified by ASIC in Regulatory Guide 165: *Licensing: Internal and external dispute resolution*. ASIC's requirements take into account Australian Standard AS/NZS 10002:2014 *Guidelines for complaint management in organizations*. Consistent with these existing requirements, the ACCC proposes to specify requirements for internal dispute resolution mechanisms for CDR participants in the first version of the rules which will largely replicate those in ASIC's Regulatory Guide (adapted for complaints relating to the CDR regime).

In particular, the rules will require the internal dispute resolution procedures of CDR participants to:

- adopt a definition of 'complaint' that is based on that used in AS/NZS 10002:2014 and adapted to cover complaints related to the use, storage, disclosure or handling of CDR data by the CDR participant and disputes related to compliance with the standards
- comply with the guiding principles of AS/NZ 10002:2014 and the sections related to commitment, resources, collection of information and analysis and evaluation of complaints
- be documented and made available in manner to enable a person or complainant to find out how to make a complaint and how and by whom that complaint will be handled
- include procedures for informing those with a complaint or dispute about the availability and accessibility of any relevant external dispute resolution scheme and any ability to take complaints to the OAIC
- provide a final response to a complaint within 45 days
- provide that if dispute resolution is outsourced to a third party the participant remains responsible for ensuring the procedures comply with the rules.

The rules will supplement the requirements placed on CDR participants by privacy safeguard 1, which requires all CDR participants to have a policy about the management of CDR data which explains to consumers how they can make complaints and how the participant will deal with complaints.[146]

15.3. External dispute resolution

15.3.1. Existing schemes

The ACCC intends to recognise AFCA as the external dispute resolution scheme for Open Banking. The ACCC understands that the AFCA's rules will be amended to expand its

146 Draft legislation, sections 56ED (4) and (5).

jurisdiction with respect to complaints by eligible persons in relation to CDR participants. [147] Many CDR participants in Open Banking are likely to already be members of AFCA as a result of existing regulatory requirements at the time that the CDR regime commences. As other sectors of the economy are designated under the CDR regime, the ACCC will consider the appropriate external dispute resolution schemes for those sectors as part of the broader consideration of the need for variation of the rules to accommodate new sectors.

For the first version of the rules, the ACCC proposes to make a rule requiring that all CDR participants (i.e. both data holders and accredited data recipients) be a member of the external dispute resolution scheme recognised by the ACCC for Open Banking.

15.3.2. Alternative dispute resolution

AFCA's jurisdiction will not extend to complaints by larger business consumers nor disputes between CDR participants in relation to the statutory contract that the draft legislation deems to apply between data holders and accredited data recipients requiring compliance with the standards.[148]

The ACCC recognises that alternative dispute resolution, such as mediation or commercial arbitration, can provide cheaper and quicker outcomes for disputes than pursuing court action, and that these options are generally available to commercial entities. The ACCC expects CDR participants to take advantage of alternative dispute resolution options where this assists in resolving disputes and complaints in an efficient and timely manner.

However, requiring CDR participants to pursue a particular form of alternative dispute resolution raises complex policy considerations. These include identifying the appropriate form of alternative dispute resolution, both for disputes involving large businesses as CDR consumers and disputes between CDR participants. An option that may be suitable for complaints by large business consumers would be to provide for a commercial mediation process that could facilitate the resolution of such complaints, while disputes between CDR participants relating to the technical standards may be more appropriately resolved through some form of expert determination. Another issue is the extent to which particular forms of alternative dispute resolution can or should be mandated. The ACCC does not intend to make rules relating to alternative dispute resolution in these situations in the first version of the rules and considers this to be an issue which could be addressed in a later version of the rules if the need for such arrangements becomes apparent in light of experience with the CDR regime. However, the ACCC welcomes views from stakeholders about the need for the first version of the rules to make provision for alternative dispute resolution for large business consumers and for disputes between CDR participants and what the appropriate alternative dispute resolution model for these kinds of disputes may be.

16. Data Standards Body

Summary of proposed rules

The ACCC proposes to make rules that set out the process by which standards are developed by the Data Standards Body, including specified principles for developing standards to which the Data Standards Body must have regard and requirements that draft standards be publically available for stakeholder testing and feedback.

The ACCC proposes to make rules that require the Data Standards Chair to review the operation of a standard where directed to do so by the ACCC, and rules that facilitate urgent or purely technical changes to the standards being made without undertaking the usual consultation processes.

The ACCC proposes to make rules that require the Data Standards Chair to establish and maintain at

147 Under the AFCA's draft rules, eligible persons are individuals and small businesses with less than 100 employees at the time of the act or omission giving rise to the complaint. The draft rules are available at: https://www.afca.org.au/custom/files/docs/1527568173029/australian-financial-complaints-authority-draft-rules.pdf.

148 Draft legislation, section 56FF.

least one Advisory Committee, as well as a consumer experience consultative group.

16.1. Background

The Open Banking review provided for the establishment of a Data Standards Body to work with regulators to develop the standards for Open Banking, and for the Data Standards Body to incorporate expertise in the standards setting process and consumer data sharing, as well as participant and consumer experience.[149]

The draft legislation provides that the Minister may, by written instrument, appoint a person to be the Data Standards Chair and a body to be the Data Standards Body to assist the Data Standards Chair.[150] The draft legislation sets out the functions and powers of the Data Standards Chair which include to make the standards and to review the standards regularly.[151]

Under the draft legislation, the rules may include requirements to be complied with by the Data Standards Chair when making, varying or revoking a standard in relation to approval, consultation, and the formation of committees, advisory panels, and consultative groups.[152]

To date, an interim Data Standards Chair has been appointed who is assisted by an interim Data Standards Body, CSIRO's Data61, and an interim Advisory Committee,[153] to provide industry and consumer perspectives and strategic advice on the design and implementation of the standards.

16.2. Proposed Data Standards Body rules

The ACCC proposes to make rules that will set out the process for developing standards as set out below.

The ACCC also proposes to make a rule that the Data Standards Chair must review the operation of a standard where directed to do so by the ACCC.

The ACCC does not propose to make rules relating to the governance of the Data Standards Body in the first version of the rules. The need for rules of this kind will be considered in the future if a body other than Data61 is appointed as the Data Standards Body.

16.2.1. Consultation and advice

The ACCC supports consultation as an important part of the standards development process. The rules will require standards to be made publically available, during a consultation period, for testing and feedback from stakeholders. The length of the consultation period will be determined by the Data Standards Chair. Consultation will be required for both new standards and for substantive or major changes to existing standards.

However, given the technical nature of the standards, the ACCC is aware that some updates to the standards will be routine or minor in nature. Therefore, the ACCC proposes to make rules that will enable the making of urgent or minor technical changes to the standards without undertaking the usual consultation process.

The ACCC proposes to make a rule that requires the Data Standards Chair to establish and maintain at least one Advisory Committee. The ACCC considers that an ongoing Advisory Committee (like the interim Advisory Committee) will be made up of stakeholders with

149 Open Banking review, recommendation 2.6.
150 Draft legislation, section 56FA(1).
151 Draft legislation, section 56FB(1).
152 Draft legislation, section 56FE(4).
153 See https://data61.csiro.au/en/Who-we-are/Our-programs/Consumer-Data-Standards for further information.

relevant industry experience, training or qualifications as well as consumer representatives. The ACCC notes that the composition of the Advisory Committee will inevitably change as new sectors are added to the CDR regime over time. Therefore, the rules should allow for maximum flexibility in terms of who may be appointed in order to facilitate this evolution. The ACCC also proposes to make a rule that allows the OAIC and the ACCC to elect to be observers on the Advisory Committee.

The ACCC also proposes to make a rule that requires the Data Standards Chair to establish and maintain a consumer experience consultative group. A consumer experience consultative group currently exists under the interim arrangements. This group will assist the Data Standards Body in the design and testing of the open API standards and will ensure that the ultimate experience of a CDR consumer is taken into account in developing the standards in relation to consent, authorisation and authentication (see section 9.3.3).

16.2.2. Matters to be considered in standards making

The ACCC also proposes to make rules that set out the matters to which the Data Standards Chair must have regard in making the standards. These matters will include:

- any feedback received from stakeholders during the consultation period
- any feedback received from the consumer experience consultative group
- the advice of the Advisory Committee
- any feedback received from other committees, advisory panels, or consultative groups that the Data Standards Chair may have established
- the principles applying to the development of the standards.

16.2.3. Principles guiding development of the standards

The ACCC proposes to make rules that will require the development of the standards to occur having regard to particular principles. The proposed principles reflect the principles that applied to the development of the UK's Open Banking API technical standards,[154] with the addition of a principle relating to security. These principles have been adopted by the interim Advisory Committee.

The proposed principles are:

- **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 data can be exchanged between parties in a frictionless manner across organisational and technological boundaries.
- **Re-use** - adopting and leveraging existing standards, taxonomies, and 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.

154 Open Banking review, page 80.

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

Part C – Appendix

Glossary

AAT	Administrative Appeals Tribunal
ACCC	Australian Competition and Consumer Commission
ADI	Authorised Deposit-taking Institution
AFCA	Australian Financial Complaints Authority
AISP	account information service provider
API	application programming interface
APPs	Australian Privacy Principles
APRA	Australian Prudential Regulatory Authority
ASIC	Australian Securities and Investment Commission
ASIC Act	*Australian Securities and Investment Commission Act 2001* (Cth)
Banking Act	*Banking Act 1959* (Cth)
Banking Regulation	Banking Regulation 2016
CCA	*Competition and Consumer Act 2010* (Cth)
CDR	Consumer Data Right
CMA	Competition and Markets Authority
CMA Order	Competition and Markets Authority Retail Banking Market Investigation Order 2017
Corporations Act	*Corporations Act 2001* (Cth)
CSIRO	Commonwealth Scientific and Industrial Research Organisation
draft explanatory materials	the draft explanatory memorandum to the exposure draft *Treasury Laws Amendment (Consumer Data Right) Bill 2018* released on 14 August 2018
draft legislation	the exposure draft *Treasury Laws Amendment (Consumer Data Right) Bill 2018* released on 14 August 2018
FCA	Financial Conduct Authority
GRI	government related identifier
OAIC	Office of the Australian Information Commissioner
OBIE	Open Banking Implementation Entity
Open Banking review	*Review into Open Banking: giving customers choice, convenience and confidence*, Final Report, December 2017
PISP	payment initiation service provider
Privacy Act	*Privacy Act 1998* (Cth)
PSR	*Payment Services Regulations 2017 (UK)*
PSD2	revised Payment Services Directive (EU)

Register	Register of Accredited Data Recipients
RTS	Regulatory technical standards for strong customer authentication under PSD2