Accreditation checklist

April 2023

What is accreditation?

The Consumer Data Right (CDR) gives consumers the right to require a service provider that holds their personal data (data holder) to share that data with another service provider (accredited data recipient) in a secure online environment. The CDR aims to give consumers more access to and control over their personal data. Being able to share data easily and efficiently between service providers will make it easier for consumers to compare and switch between products and services.

To participate fully in the CDR, a service provider must be accredited. There is currently no application fee to apply for accreditation.

There are 2 levels of accreditation:

- Unrestricted accreditation: Section 3.1 in our guidelines

  See sample version of the unrestricted application form.

- Sponsored accreditation: Section 3.2 in our guidelines

  See sample version of the sponsored accreditation form.

Provided all required information and documents have been provided, an average accreditation assessment can take around 3 months to process.

There are also a number of alternative pathways to participate in some aspects of the CDR – see section 9.1 to 9.3 of our guidelines. However, this checklist only covers accreditation at the unrestricted and sponsored levels.

Before you start your accreditation application, we recommend you read and complete the steps below, and have the required documents ready.

Accreditation process preparation

Read our Accreditation Guidelines as well as the Supplementary Guidelines on insurance and information security as this will help you to submit a valid application.

Ensure any documents listed below which are not in English have a translated version by an accredited translator.

Accreditation – required information and documents

The accreditation process requires you to provide the following information and documents with your application. It will be helpful to have these prepared to the standards outlined in our guidelines prior to beginning your application.

- ☐ A clear description of the products or services that will be offered if accredited. We recommend you provide a diagram of how your product will work in practice, accompanied by a step-by-step walkthrough.

- ☐ Current corporate and organisation structure charts.

- ☐ Signed [Fit and proper person declaration form] for each [associated person] identified in the application (including the applicant itself and any related body corporates).

- ☐ Financial statements from the last financial year (or latest draft).

- ☐ Insurance policy documents for each policy relied on, including:

  - certificates of currency for each policy

  - insurance schedules for each policy

  - a written statement, signed by an authorised representative, explaining how your organisation's insurance is adequate to cover the risks it may be exposed to in connection with the management of CDR data.

  Please see our [insurance guidelines] for more detail.

- ☐ A document outlining your internal dispute resolution process. The IDR policy must comply with [Regulatory Guide 271] unless you are an energy retailer (as defined in clause 1.4 of Schedule 4 of the CDR Rules).

  Applicants that are energy retailers must have IDR processes that satisfy the applicable requirements for the retailer's standard complaints and dispute resolution procedures under the National Energy Retail Law or the Energy Retail Code (Victoria).

  Further detail on what the IDR process policy must contain can be found in Section 6.3 of our [guidelines].

- ☐ Ensure you are a member of a relevant external dispute resolution scheme under the CDR Rules and have your membership number and start date ready.

- ☐ **Information security requirements**

  Unrestricted accreditation

  An information security assurance report in accordance with one of our accepted standards. See Section 2.1.1 and 2.1.2 of our [information security guidelines].

  Sponsored accreditation

  A [self-assessment and attestation form] to confirm that the applicant meets the information security obligations for its CDR data environment. Please refer to Section 2.2 of our [information security guidelines] for more information.

- ☐ To start an application, log in to your [Participant Portal account] and open the relevant accreditation application form.

  A member from the accreditation team will be touch once your application has been received and a completeness check has been undertaken (usually within 5 business days).

  We encourage applicants with questions about accreditation to contact the ACCC at

  [ACCC-CDR@accc.gov.au]
  See also [further useful resources].