Accreditation frequently asked questions (FAQs) – Consumer Data Right

The following document has been prepared to address questions specifically relating to the accreditation process within the Consumer Data Right regime. In order to obtain a more complete view of the regime, we recommend that these FAQs be read in conjunction with the following documents:

- The Consumer Data Right interagency FAQs, available here
- The ACCC's final Accreditation Guidelines, available here
- The Consumer Data Right Rules, available here
- The OAIC's Consumer Data Right Privacy Safeguard Guidelines, available here
- The Consumer Data Standards, available here.

1.1. Applying for accreditation

What is accreditation and what is the role of the ACCC?

Entities that wish collect to receive consumer data to provide products or services to consumers under the Consumer Data Right regime must be accredited by the Data Recipient Accreditor (currently the ACCC). The Consumer Data Right Rules set out the criteria that the Data Recipient Accreditor will apply when considering an application for accreditation. Once accredited, an accredited person must comply with ongoing obligations to maintain accreditation. Further details about the accreditation criteria and how to apply for accreditation are available in our Accreditation Guidelines.

How do I apply for accreditation?

Accreditation applicants are required to complete an electronic application form which will be available on the Consumer Data Right participant portal. Authorised-deposit taking institutions (ADIs) can apply for accreditation through the streamlined form. Application forms can be accessed and lodged once participants have created an account in the Consumer Data Right participant portal.

Further details about how to apply for accreditation are available in our Accreditation Guidelines. These guidelines are designed to assist applicants with preparing their accreditation applications.

How does onboarding work?

Once accreditation is granted, an accredited person will proceed through onboarding processes. We are in the process of developing requirements for the technical onboarding process and will provide more information on this in due course. As part of the onboarding

process, data holders and accredited persons will be required to complete conformance testing before they can be made active on the Consumer Data Right Register. Completing these tests will ensure conformance with the Consumer Data Standards and Consumer Data Right Register design, with initial focus on the information security profile and consent.

Will authorised deposit-taking institutions (ADIs) be required to apply for accreditation?

Any entity that wishes to receive consumer data to provide products or services to consumers under the Consumer Data Right regime must be accredited.

An applicant who is an ADI (but not a restricted ADI) meets the criteria for streamlined accreditation in the banking sector and may complete the streamlined accreditation form when it becomes available.

Where can I access the streamlined and full accreditation application forms?

Sample versions of the accreditation application forms will be published on our website upon release of the Consumer Data Right participant portal. The sample forms will show the questions that will be asked in the online application forms and are intended to help potential applicants prepare their accreditation application. Applications will only be able to be made via the online forms available on the Consumer Data Right participant portal.

Interested parties may refer to our Accreditation Guidelines as these indicate the criteria which must be met and the information that will be required to complete an application.

Is there a filing fee for lodgement of an accreditation application?

There is no cost to lodge an accreditation application.

Are non-Australian companies required to be accredited? Can they be accredited?

All entities that wish to receive consumer data to provide products or services to consumers under the Consumer Data Right regime must be accredited. Foreign entities are able to be accredited as an accredited person. A foreign entity is required to have a local agent, and include details of its local agent and its local agent's address for service in its application for accreditation.

How long will the accreditation process take?

The time taken to assess a completed application will vary depending on matters such as whether the applicant has all the required information available and the complexity of the application. Fulsome responses and all documents are required to enable efficient consideration of applications.

Will there be a further round of testing in addition to that which commenced with initial data recipients in October 2019?

Once accreditation is granted, an accredited person will proceed through required onboarding processes. The ACCC is developing a Conformance Test Suite for this purpose, consequently, additional rounds of testing similar to that which commenced in October 2019 will not be required.

Is there a sandbox for Consumer Data Right?

A sandbox has not been developed for the Consumer Data Right at this stage. Swagger definitions on the Consumer Data Right Register and Consumer Data Standards provide sample responses to calls made to the Consumer Data Right Register, data holders and data recipients. These can be used to inform development work for prospective data recipients and data holders.

The ACCC is developing a Conformance Test Suite which will include tests to call the Consumer Data Right Register, data holders and data recipients to ensure information security profile and consent arrangements conform to the Consumer Data Standards and Consumer Data Right Register design. However it will only be made available to participants (accredited persons or data holders) who are in the process of onboarding to the ecosystem. It won't be publically available as a sandbox.

How do I create an account on the Consumer Data Right participant portal?

In order to apply for accreditation, an applicant's primary business contact must first set up an account through the Consumer Data Right participant portal. The Consumer Data Right participant portal is the online mechanism through which an applicant must complete and submit an accreditation application. The Consumer Data Right participant portal is also the place for Consumer Data Right participants to update and manage their information and view the Register of Accredited Persons.

The applicant's primary business contact must be an office holder of the applicant who is listed on the applicant's business record as confirmation that the person creating the account has the requisite authority to act on behalf of the applicant.

As part of creating this account, the office holder must verify their identity. Detailed information about creating an account and verifying the office holder's identity will be provided in a separate guide and included on the Consumer Data Right website upon release of the Consumer Data Right participant portal.

Once the account creation form is completed and the officer holder's identity has been verified an activation code will be sent to the office holder to confirm the account. This will then allow the office holder to log into the Consumer Data Right participant portal to complete the relevant accreditation form and submit it to the Data Recipient Accreditor for assessment. Alternatively, the office holder may nominate an additional or alternative primary business contact to complete the accreditation application.

Can intermediaries and third parties participate in the Consumer Data Right ecosystem?

While the Consumer Data Right Rules do not currently provide for the use of third party service providers who collect or facilitate the collection of Consumer Data Right data on behalf of accredited persons (intermediaries),the ACCC anticipates amending the Consumer Data Right Rules in the near future (subject to consent from the Treasurer). The

Data Recipient Accreditor will accept applications from entities who plan to use outsourced service providers to collect data. However, such entities will only be onboarded after relevant amendments take effect. Further information about the proposed changes will be available shortly.

1.2. Sharing data

How do I, as a data holder, share product reference data? Do I need to register on the Consumer Data Right Register to do so?

A data holder is required to share product reference data in accordance with Schedule 3 of the Consumer Data Right Rules and is not required to register on the Consumer Data Right Register in order to do so. A data holder is required to be registered on the Consumer Data Right Register to share Consumer Data Right data in response to a request from an accredited person. Data holders will need to complete this registration process via the Consumer Data Right participant portal.

1.3. Reciprocal data holder obligations

An accredited person (ADIs and non ADIs) may be subject to reciprocal data holder obligations. This means that an accredited person may be required to share particular Consumer Data Right data at particular times in accordance with the obligations of a data holder under the Consumer Data Right Rules, separate to the obligations of an accredited person.

Reciprocity under the Consumer Data Right Rules applies in respect of Consumer Data Right data that is:

- generated and held by or on behalf of an accredited person and
- where the data is generated in respect of a product that is publicly offered by the accredited person to consumers and generally known as one of the types of products in Phase 1, Phase 2 or Phase 3 products.

For example, a non-bank lender that is accredited may become a reciprocal data holder in respect of data they generate for their personal loan products. A non-bank accredited person that provides a budgeting app, but does not offer any of the banking-like products listed in Phase 1, Phase 2 or Phase 3, will not be a reciprocal data holder.

Reciprocal data holders will need to complete their registration as a data holder via the Consumer Data Right participant portal.

1.4. Accreditation criteria

Applicants are encouraged to refer to our Accreditation Guidelines when preparing an application. You may also find the OAIC's guidance on the privacy standards (here) and the Consumer Data Standards (here) helpful.

1.5. Fit and Proper Person criteria

What associated persons are required to be disclosed for the purposes of the fit and proper person criteria?

The *Corporations Act 2001 (Cth)* clearly sets out the definition of associated persons (section 11) and associated entitles (section 50AAA) and should be referred to when identifying an applicant's associated persons. If the person is an individual this will require

providing the full name, date of birth and contact details for that person. When completing the application each fit and proper person question in the application form must be answered in relation to the applicant and each associated person. Applicants should also include:

- a current corporate structure chart which identifies the applicant, its subsidiaries, relevant related bodies corporate and all companies in which the applicant or its subsidiaries hold minority shareholdings that are involved in the relevant business; and
- a current organisation chart which identifies the full name and title of the applicant's senior management who have the capacity to make decisions affecting the management of Consumer Data Right data.

1.6. Information Security

What type of assurance report is suitable to meet the information security requirements for accreditation?

The required assurance report must be prepared in accordance with the Australian Standard on Assurance Engagements (ASAE) 3150 *Assurance Engagement on Controls* standard, or an accepted comparable standard, and must address all aspects of the information security obligation and control requirements specified at Schedule 2 of the Consumer Data Right Rules. ASAE 3150 is an Australian method of auditing and reporting.

The following are accepted comparable standards for assurance reports:

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

When applying for accreditation, an applicant may also seek to use an existing assurance report prepared in accordance with ASAE 3150, or one of the accepted comparable standards. However, the existing report must be no more than 6 months old at the time of submission of the accreditation application, and if it contains only partial coverage over the required controls in Schedule 2 while require certain treatment for acceptance. See our Supplementary Accreditation Guidelines on Information Security for further information.

Is an ISO 27001 certification sufficient to fulfil the information security requirement for accreditation?

An ISO 27001 certification does not meet the information security requirement for accreditation. ISO 27001 is a standard for implementing an information security management system, and an ISO 27001 certification attests that the organisation uses this framework to manage security and has certain controls in place. However the certification does not give assurance that these controls are designed effectively or adequately to mitigate the risk of an information security breach or incident. Nor does an ISO certification meet the information security requirements specified in Schedule 2 of the Consumer Data Right Rules as it can be implemented at different organisations in different ways and it does not require a minimum baseline for each control.

1.7. Internal Dispute Resolution

Do non-financial service providers need to comply with Regulatory Guide 165?

Applicants for accreditation who are not financial services providers are required to develop an internal dispute resolution policy compliant with the Australian Securities and Investments Commission's Regulatory Guide 165 *Licensing: Internal and External Dispute Resolution*, as in force from time to time, which is tailored to their business.

1.8. External Dispute Resolution

Do non-financial service providers need to be members of Australian Financial Complaints Authority (AFCA) in order to be accredited?

AFCA is the recognised external dispute resolution scheme for the banking sector. Applicants for accreditation must have a membership to AFCA. AFCA will receive applications for membership from non-financial service providers. Presently the only accepted external dispute resolution body is AFCA.

Information on the process for applying for AFCA membership as a non-financial services provider in the banking sector is set out in the Accreditation Guidelines.

1.9. Local agent

When a foreign entity applies for accreditation, what local agent details are required?

If a foreign entity wishes to apply for accreditation under the Consumer Data Right regime they must have a local agent, and as part of accreditation process provide their local agent's physical and electronic addresses for service.

1.10. Insurance

What constitutes adequate insurance to participate in the Consumer Data Right ecosystem?

An accredited person is under an ongoing obligation to maintain adequate insurance, or a comparable guarantee, relevant to the nature and extent of their management of Consumer Data Right data.

The objective of the insurance obligation is to ensure an accredited person has adequate insurance in light of the risk of Consumer Data Right 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 Consumer Data Right data.

Accredited persons will have different businesses and risks. These differences will affect what insurance cover is adequate. An accredited person will need to undertake their own analysis in order to determine what is adequate for them.

Without limiting the matters that the Data Recipient Accreditor may have regard to, the matters set out in Table 1 of our Supplementary Accreditation Guidelines on Insurance are matters that the Data Recipient Accreditor is likely to take into account in considering whether the applicant would, if accredited, be able to comply with the insurance obligation. These matters, as well as any other relevant matters, should be addressed in an applicant's written statement submitted for accreditation.

See our Supplementary Accreditation Guidelines on Insurance for further information.

1.11. Consumer Data Right Policy

If an applicant already has an information security policy and a privacy policy is a separate Consumer Data Right policy required?

Applicants must have a Consumer Data Right policy distinct from any existing privacy or information security policy (per rule 7.2(2) of the Consumer Data Right Rules). Any document prepared for the purpose of an accreditation application must specifically address Consumer Data Right requirements as set out in the Consumer Data Right Rules and guidelines, including the OAIC's guidance on Privacy Safeguard 1.

What format should the Consumer Data Right policy be in? Does it have to be a document or can it be another format?

Rule 7.2(2) of the Consumer Data Right Rules states that a Consumer Data Right policy must be in the form of a 'document', the definition of which is considered broadly. Applicants must, however, be able to provide hard copies of their Consumer Data Right policies if requested to do so (see clauses 7.2(2), 7.2(8) and 7.2(9) of the Consumer Data Right Rules).

Does the Consumer Data Right policy need to be accessible via all online channels or just those channels that Consumer Data Right consumers will be using for Consumer Data Right activities?

Access to the Consumer Data Right policy must be provided via each online service through which a Consumer Data Right participant deals with Consumer Data Right consumers (see clause 7.2(8) of the Consumer Data Right Rules). If a Consumer Data Right participant deals with Consumer Data Right consumers through a particular channel, such as internet banking, then the Consumer Data Right policy must be available through that channel.