Australian Government

Consumer Data Right

Accreditation fact sheet

Version 2
December 2022

Table of Contents

1. Introduction 2
2. Applying for accreditation 3
   - 2.1. Types of accreditation 3
   - 2.2. Applying for accreditation 4
   - 2.3. The assessment process 5
3. Accreditation requirements 7
   - 3.1. 'Fit and proper person' criteria and 'associated persons' 7
   - 3.2. Information on corporate and organisational structures 8
   - 3.3. Information security criteria 8
   - 3.4. Information security evidence 8
   - 3.5. Insurance obligation 9
   - 3.6. Risk analysis and written statement on insurance 9
   - 3.7. Dispute resolution policy 10
   - 3.8. Other requirements 10
4. Alternatives to accreditation 12
   - 4.1. CDR representative model 12
   - 4.2. Outsourced service provider model 12
   - 4.3. Trusted adviser model 12
   - 4.4. CDR insights model 12
5. Ongoing obligations after accreditation 13

1. Introduction

1.1. Consumer Data Right

The Consumer Data Right (CDR) gives consumers greater control over their data, enabling them to access and share their data with accredited third parties to access better deals on everyday products and services.

A glossary of common terms is published on the CDR Support Portal.

1.2. Accreditation

Entities that wish to collect consumer data to provide products or services to consumers under the CDR must be accredited as a **data recipient** by the Data Recipient Accreditor (the Accreditor), currently the ACCC.

1.3. This fact sheet

This fact sheet provides basic information on the CDR accreditation process. For more detailed information on accreditation, see the Accreditation guidelines (including the supplementary guidelines on information security and insurance).

This fact sheet should be read together with the latest version of the Competition and Consumer (Consumer Data Right) Rules 2020 (CDR Rules).

Separate fact sheets, such as for CDR representatives, on-boarding and privacy for consumers, are available on the CDR FAQs webpage.

2. Applying for accreditation

The CDR Rules set out the criteria that the Accreditor will consider in assessing an application for accreditation at either the unrestricted or sponsored level. Once accredited, an accredited person must comply with ongoing obligations to maintain their accreditation.

Further details about how to apply for accreditation are available in our Accreditation guidelines.

2.1. Types of accreditation

There are 2 levels of accreditation available to CDR participants:

- ***Unrestricted:*** the highest level of accreditation. Unrestricted level participants:
  - can collect CDR data from data holders, when requested and consented to by a consumer
  - must provide an independent third-party assurance report as part of their application.
- ***Sponsored:*** this accreditation level reduces barriers to entry for entities that want to participate in the CDR. Sponsored participants:
  - cannot collect CDR data directly from data holders – they must request their sponsor (an unrestricted level participant) to collect it for them
  - must meet the same accreditation criteria as unrestricted applicants but do not have to provide an independent third-party assurance report as part of their application – they can use the sponsored accreditation self-assessment and attestation form to self-assess and attest to information security requirements.

2.1.1. Roles of 'affiliate' and 'sponsor'

A person with unrestricted accreditation can be a 'sponsor'. A person with a sponsored accreditation is an 'affiliate'. An affiliate must have both **sponsored accreditation** and a **sponsorship arrangement with a sponsor** before it can access CDR data or provide related products or services to a CDR consumer.

Both the affiliate and its sponsor must comply with the accreditation obligations in the CDR Rules. A sponsor must comply with specific requirements with respect to its affiliate, including:

- undertaking due diligence on its affiliate
- providing appropriate training and assistance to its affiliate on technical and compliance matters
- using reasonable steps to ensure the affiliate complies with its obligations as an accredited person.[1]

[1] See CDR Rules, Schedule 1.

2.2. Applying for accreditation

2.2.1. Eligibility

Any business that believes it can satisfy the accreditation obligations in the CDR Rules may apply for accreditation.

New and small businesses (including sole traders) can apply for accreditation. However, there are also alternative pathways to access CDR data that potential participants may wish to consider if they do not want to apply for accreditation (see section 4 below).

Authorised deposit-taking institutions (ADIs) are only required to be accredited if they wish to collect CDR consumer data to provide products or services to consumers. If an ADI would like to be accredited (and they are not a restricted ADI), they may apply for **streamlined accreditation**. There is a streamlined version of the accreditation application form in the CDR Participant Portal. A sample version of the streamlined form is available on the CDR website.

Non-Australian businesses can also be accredited if they wish to receive consumer data to provide products or services to consumers under the CDR. When applying for accreditation, a non-Australian business must:

- have a local agent
- provide their local agent's physical and electronic addresses for service (when creating an account through the CDR Participant Portal)
- provide full copies of original documents, including documents that are not in English. They must also provide English-language translations of these documents. Translations should be undertaken by a National Accreditation Authority for Translators and Interpreters (NAATI) accredited translator.

2.2.2. Creating an account to access the CDR Participant Portal

The applicant must first create an account to access the CDR Participant Portal.

2.2.3. Selecting the correct application form

Once the applicant has access to the CDR Participant Portal they will be able to start their application using one of the electronic application forms. Accreditation applications can only be submitted using one of these approved forms through the portal.

Applicants can select one of 3 application types:

- unrestricted
- sponsored
- streamlined (only available to ADIs).

To help potential applicants prepare their application for accreditation, we have created sample versions of all of these forms. The sample forms show the questions that will be asked and the documentation that will be required. The sample forms are available on the CDR website.

2.2.4. Fees

There is no fee to apply for accreditation.

2.2.5. Amending an application

Once an accreditation application has been submitted, it can be viewed but not amended. Further information or clarification on an application can be provided by email to the ACCC's CDR inbox (ACCC-CDR@accc.gov.au).

2.2.6. Withdrawing an application

An applicant may request to withdraw a submitted application through the change request function in the CDR Participant Portal.

2.3. The assessment process

Once an accreditation application is received, the ACCC will check that all the required questions have been answered and all supporting documents have been provided. If the application is incomplete – for example, it is missing mandatory information such as insurance policies or details – we will return the application and change the status to 'draft' so that the applicant can address the deficiencies and resubmit the application.

If the application is complete, the Accreditation team will contact the applicant and may arrange to meet to discuss their use case, provide clarification or seek further information. We may also consult with other Australian Government authorities or overseas counterparts if required.

The ACCC will assess the application, taking into account the criteria discussed in section 3 below.

Further details about the accreditation process, including conditional accreditation and the review process, are available in our Accreditation guidelines.

2.3.1. Timeframe for accreditation decisions

Accreditation decisions may take approximately 3 months from receiving a complete application. The time taken to assess an application will vary depending on matters such as:

- whether the applicant has provided all the required information in sufficient detail – to ensure that the application is assessed quickly, applicants should include full responses and all required documents
- the complexity of the application.

2.3.2. Accreditation decision

Once the Accreditor has made an accreditation decision, we will notify the applicant of the outcome by phone and in writing. The Accreditation Registrar will also be notified of the decision. They will be given the accredited person's name, any conditions of accreditation and the effect of these conditions where appropriate. Accreditation will take effect when this information is included on the Register of Accredited Persons.

If a decision is made not to accredit the applicant, or to set conditions on accreditation, we will advise the applicant and provide reasons for the decision. The applicant may seek a review of the decision by the Administrative Appeals Tribunal.

2.3.3. Transfer of accreditation to another entity

Accreditation cannot be transferred from one entity to another, even if those entities are related bodies corporate. Changes in control of an accredited person will not affect the accredited status. However, applicants must notify the ACCC of any material change(s) – for example, any matter that could be relevant to the Accreditor's decision on whether a person is a fit and proper person.

3. Accreditation requirements

The CDR Rules set out the criteria that the Accreditor will apply when considering an application for accreditation.

Further details about the accreditation criteria are available in our Accreditation guidelines (including the supplementary guidelines on information security and insurance).

3.1. 'Fit and proper person' criteria and 'associated persons'

An applicant must be a **fit and proper person** to be accredited.[2]

Further details about the fit and proper person criteria are available in our Accreditation guidelines.

When we assess an application against the fit and proper person criteria, we take into account all of the applicant's **associated persons**. An 'associated person' is:

- a natural person (an individual) who:
  - is involved, or would be involved if accredited, in the decision making by the applicant that affects the applicant's management of CDR data, or
  - can significantly impact the applicant's management of CDR data
- if the applicant is a body corporate – a person who:
  - is an associate of the applicant (within the meaning of the *Corporations Act 2001* (Cth) (Corporations Act)), or
  - is an associated entity of the applicant (within the meaning of the Corporations Act).[3]

An accreditation application must disclose all persons that meet the definition of an 'associated person' of the applicant, including the applicant itself. A wide group of individuals and businesses, including individuals who belong to related overseas businesses, can be viewed as associated persons.

As part of their application, an applicant must provide declarations signed by each associated person (natural or body corporate) addressing the fit and proper person criteria. Declaration forms can be found on the CDR website.

If an associated person is an individual, in their declaration they must provide their:

- full name
- date of birth
- contact details.

If an associated person is a body corporate, the declaration must be completed by an authorised officer of the company (that is, a company director, company secretary, chief executive officer, chief operating officer, chief financial officer or managing director).

[2] CDR Rules, rules 5.12(2)(a) (requirement to be a fit and proper person) and 1.9 ('fit and proper person' criteria).

[3] CDR Rules, rule 1.7.

3.2. Information on corporate and organisational structures

An applicant must also include in their application:

- a current corporate structure chart which identifies the applicant, its subsidiaries and related bodies corporate (including all companies in which the applicant or its subsidiaries hold minority shareholdings that are involved in the relevant business)
- a current organisation chart which identifies the full name and role of relevant individuals who are associated persons of the applicant and who have the capacity to make decisions affecting the management of CDR data.

3.3. Information security criteria

An applicant must take the steps set out in Schedule 2 of the CDR Rules for the purposes of Privacy Safeguard 12 to protect CDR data from misuse, interference, loss, unauthorised access, modification or disclosure.[4]

When applying for accreditation, an applicant must provide evidence, in the form set out in the Supplementary accreditation guidelines: information security.

3.4. Information security evidence

3.4.1. Unrestricted accreditation

When applying for unrestricted accreditation, an applicant's assurance report must be prepared in accordance with one of the following accepted standards:

- Australian Standard on Assurance Engagements (ASAE) 3150 *Assurance Engagement on Controls* standard
- ASAE 3402 *Assurance Reports on Controls at a Service Organisation*
- International Standard on Assurance Engagements (ISAE) 3000 series
- SOC1/SOC2 reports prepared in accordance with applicable Statement on Standards for Attestation Engagements (SSAE) standards.

Applicants may also leverage existing standards to satisfy the information security criteria as set out below.

Use of existing standards

An applicant may have prior certification or compliance with the following standards:

- ISO 27001 certification
- level 1 PCI DSS compliance
- top tier ATO Digital Service Provider Operational Security Framework compliance.

If so, they will be able to rely on this evidence. They will also need to provide an assurance report covering the controls that are not covered by their ATO Digital Service Provider Operational Security Framework letter of confirmation, ISO 27001 certification or

[4] CDR Rules, rule 5.12(1)(a).

level 1 PCI DSS compliance, and other relevant evidence to satisfy the information security obligation.

The assurance report must address the information security criteria in the CDR Rules (including the control requirements specified at Schedule 2).

An applicant may use an existing assurance report prepared in accordance with one of the standards listed above. The Accreditor will generally accept an existing report that contains partial coverage of the controls in Schedule 2 of the CDR Rules if certain conditions are met (as specified in section 3.1.3 of the Supplementary accreditation guidelines: information security).

The assurance report should be no more than 3 months old at the time of submitting the accreditation application. If an applicant is using an existing assurance report that is more than 3 months old, the Accreditor may impose a condition that they must submit a new report in the initial reporting period after accreditation instead of an attestation statement as required in Schedule 1 of the CDR Rules.

3.4.2. Sponsored accreditation

When applying for accreditation at the sponsored level, applicants must provide a completed self-assessment and attestation form covering the information security obligations.

The template attestation form is available on the CDR Resources webpage. Further information about the information security component of the sponsored accreditation criteria is available in our Supplementary accreditation guidelines: information security.

3.5. Insurance obligation

The insurance obligation ensures that an accredited person has adequate insurance to cover the risk of CDR consumers not being properly compensated for any loss that might reasonably be expected to arise from a breach of obligations under any law relevant to the management of CDR data.

Further details about the insurance obligation are available in our Supplementary accreditation guidelines: insurance.

3.5.1. Risk analysis and written statement on insurance

Accredited persons will have different businesses and risks. These differences will affect what insurance cover is adequate. It is therefore essential that each applicant undertakes their own analysis to determine what is adequate for them and clearly sets this out in appropriate detail in a signed written statement as part of their accreditation application.

The written statement must be signed by a duly authorised representative and:

- outline the details of the applicant's insurance policy (or policies) that they consider satisfy the insurance obligation
- provide a detailed explanation of how they have determined that their insurance policy (or policies) is adequate to cover the risks that they may be exposed to in connection with the management of consumer data.

In drafting a statement about the adequacy of insurance for their business, the applicant should understand the insurance obligation, properly examine and understand their policy or policies and explain any gaps or exclusions.

The accreditor will consider, amongst other things, the matters set out in Table 1 of our Supplementary accreditation guidelines: insurance in assessing whether the applicant would, if accredited, be able to comply with the insurance obligation.

For example, the applicant should consider and address in their written statement the:

- nature and volume of CDR data they are likely to manage, to ensure their insurance cover is appropriate to cover any related risks
- financial resources, to ensure they have sufficient financial resources to cover any gaps or exclusions in their insurance cover.

3.6. Dispute resolution policy

3.6.1. Internal dispute resolution

Applicants for unrestricted or sponsored accreditation, even if they are not financial services providers, must develop an internal dispute resolution policy that complies with the Australian Securities and Investments Commission's Regulatory Guide 271 *Internal dispute resolution,* as in force from time to time.

However, applicants who are retailers in the energy sector must have internal dispute resolution processes that satisfy the applicable requirements for that retailer's standard complaints and dispute resolution procedures under the National Energy Retail Law or the Energy Retail Code (Victoria).

3.6.2. External dispute resolution

Generally, accreditation applicants must be a member of the Australian Financial Complaints Authority (AFCA) even if they do not provide financial services.

However, energy retailer applicants who will not use any energy sector CDR data to provide services outside the energy sector do not need to belong to AFCA. They must be a member of the energy and water Ombudsman in their state or territory. If there is no recognised energy and water Ombudsman in their state or territory, they must take the necessary steps to participate in the dispute resolution process in their jurisdiction appropriate for CDR consumer complaints.[5]

Further details about the process for applying for AFCA membership as a non-financial services provider are set out in our Accreditation guidelines.

3.7. Other requirements

3.7.1. Reciprocal data holder obligations

An accredited person may be subject to the **reciprocal data holder obligations**. This means they may be required to share particular CDR data at particular times, at the direction of a consumer, in accordance with the obligations of a data holder under the CDR Rules (separate to the obligations of an accredited person).

[5] CDR Rules, Schedule 4, rule 5.2(3)(d).

Reciprocal data holder obligations apply for CDR data that is:

- generated and held by or on behalf of an accredited person
- generated in respect of a product that is publicly offered by the accredited person to consumers.

Therefore, an accredited person will be required to share CDR data that they generate and hold, as a data holder in accordance with the reciprocal data holder obligations, with other accredited data recipients. For example, an accredited non-bank lender may become a reciprocal data holder in respect of data they generate for their personal loan products. These obligations are intended to create a more vibrant and dynamic CDR ecosystem.

The reciprocal data holder obligations are also intended to bring elements of fairness into the CDR scheme. The ACCC considers that providing some short-term flexibility in the timing of reciprocal data holder obligations may benefit the overall CDR by encouraging earlier participation and increased competition. Therefore, an accreditation applicant can apply to the ACCC for an exemption to the reciprocal data holder obligations under section 56GD of the *Competition and Consumer Act 2010* (Cth). This includes granting a time-limited exemption to prospective applicants, delaying their reciprocal data holder obligations for a set period. Each exemption application will be considered on a case-by-case basis.

Exemption applications should be made to the ACCC at ACCC-CDR@accc.gov.au. The application will be considered alongside the applicant's accreditation application.

Further details about the reciprocal data holder obligations are set out in our Accreditation guidelines. Prospective applicants with questions about the reciprocal data holder obligations should contact the ACCC at ACCC-CDR@accc.gov.au.

4. Alternatives to accreditation

Entities that wish to participate in the CDR without accreditation may use one of the following alternative CDR participation pathways or data sharing options:

- CDR representative model
- outsourced service provider model
- trusted adviser model
- CDR insights model.

There are requirements that must be satisfied when using these pathways. Further details about these alternative pathways are available in our Accreditation guidelines.

Currently, unless they are accredited, a consumer cannot receive their own CDR data through an application programming interface. Persons who wish to access their own CDR data could seek access to this data from an accredited provider or through another channel, such as directly from their bank.

4.1. CDR representative model

The CDR representative model provides for an 'agency-like' arrangement that allows unaccredited persons to partner with an unrestricted accredited person to provide goods and services using CDR data.

4.2. Outsourced service provider model

Outsourced service providers may be used to collect CDR data on behalf of an accredited person and to provide goods and services to an accredited person.

4.3. Trusted adviser model

Under the trusted adviser model, a consumer can nominate persons outside the CDR scheme as trusted advisers that accredited persons may disclose the consumer's data to. The classes of trusted advisers are listed in the CDR Rules. They include professions that are considered to be appropriately regulated to ensure a strong level of consumer protection.

4.4. CDR insights model

The CDR insights model also allows a consumer to consent to their data being shared outside the CDR scheme for prescribed purposes that are considered low risk and that are designed to limit the data shared to only what is necessary for the consumer to receive a service.

5. Ongoing obligations after accreditation

Once accredited, to maintain your accreditation you must continue to comply with:

- ongoing reporting and record keeping obligations
- specific ongoing information security obligations.[6]

For details of key ongoing accreditation obligations, see the CDR Rules, rule 5.12, Part 9 and Schedule 1.

[6] CDR Rules, rule 5.12.