Australian Government

Consumer Data Right

Participant Portal User Guide

Register and Accreditation Application Platform

Table of Contents

1 Glossary 6
2 About the Participant Portal 9
2.1 Overview 9
2.2 Services available in the Participant Portal 9
3 Creating a Participant Portal account 10
3.1 Who can create a Participant Portal account? 10
3.2 Information needed to create a Participant Portal account 10
3.3 Complete the request to create an account in the Participant Portal - local entities 11
3.4 Complete the request to create an account in the Participant Portal - foreign entities 18
3.5 Activate your Participant Portal account 28
4 Logging into the Participant Portal 30
5 Managing users in the Participant Portal 31
5.1 Inviting participants 31
5.2 Users across multiple legal entities 32
5.3 Modifying a user's access 33
5.4 Removing a user's access 34
6 Data holders 36
6.1 Complete data holder registration 36
6.2 Reciprocal data holder obligations 37
7 Data recipients 38
7.1 Accreditation levels 38
7.1.1 Unrestricted 38
7.1.2 Sponsored 38
7.2 Accreditation application 38
7.2.1 Start an accreditation application 38
7.2.2 Edit your application 39
7.2.3 Finalise and submit your application 40
7.2.4 Withdraw a draft application 41

7.2.5 Withdraw a submitted application 41
7.2.6 Incomplete applications 42
7.3 Other change requests 42
7.4 Surrender accreditation 44
7.4.1 Submit a request to surrender accreditation 44
7.4.2 Withdraw your request to surrender accreditation 44
8 Post accreditation or registration 46
9 Manage organisation details 48
9.1 Maintain organisation details 48
9.2 CDR representative arrangement notification 49
9.2.1 Notify a new CDR representative arrangement 49
9.2.2 Edit or end a representative arrangement 50
9.3 CDR sponsorship arrangement notification 50
9.3.1 Notify a new sponsorship arrangement 51
9.3.2 Notify the end date of a sponsorship arrangement 51
9.3.3 View sponsorship arrangements 52
10 Manage participation details 53
10.1 Maintain brand details 53
10.1.1 Add a new brand 53
10.1.2 Modify an existing brand 57
10.2 Maintain brand participation details 62
10.2.1 Add new brand participation 62
10.2.2 Modify existing brand participation details 67
10.3 Progression to consumer data sharing 71
10.3.1 Certificate details 74
10.3.2 Authentication details 75
10.3.3 Endpoints 76
10.3.4 Validate Production Details 78
10.4 Maintain software product details 82
10.4.1 Adding new software products 82
10.4.2 Maintaining existing software products 83

10.5 Maintain Public Key Infrastructure (PKI) certificates 90
10.6 Server certificates 91
10.6.1 Request a server certificate 91
10.6.2 Server certificate - CSR Validation 94
10.6.3 Server certificate - Renew a certificate 98
10.6.4 Server certificate - Revoke a certificate 99
10.7 Client certificates 102
10.7.1 Request a client certificate 102
10.7.2 Client certificate - Renew a certificate 105
10.7.3 Client certificate - Revoke a certificate 107
10.8 CTS Certificates 108
10.8.1 Request a CTS certificate 108
10.8.2 Renew a CTS certificate 109
10.8.3 Revoke a CTS certificate 110
10.8.4 Obtain a valid production certificate 111
10.8.5 Maintain authentication details 112
10.8.5.1 Renew a CTS certificate 115
10.8.6 Obtain a valid production certificate 115
10.8.7 Maintain authentication details 116
11 Maintain Conformance Test Suite (CTS) details 118
11.1 View CTS details 118
11.2 Submit CTS Enrolment 120
11.3 Maintain CTS certificates 121
11.3.1 Request a CTS certificate 121
11.3.1.1 Data Holder Server CTS Certificate type default screen 123
11.3.1.2 Data Recipient Client CTS Certificate type default screen 124
11.3.2 Receive CTS certificate 124
11.3.2.1 Successful submission 124
11.3.2.2 Unsuccessful submission 127
11.3.3 Download CTS certificate 128
11.3.4 Revoke a CTS certificate 128

11.3.5 Renew a CTS certificate 130
11.4 Maintain CTS authentication details 134
11.4.1 Submit CTS authentication details 134
11.4.2 View CTS authentication details 135
11.5 Maintain CTS endpoints 136
11.5.1 Submit CTS endpoints 136
12 Rule 9.4 reporting 138
12.1 Lodging a rule 9.4 report on the Participant Portal 138
12.1.1 Start and submit a rule 9.4 report 138
12.1.2 Edit a rule 9.4 report 140
12.1.3 Download a rule 9.4 report 140
12.2 Amend a submitted report 141
13 Schedule 1 reporting 143
13.1 Lodging a Schedule 1 report on the Participant Portal 143
13.1.1 Start and submit a Schedule 1 report 143
13.1.2 View a submitted Schedule 1 Historical report 144
13.1.3 Edit a submitted Schedule 1 Historical report 145
14 Getting help 147
15 Appendix: User roles and permissions 148

1 Glossary

Term	Definition
Accredited person	An accredited person means a person who has satisfied the Data Recipient Accreditor that it meets the criteria for accreditation specified in the Consumer Data Right Rules and has been accredited by the Data Recipient Accreditor.
Accreditor	Data Recipient Accreditor – currently the Australian Competition and Consumer Commission.
ACCC	Australian Competition and Consumer Commission
ADI	Authorised deposit-taking institution
ADR	Accredited data recipient
AFCA	Australian Financial Complaints Authority
Affiliate	A person accredited to the sponsored level and in a sponsorship arrangement is known as an affiliate of its sponsor. A person does not need to have sponsored accreditation to enter into a sponsorship arrangement as an affiliate, but will need it to make the consumer data requests.
Applicant	A person who submits an application for accreditation as an accredited person.

Associated person	A person involved/or could be involved, or who would be involved if accredited, in decision making by the applicant or accredited person or who has the ability to significantly impact another person's management of CDR data. For a body corporate – an associate of another person or associated entity has the meaning given to it under the *Corporations Act 2001.*
CDR	Consumer Data Right
CDR Participant Portal	The online mechanism to create a CDR portal account, complete and submit an accreditation application, register as a data holder, manage and update a participant's information.
CDR Register	Register of Accredited Persons
CDR Rules	*Competition and Consumer (Consumer Data Right) Rules 2020*
Data holder	A holder of CDR data.
Participant	A data holder or an accredited data recipient participating in the CDR regime.
Sponsor	An Unrestricted ADR who has entered into a sponsorship arrangement with a sponsored ADR. The Sponsor must collect data for the Affiliate. A Sponsor can have many affiliates.

Sponsored Accredited Data Recipient (Sponsored ADR)	A Data Recipient who is able to obtain consent from consumers to receive their data, however they cannot collect data directly from a data holder and must do this through an unrestricted accredited data recipient (Unrestricted ADR) with consumers' consent when a sponsorship arrangement is in place.
Sponsorship Arrangement	A sponsorship arrangement is a written contract between a person with unrestricted accreditation (the *sponsor*) and another person (the *affiliate*).
Unrestricted Accredited Data Recipient (Unrestricted ADR)	A Data Recipient who is able to obtain consent from consumers and collect data from data holders without any restrictions for all designated sectors.

2 About the Participant Portal

2.1 Overview

The Consumer Data Right (CDR) aims to give consumers greater access to and control over their data. It will improve consumers' ability to compare and switch between products and services, and will encourage competition between service providers, leading not only to better prices for customers but also more innovative products and services. Banking is the first sector to be brought into the CDR.

The CDR Participant Portal (Participant Portal) is the online mechanism through which a data holder can complete the data holder registration process and a legal entity/person can complete and submit an application to become an accredited data recipient. The Participant Portal is also the place for CDR participants - data holders and accredited data recipients - to update and manage their information and view the CDR Register of Accredited Persons (CDR Register).

This guide aims to provide information and guidance to assist CDR participants on the key features of the Participant Portal.

For more information, visit the https://www.cdr.gov.au/.

> **Note:** Before you make the initial request to access the Participant Portal for your organisation, it is highly recommended you read this guide to ensure you have all the relevant details at hand.

2.2 Services available in the Participant Portal

The Participant Portal can be used by an organisation to:

- register as a data holder
- submit an application for accreditation
- invite and manage users
- manage an organisation's details
- manage brands and software products.

3 Creating a Participant Portal account

3.1 Who can create a Participant Portal account?

Only potential CDR participants need a Participant Portal account. An initial primary business contact is responsible for creating an account for their legal entity through the Participant Portal. See the Appendix of this guide for more information about the primary business contact.

> **Note:** The initial primary business contact for a legal entity must be a person who is listed on the organisation's Australian Securities and Investments Commission (ASIC) or Australian Business register record (ABR), or the equivalent foreign business record if the organisation is a foreign entity. For example, a director, company secretary or an authorised contact listed on the organisation's business record.

3.2 Information needed to create a Participant Portal account

A primary business contact will need the following information to create an account.

Organisation details

- Your organisation's ABN or ACN (for Australian entities). You can use the search box in the request form to match your ABN or ACN with the corresponding ABR/ASIC record in order to progress your account creation in the Participant Portal . For non-Australian entities you will need your relevant business registration number.
- Your Personal details - Only an authorised contact or office holder of the organisation can make a request to create a CDR Participant Portal account. An authorised contact or office holder is a director, company secretary, associate or a person listed on the organisation's Australian Business Register / ASIC record.
  Please ensure that you are an authorised contact or office holder for your organisation and your personal details entered in the form match your personal details as recorded in your organisation's Australian Business Register record or Australian Securities & Investments Commission record.
  If these authorised contacts are out of date, please update your business details on the relevant business register. If your organisation's authorised contacts have recently been updated on the ASIC/ABR business register, it may take up to 4 weeks for the changes to be reflected in our business database before we can verify your organisation's details.
- Organisation address - The registered address for service must be a physical address associated with your organisation, it cannot be a PO Box. If the service of notice address in your organisation's Australian Business Register or ASIC record is a PO Box, please update it to a physical address.
  If your organisation's address for service has recently been updated with the Australian Business Register or ASIC record, it may take up to 4 weeks for the changes to be reflected in our business database before we can verify your organisation's details. Your organisation's registered business address (e.g. principal place of business) may be the same as your registered address for service.
- The electronic address for service for your organisation (i.e. email).

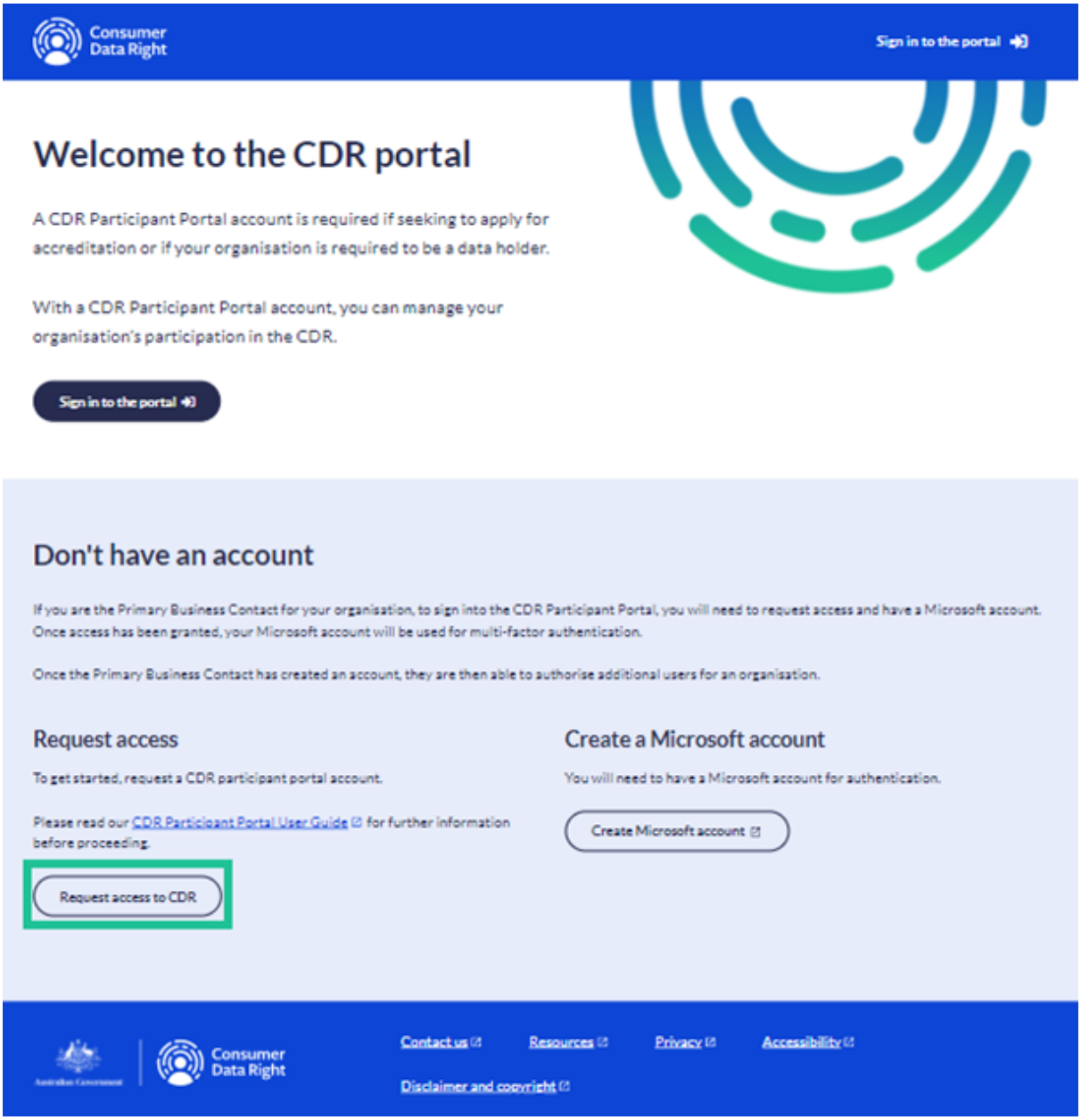
- Whether your organisation is a foreign entity. If your organisation is a foreign entity, you will be required to have a local agent and provide their electronic and physical addresses for service.

Initial primary business contact details

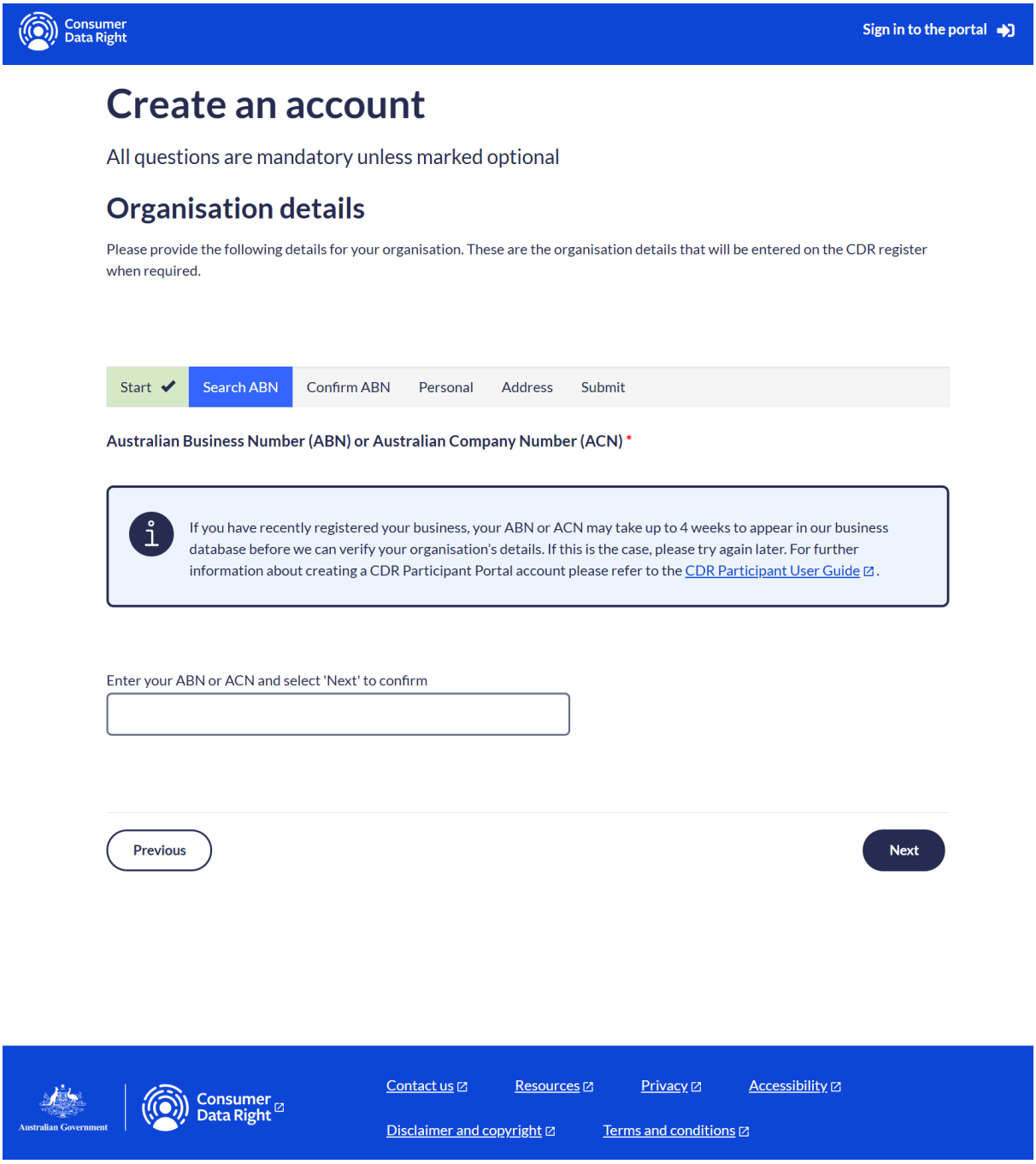
- the initial primary business contact's email address
- the initial primary business contact's mobile phone number.

3.3 Complete the request to create an account in the Participant Portal - local entities

1. To complete the request to create an account in the Participant Portal as an initial primary business contact, open an internet browser and navigate to https://portal.cdr.gov.au . The website works best on Microsoft Edge, Internet Explorer version 11, or Chrome on Windows and Safari, or Firefox on Mac OS.
2. Select **Request access to CDR**.



3. Complete all mandatory questions on the form (all questions are mandatory unless marked optional).
4. Search by your company ABN or ACN. On clicking Next, the system will validate your details against ABN/ASIC business records to find a match. If you have provided invalid details, you will be notified with a message including the option to search again.



5. Confirm the ABN/ACN details and click on Next.
6. Complete the personal details section by answering all questions and mandatory fields. On clicking Next, the system will validate your details against ABN/ASIC business records to find a match. If you have provided invalid details, you will be notified with a message including the option to update details again.

All questions are mandatory unless marked optional

Organisation details

Please provide the following details for your organisation. These are the organisation details that will be entered on the CDR register when required.

Start ✔ | Search ABN ✔ | Confirm ABN ✔ | Personal | Address | Submit

Personal details

Only an authorised contact or office holder of the organisation can make a request to create a CDR Participant Portal account. An authorised contact is a person listed on your organisation's Australian Business Register record (ie ABN), and an office holder is a director or company secretary listed on the organisation's Australian Business Register record (under "Associates") or on your organisation's Australian Securities & Investments Commission record (ie ACN). If these authorised contacts or office holders are out of date, please update your business details on the relevant business record.

If your organisation's authorised contacts or office holders have recently been updated on the relevant business record, it may take up to 4 weeks for the changes to be reflected in our business database and before we can verify your organisation's details.

First name *

Last name *

Contact details

Email address *

Email confirmation *

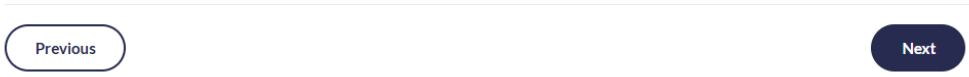
Primary mobile phone number *

Enter the primary mobile number in international format, such as +61 412 345 678

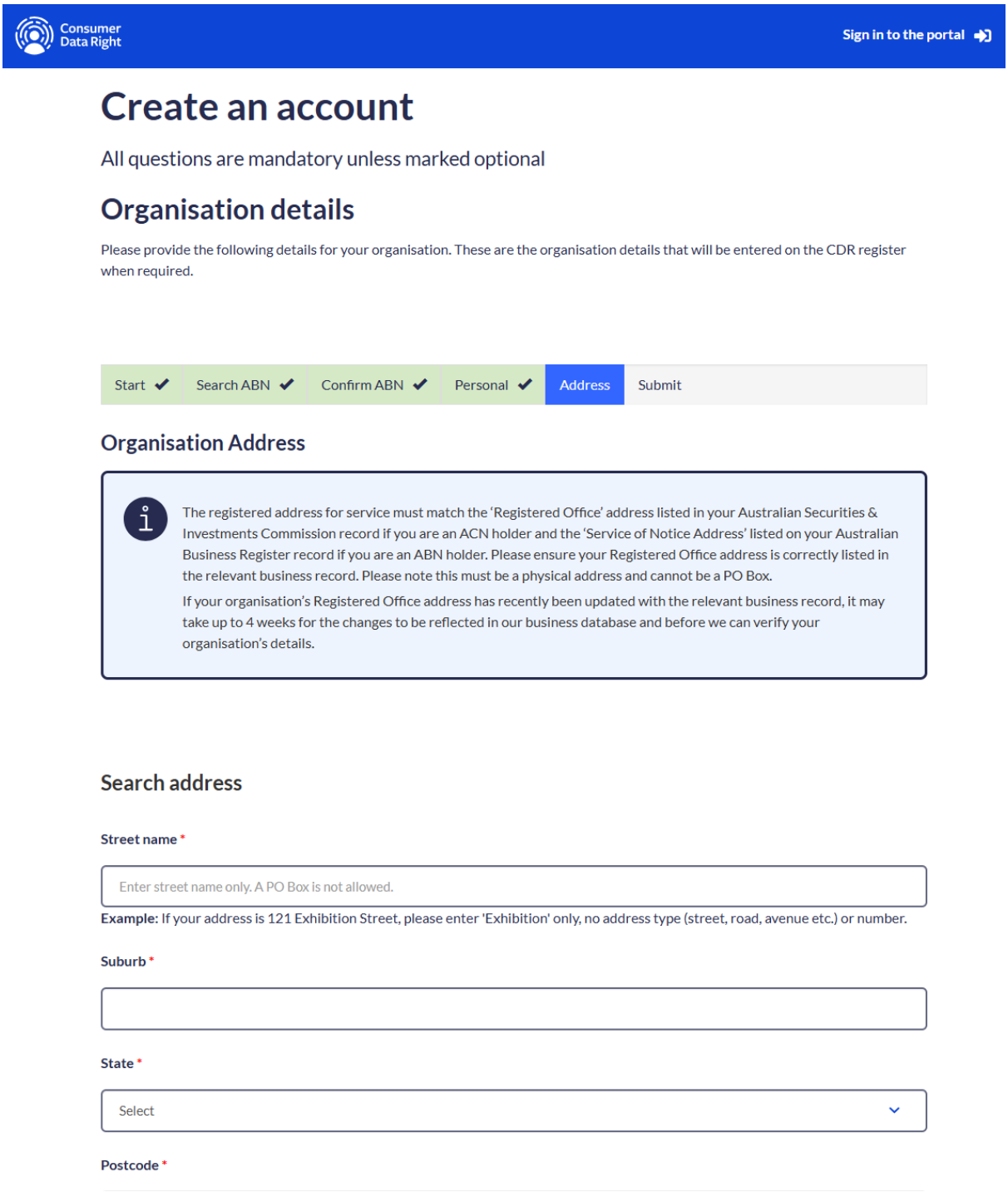
Provide a telephone number

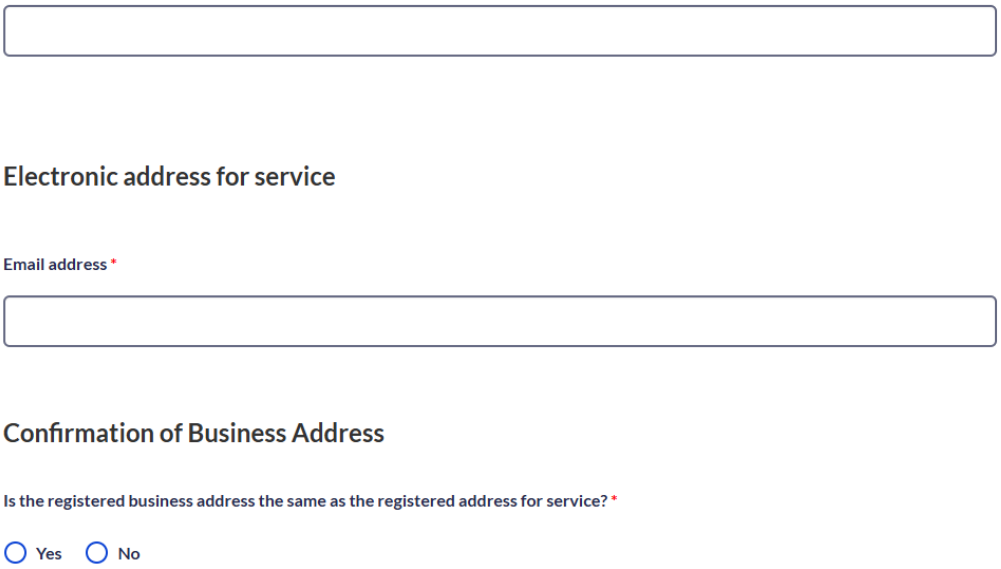
Secondary phone number (optional)

Enter the secondary number in international format, such as +61 412 345 678

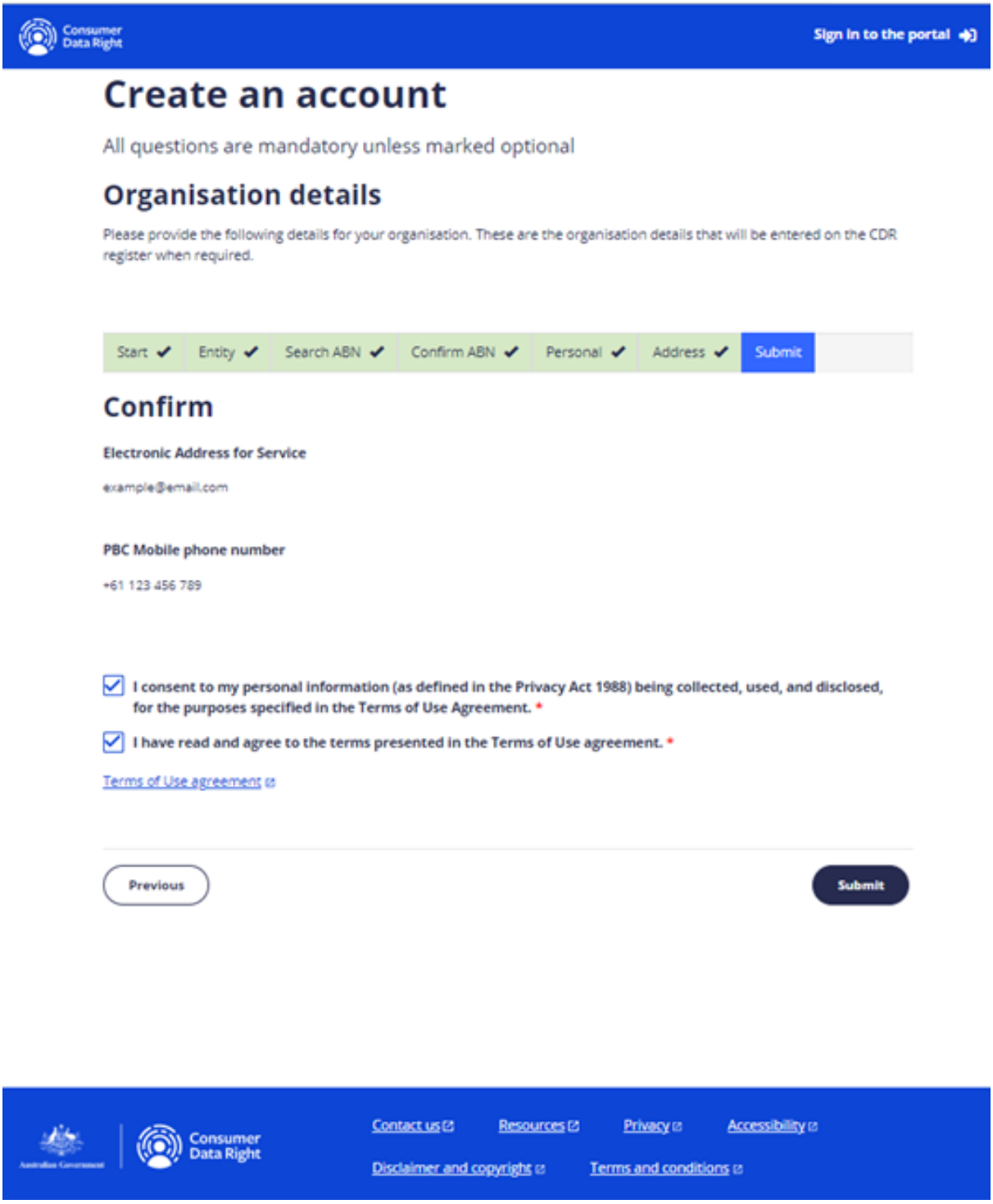


7. Under the search address section, complete the address details for each field as highlighted. Once the search fields are provided, the system will match the search address fields with ASIC/ABR business records and ask you to confirm the full address if there is a match. If you have provided invalid details, you will be notified with a message including the option to update the address details again.

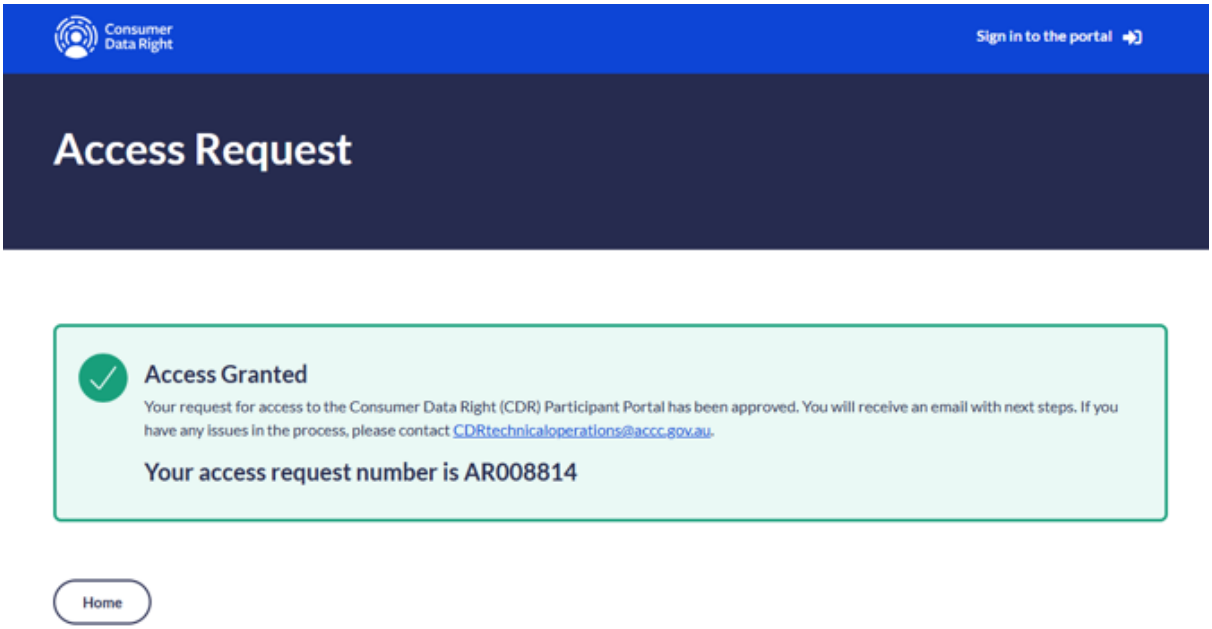




8. Submit the request to create an account. On submitting your request, the system will validate the information you have provided. If you have not answered all mandatory questions or you have provided an invalid answer, you will be notified that the form could not be submitted including the reason/s why. You then have the option to update the information and resubmit your request.



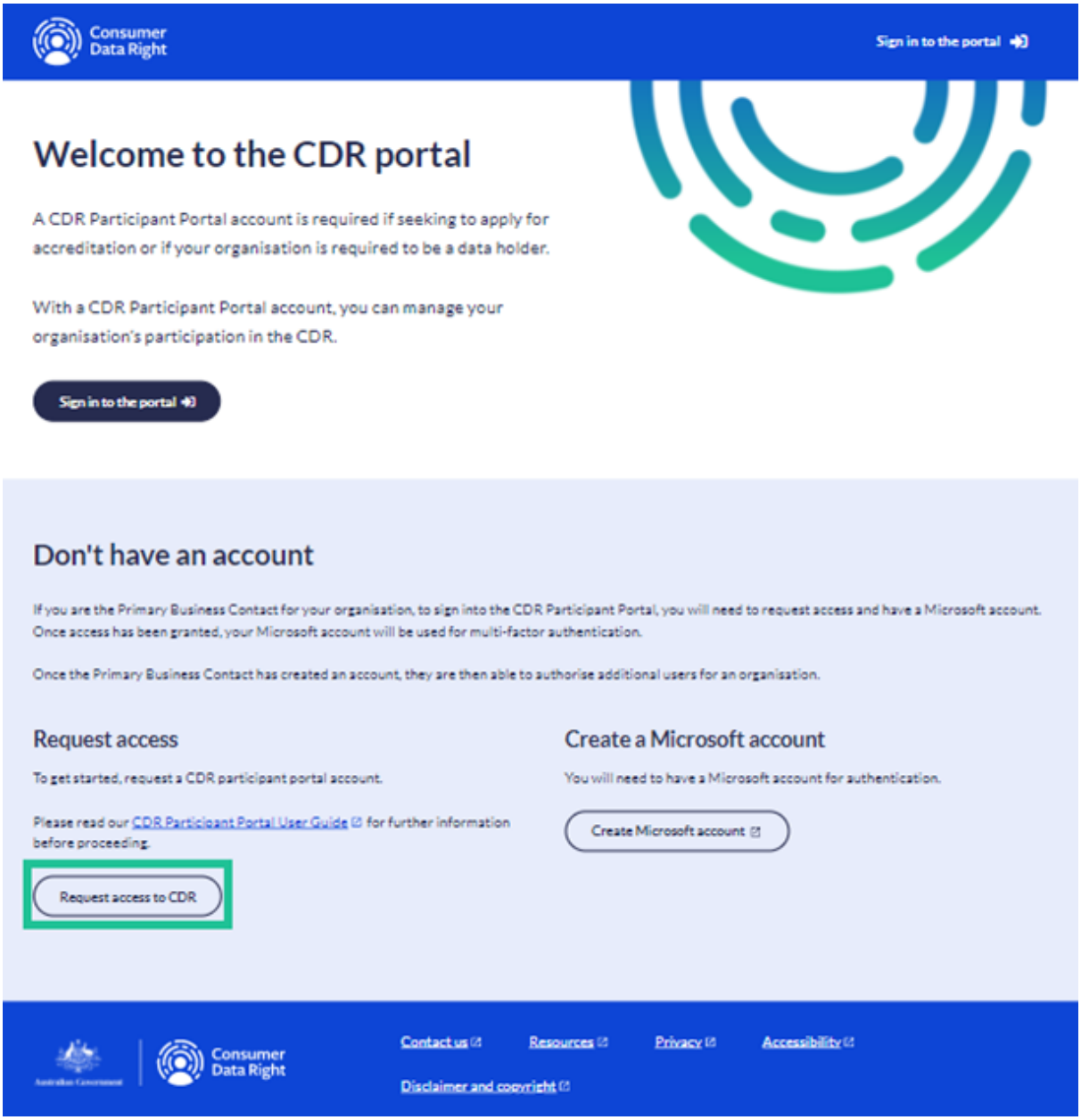
9. Once the form has been validated, you will be shown a page confirming your request has been granted with a unique ‘access request’ number.



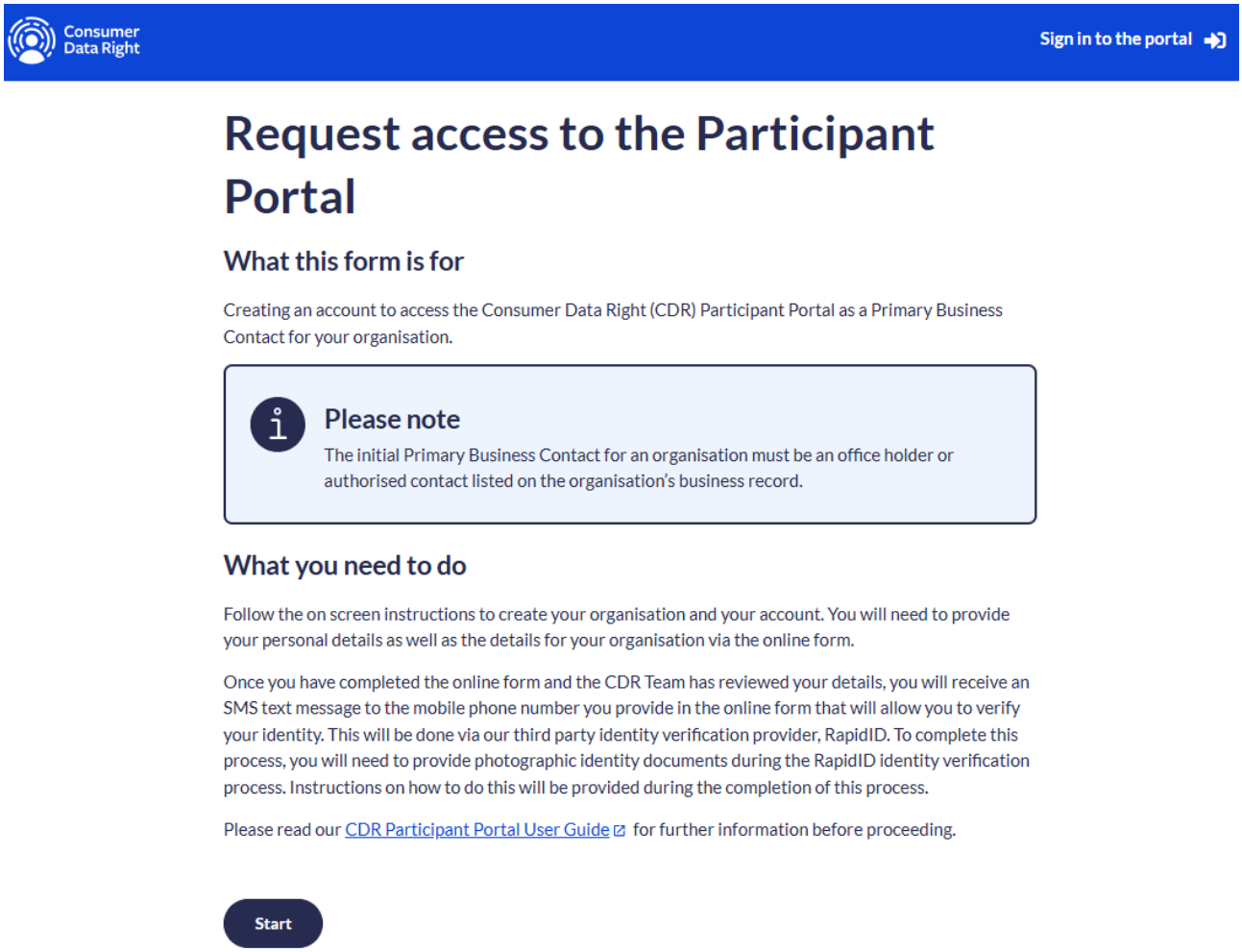
You will also receive a confirmation email with your unique access request number with further steps.

3.4 Complete the request to create an account in the Participant Portal - foreign entities

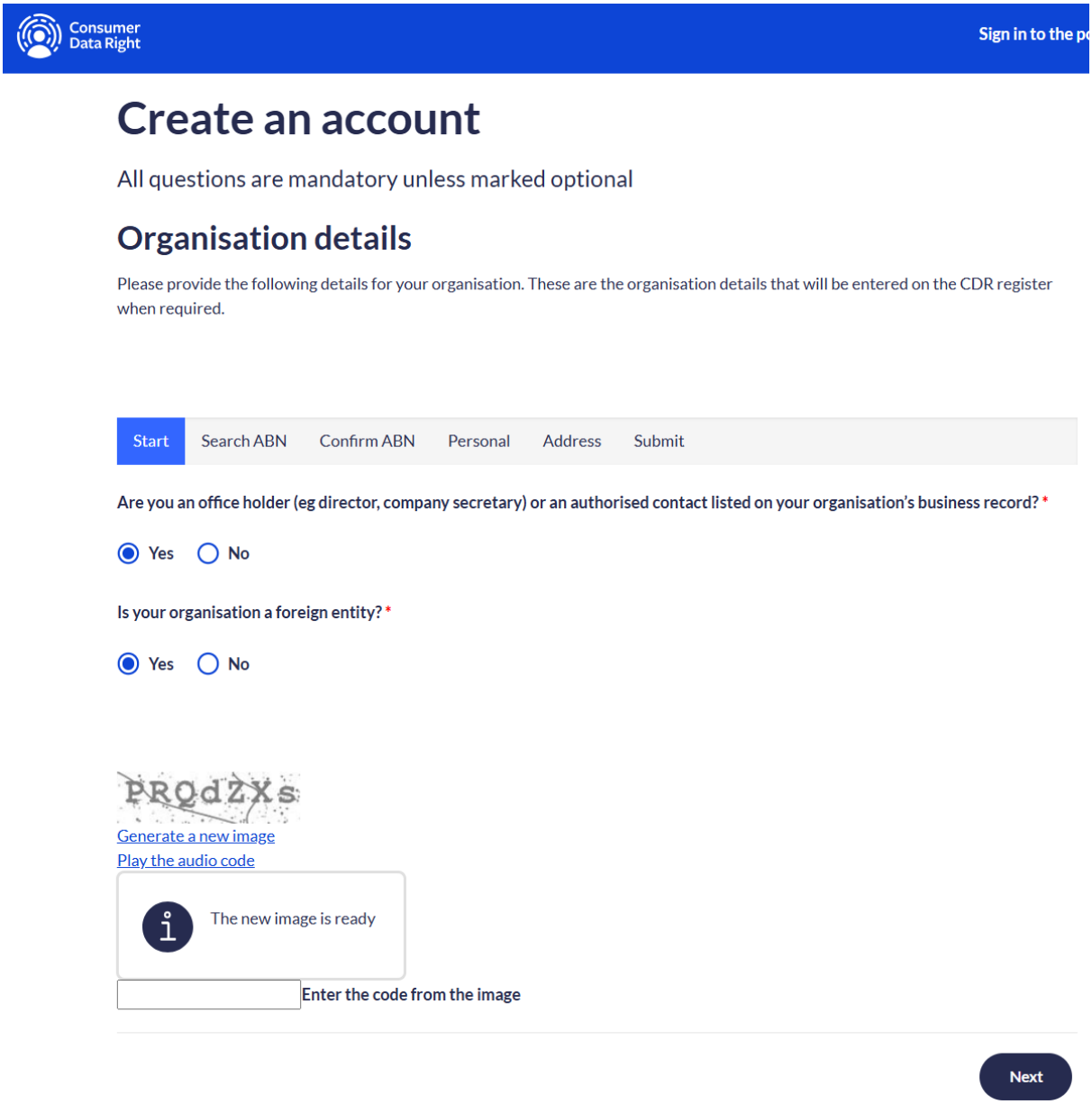
1. To complete the request to create an account in the Participant Portal as a Foreign Entity, open an internet browser and navigate to https://portal.cdr.gov.au . The website works best on Microsoft Edge, Internet Explorer version 11, or Chrome on Windows and Safari, or Firefox on Mac OS.
2. Select **Request access to CDR**.



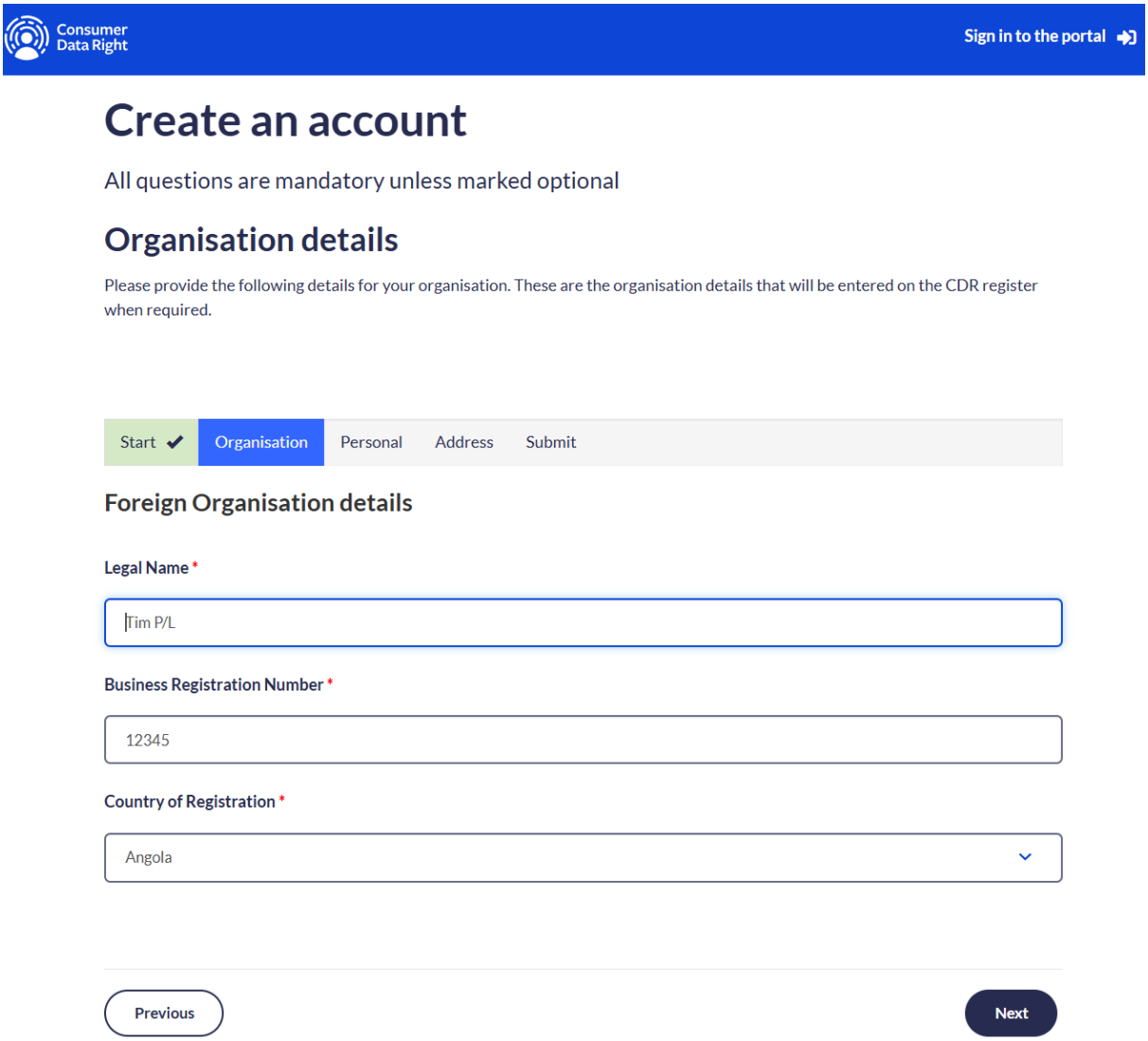
3. Select **Start.**



4. Complete all mandatory questions on the form (all questions are mandatory unless marked optional). Select your organisation as a foreign entity.



5. Complete the captcha and click Next to continue.
6. Complete the organisation details section by answering all questions and mandatory fields. the fields will accept alphanumeric values - field validation if limited due to the vast range of possibilities for foreign registration systems. Click Next to continue.



7. Under the Personal section, complete the contact details for each field. Click Next to continue.

Consumer Data Right

Sign in to the portal

Create an account

All questions are mandatory unless marked optional

Organisation details

Please provide the following details for your organisation. These are the organisation details that will be entered on the CDR register when required.

Start ✔ | Organisation ✔ | Personal | Address | Submit

Personal details

First name *

Tim

Last name *

Smith

Contact details

Email address *

tim@mail.com.au

Email confirmation *

tim@mail.com.au

Primary mobile phone number *

Enter the primary mobile number in international format, such as +61 412 345 678

+61434800000

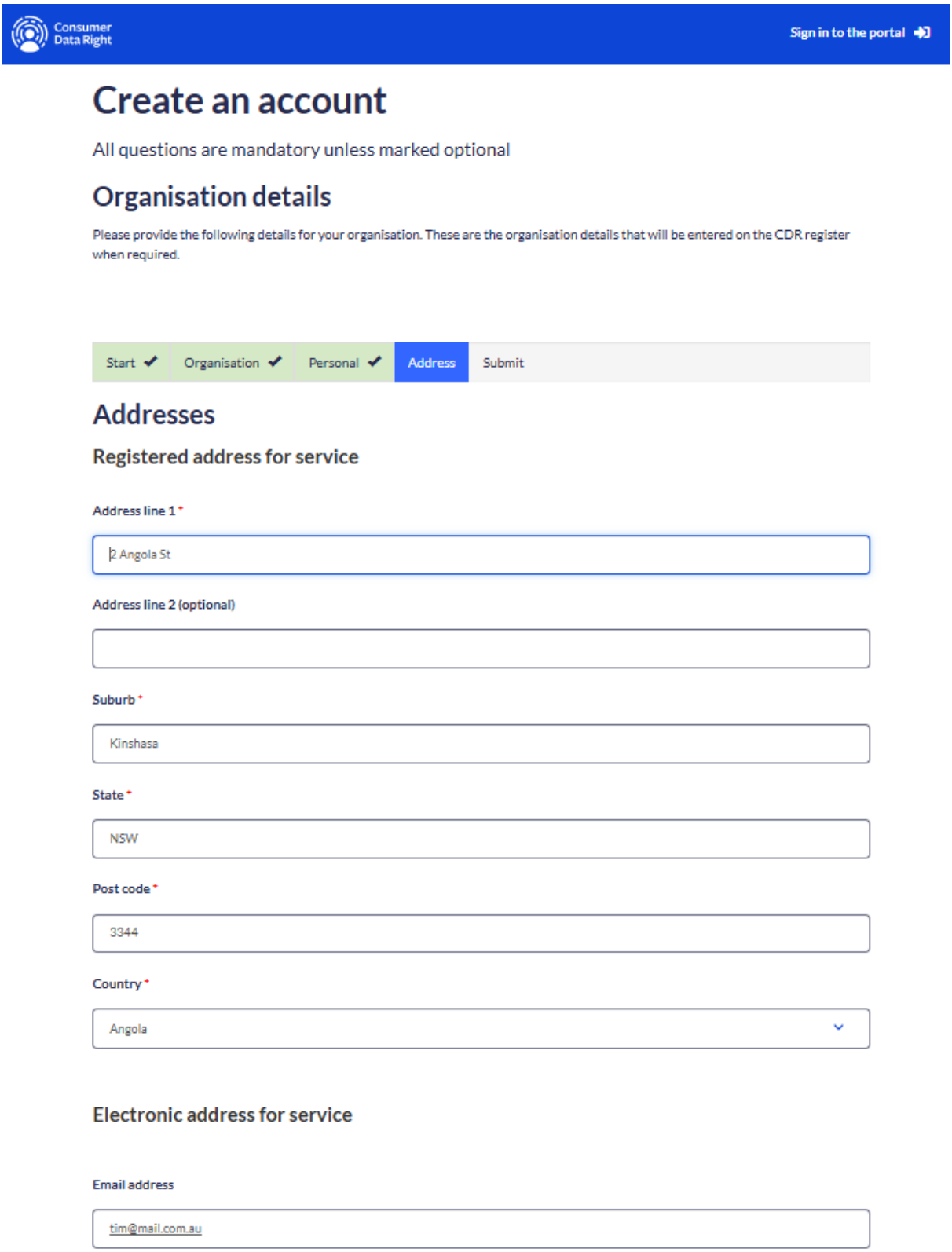
Secondary phone number (optional)

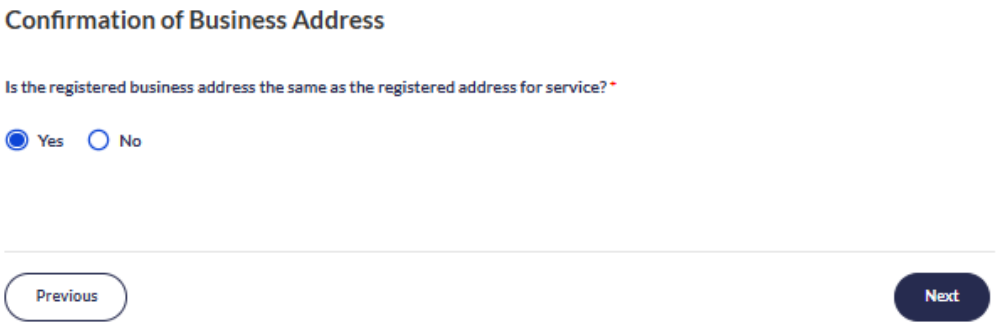
Enter the secondary number in international format, such as +61 412 345 678

Previous

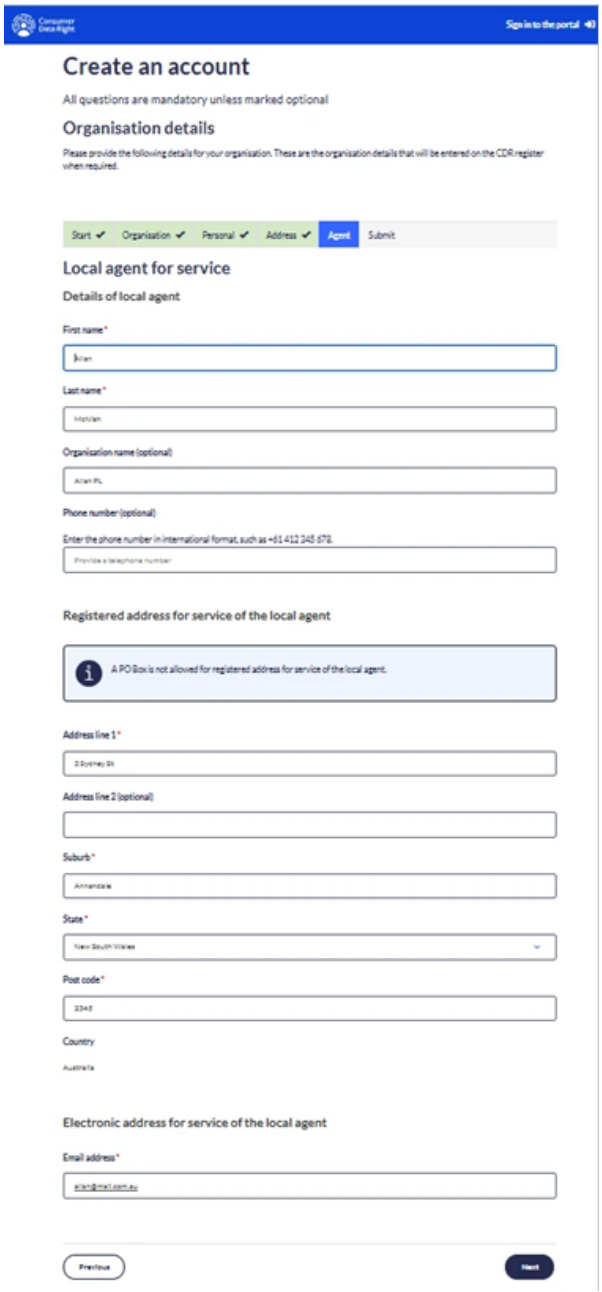
Next

8. Under the Address section, complete the contact details for each field. Click Next to continue.



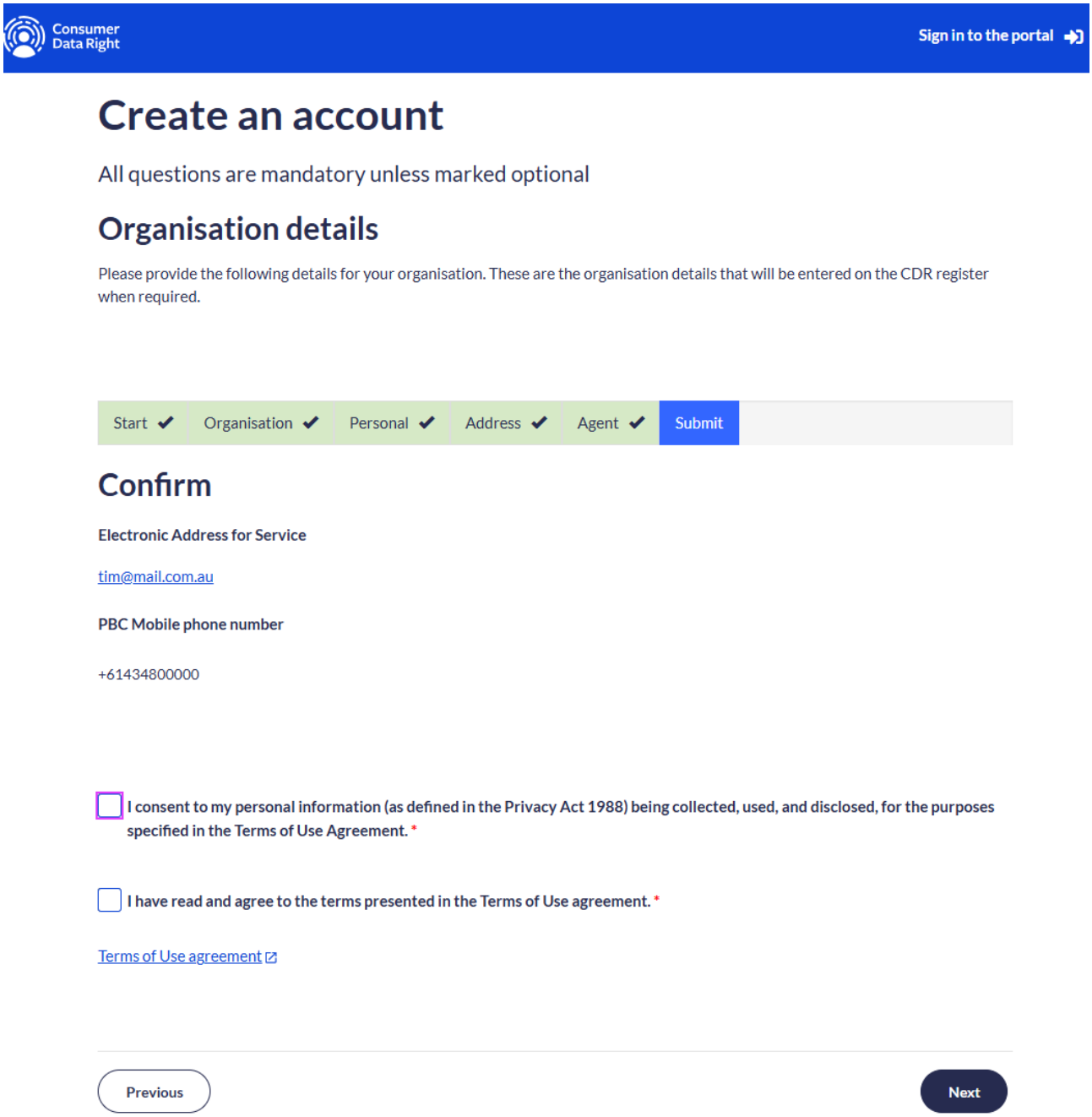


9. Under the Agent section, complete the contact details for each field. Please note that the details in this section will refer to your local (Australian) agent. Click Next to continue.

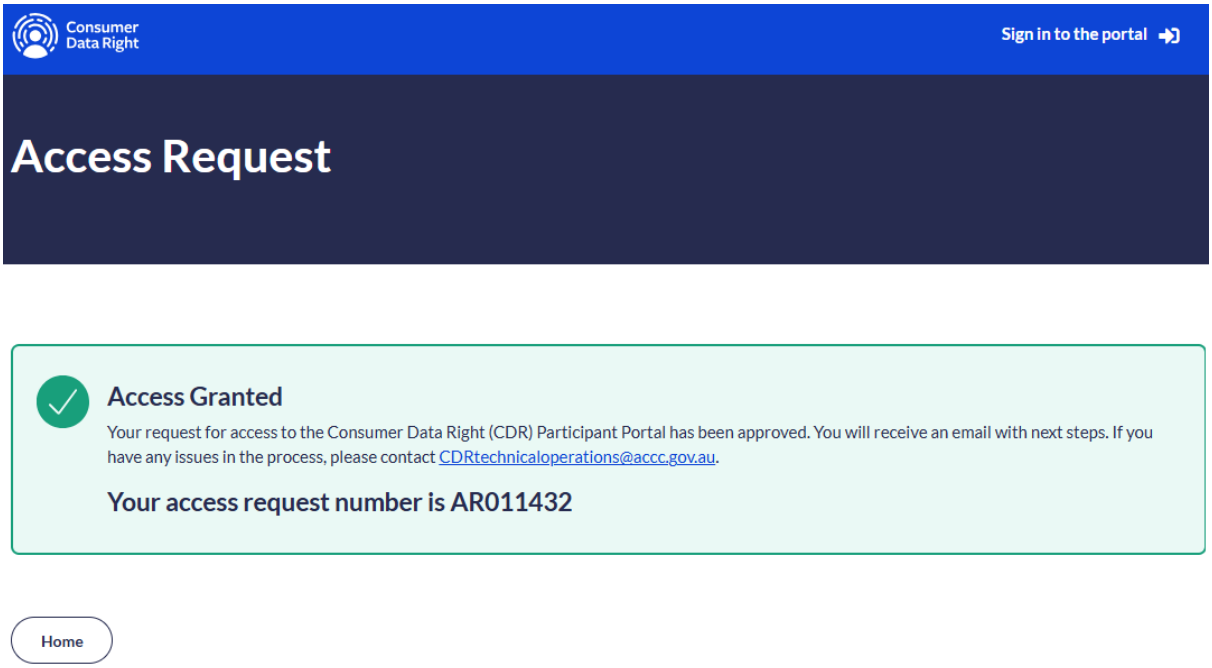


If the applicant is a foreign entity this information must include the name of the applicant's local agent and the local agent's addresses for service (both physical and electronic).

9. The system will provide a confirmation screen asking you to confirm some details of your application. Complete the fields and click Next to continue.



10. Once the form has been validated, you will be shown a page confirming your request has been granted with a unique 'access request' number.



You will also receive a confirmation email with your unique access request number with further steps.

3.5 Activate your Participant Portal account

Once your request to create an account has been approved by the CDR Team, you will receive an activation email with instructions on how to activate your account.

Follow the instructions within the activation email to activate your account.

Once your account activation process is complete, you will be able to log in to the Participant Portal. Note you must use the same email address used to create the account. If you have problems during this step, please contact us via the CDR Technical Operations mailbox CDRtechnicaloperations@accc.gov.au.

> **Note:** You have 7 calendar days to activate your account before your unique security token expires. If your token expires before you complete this step, please contact us via the CDR Technical Operations mailbox CDRtechnicaloperations@accc.gov.au.

Example email: Participant Portal account confirmation

Your CDR Participant Portal account has been created.

To activate this account, you will complete the steps below to create and/or link to a Microsoft account.

Step 1 - Creating a Microsoft account

If you do not have a Microsoft account used to register with the CDR Participant Portal, you can create one prior to proceeding. You can create a Microsoft account by clicking here and following the on-screen instructions or you can proceed through a password-less sign in if you are unable to create a Microsoft account. You do not need to complete this step if you already have a Microsoft account associated with your e-mail used to register with the CDR Participant Portal.

Step 2 - Associating your account with CDR

Please click here and sign into the CDR Participant Portal. If you are using a Microsoft Account for CDR Participant Portal access, then choose the Microsoft Account option to link your account with CDR. Otherwise, you can Sign-In with Email and use a one-time code sent to your nominated email address.

Step 3 - Setting up your Mobile Authenticator

Follow the on screen instructions to set up the Microsoft Authenticator app on your mobile device.

Step 4 - Activating your CDR Participant Portal Account

Once Step 2 and Step 3 have been completed you will be redirected back to the CDR Participant Portal and asked to provide the token below to activate your account.
Security Token

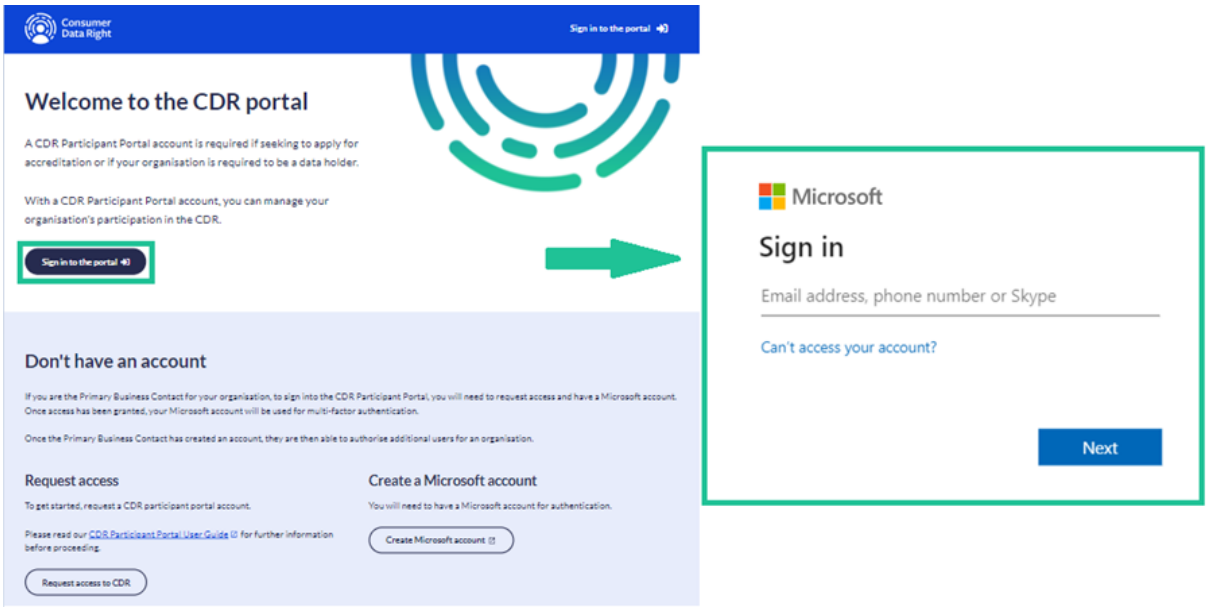
zUrp2qUG93bvMz2b2E3MZ2W-6Jr9GAfNZe6zMvWEZP-QoN1UHCiDMHs3UipzdI3kd3S06Iq0Dym5fBHW7QjxcZKLO-QPpCsGvWky61VuyfkGW-uXyCi5ZxdTlzx3twuLrTAuvug2EPTbxGymRUJd43XUHY5vsMkcCe0IQgGOA00-

Step 5 - Sign in

You can now sign into your CDR Participant Portal account.

4 Logging into the Participant Portal

1. Access the Participant Portal by opening an internet browser and navigating to https://portal.cdr.gov.au/ . The website works best on Microsoft Edge, Internet Explorer version 11, or Chrome on Windows and Safari, or Firefox on Mac OS.



2. Log in to the Participant Portal using your Microsoft account login details.
3. Every time you log in, you are required to authenticate using the Microsoft Authenticator app. If you do not have this installed or setup, refer to **step 3** in your activation email.
4. The first time you log in to the Participant Portal, you will need to enter the security token from the 'Participant Portal account confirmation' email you received. If your token expires before you complete this step, please contact us via the CDR Technical Operations mailbox CDRtechnicaloperations@accc.gov.au.

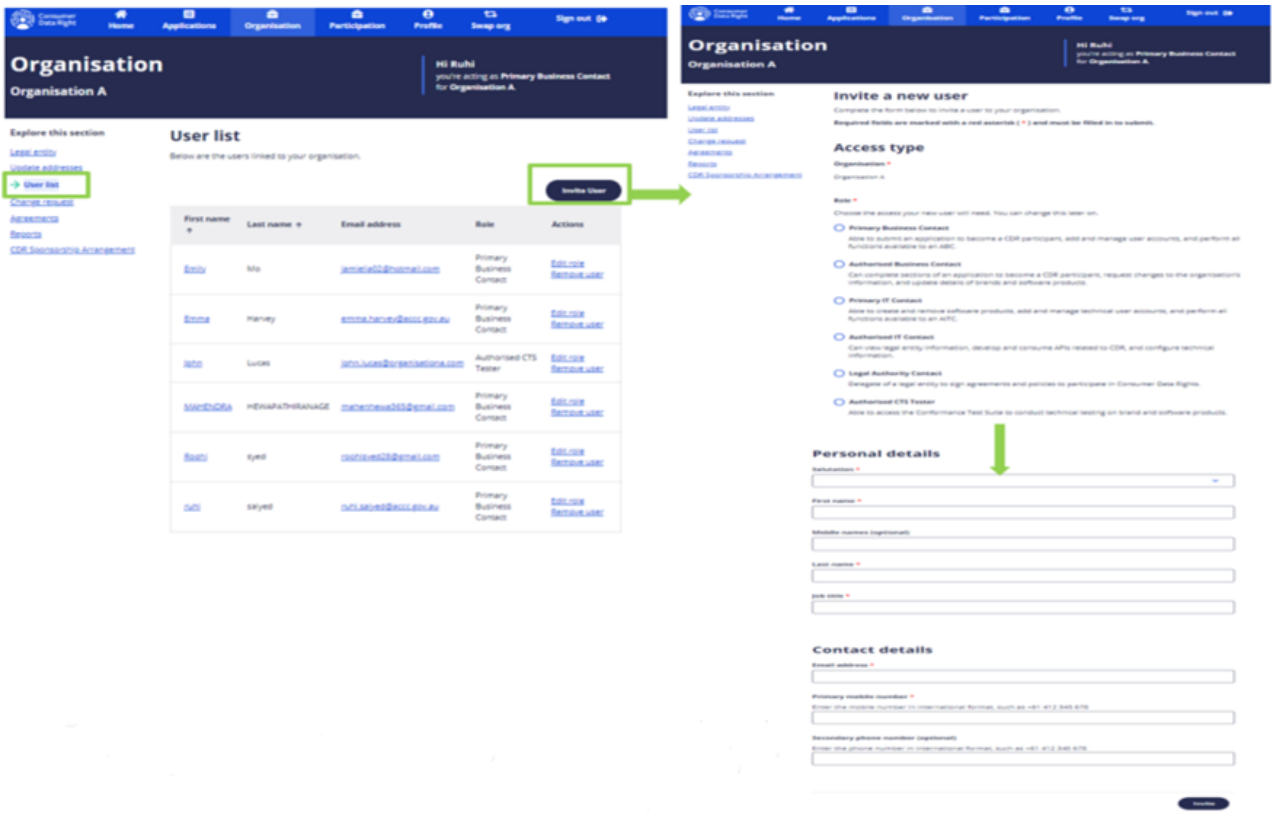
5 Managing users in the Participant Portal

The Participant Portal supports multiple user roles with different permission profiles so that participants can effectively manage their organisation's information. For more information on supported user roles, please refer to the User roles and permissions in this guide.

5.1 Inviting participants

A primary business contact can invite additional users within the organisation to have access the Participant Portal, including other primary business contacts. There may be multiple users for most roles.

1. Log in to the Participant Portal at https://portal.cdr.gov.au and select **Organisation** from the top navigation menu.
2. Select **User list** from the left side navigation menu. You will be shown a table listing all current users (first name, last name, email address and role of the person) within your organisation.
3. Select the **Invite user** button on the top right of the table.
4. The **New user** screen is displayed. From here you can invite a new user and assign an access type (role) to their account.
5. Choose the access type you want to assign to the new user. A user's role can be modified at any time.
6. Complete required fields in the form and select **Invite**.



Your invited user will receive an email requesting them to activate their Participant Portal account. New users will need a Microsoft account and need to setup and log in to the Microsoft Authenticator app to use the Participant Portal.

You will receive an email detailing the updates you made on the Participant Portal. Once invited users have activated their account, you can manage their access through the organisation's user list.

Note: To invite a user to participate in multiple entities, you can do so by selecting the swap organisation menu item at the top of the primary navigation.

5.2 Users across multiple legal entities

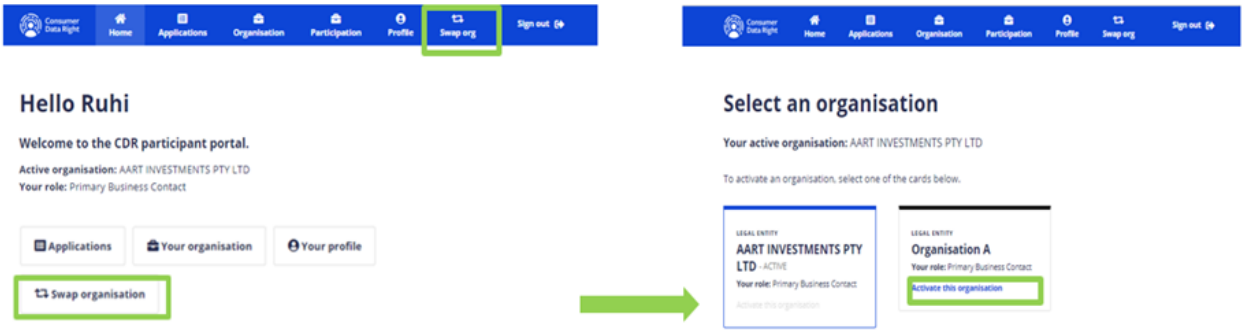
A participant may be a user for more than one organisation. For example, Jane Smith could be the primary business contact for Blue Green Pty Ltd and Purple Pins Pty Ltd both of which have Participant Portal accounts. Jane may also want key members from each organisation to participate in both Participant Portal accounts.

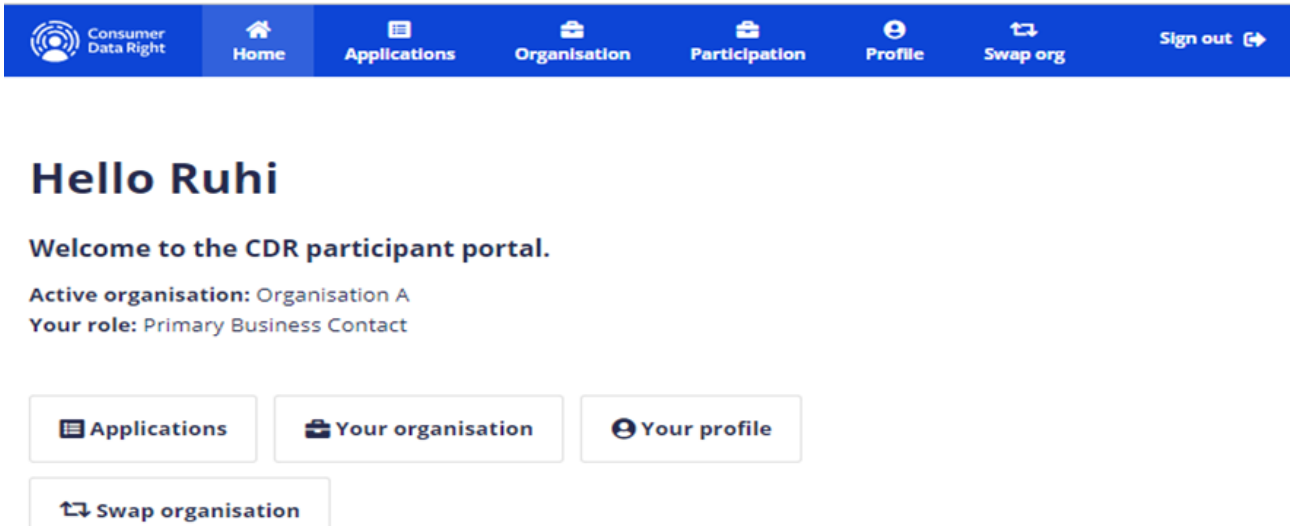
> **Note:** If there are no multiple legal entities associated with you as a user, you will not see the **Swap organisation** menu item in the Participant Portal.

To invite a user from one of your Organisation accounts to participate in a different Organisation:

1. Log in to the Participant Portal at https://portal.cdr.gov.au . Notice the page will show the organisation you are a member of and your allocated role.
2. To invite a user from a different Organisation account, select the **Swap organisation** button to display the **Select an organisation** screen.
3. Select the other legal entity - in this example, the **Organisation A**.
4. To invite the user to the other legal entity, follow the same steps as mentioned in 4.1 inviting Participants.

Only a primary business contact can invite a user from one organisation account to also be a user for a different organisation account via Swap Organisation menu item.



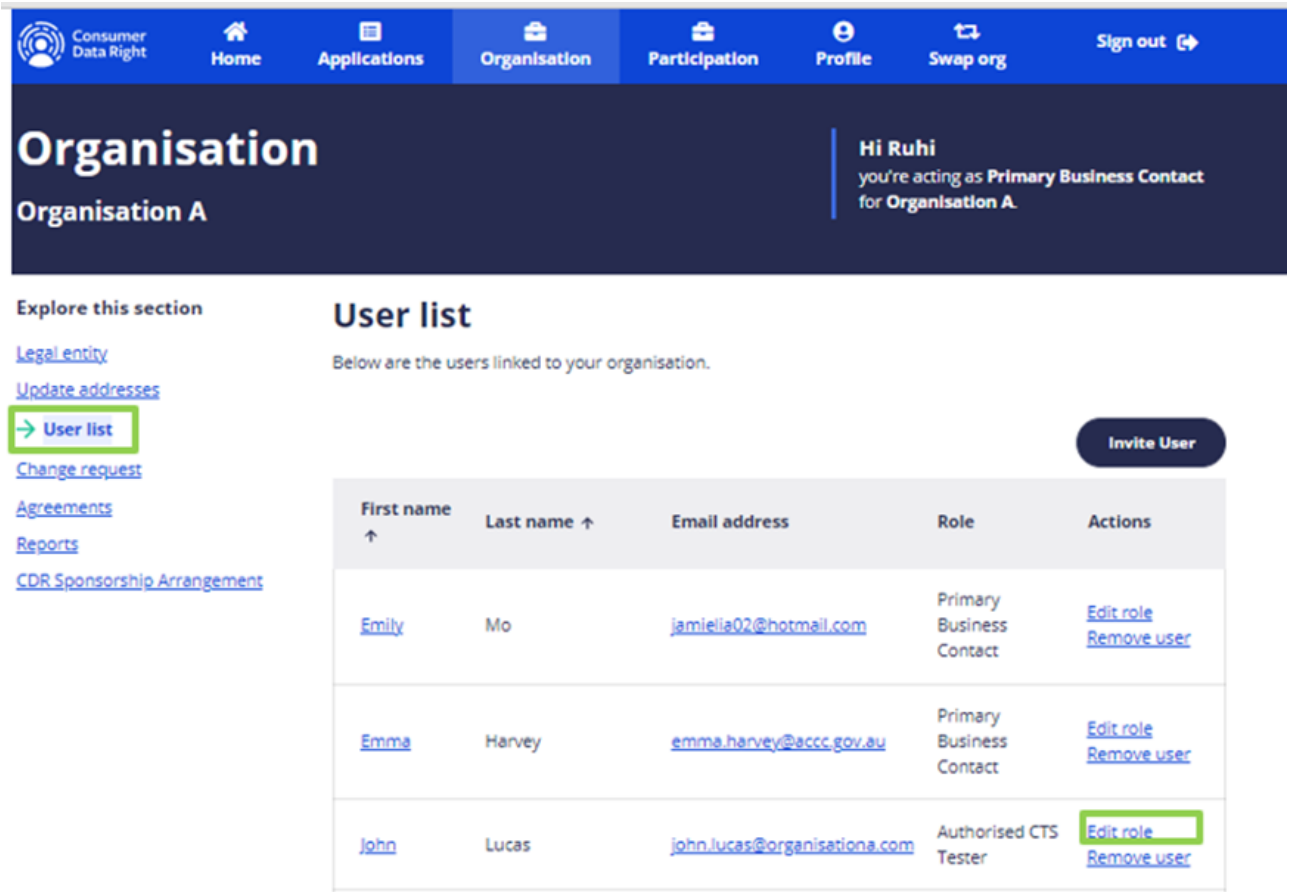


> **Note:** When the primary business contact in this example logs in again – they will see the legal entity and role that they last logged in with. In this example, user is now the primary business contact of Organisation A legal entity.

5.3 Modifying a user's access

Only a primary business contact can modify a user's access or role within the Participant Portal. However, there can be multiple primary business contacts on an organisation's portal account.

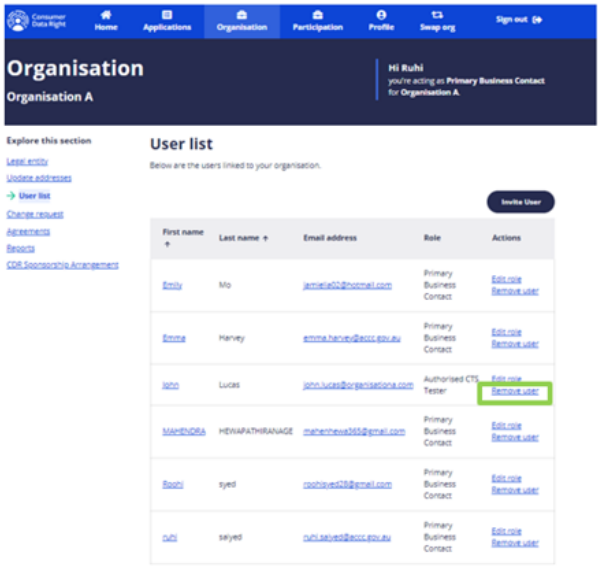
1. Log in to the Participant Portal at https://portal.cdr.gov.au and select **Organisation** from the top navigation menu.
2. Select **User list** from the left side navigation menu. You will be shown a table listing all current users (first name, last name, email address and role of the person) within your organisation.
3. Select the **Edit role** option for the user you want to modify.
4. Choose the access type you want to assign to the user. A user's role can be modified at any time by an authorised user (i.e. by a primary business contact).

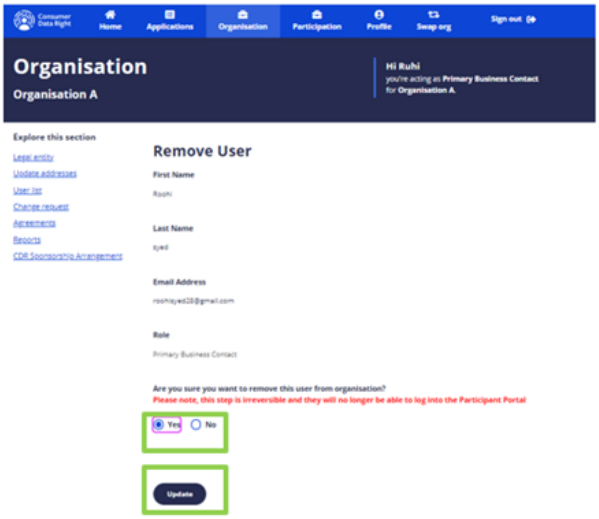


5.4 Removing a user's access

Only a primary business contact can remove a user from the Participant Portal. Removing a user is performed from the **User list** – see example below.

When a primary business contact removes a user, a note is shown advising that this step is irreversible, and the selected user will no longer be able to log into the Participant Portal. If the user previously had roles in multiple legal entities (refer to section 4.2 Users across multiple legal entities), they will no longer have access to the legal entity that the remove action is performed on.


Consumer Data Right
Home
Applications
Organisation
Participation
Profile
Swap org
Sign out
Organisation
Organisation A
Hi Ruhi
you're acting as Primary Business Contact for Organisation A.
Explore this section
Legal entity
Update addresses
User list
Change request
Agreements
Reports
CDR Sponsorship Arrangement
User list
Below are the users linked to your organisation.
Invite User
First name
Last name
Email address
Role
Actions
Emily
Mo
jamielia02@hotmail.com
Primary Business Contact
Edit role
Remove user
Emma
Harvey
emma.harvey@accc.gov.au
Primary Business Contact
Edit role
Remove user
John
Lucas
john.lucas@organisationa.com
Authorised CTS Tester
Edit role
Remove user
MAHENDRA
HEWAPATHIRANAGE
mehenhewa365@gmail.com
Primary Business Contact
Edit role
Remove user
Roohi
syed
roohisyed28@gmail.com
Primary Business Contact
Edit role
Remove user
ruhi
saiyed
ruhi.saiyed@accc.gov.au
Primary Business Contact
Edit role
Remove user


Consumer Data Right
Home
Applications
Organisation
Participation
Profile
Swap org
Sign out
Organisation
Organisation A
Hi Ruhi
you're acting as Primary Business Contact for Organisation A.
Explore this section
Legal entity
Update addresses
User list
Change request
Agreements
Reports
CDR Sponsorship Arrangement
Remove User
First Name
Roohi
Last Name
syed
Email Address
roohisyed28@gmail.com
Role
Primary Business Contact
Are you sure you want to remove this user from organisation?
Please note, this step is irreversible and they will no longer be able to log into the Participant Portal
Yes
No
Update

6 Data holders

The Participant Portal allows prospective businesses to register as a data holder and manage their organisation's information.

Data holders can:

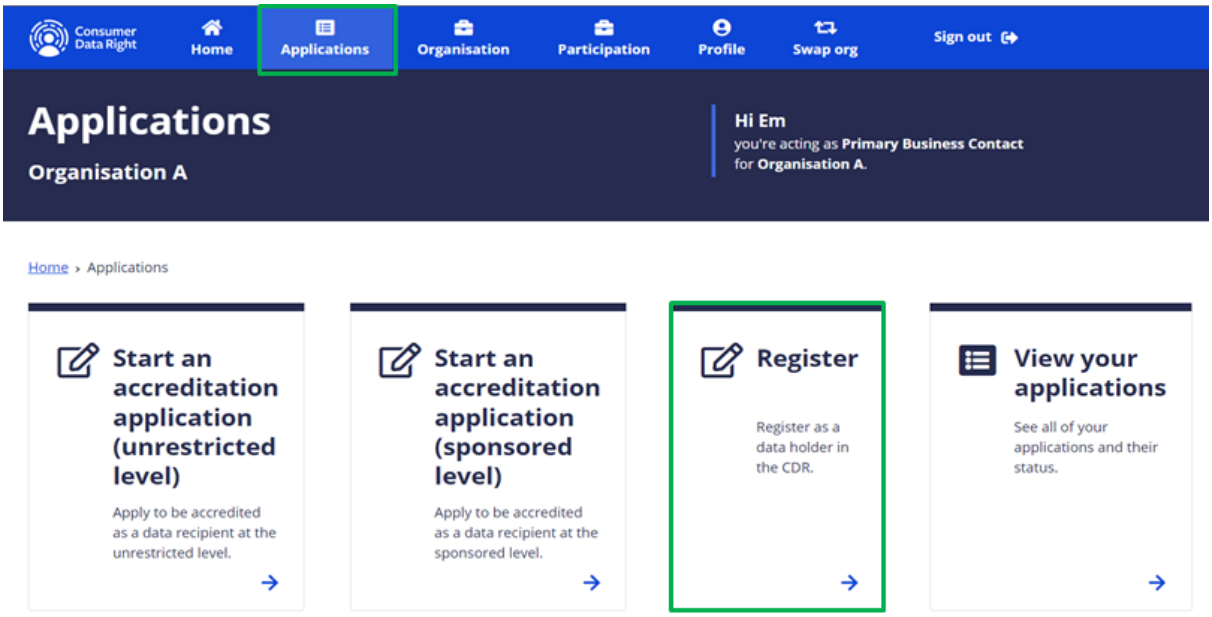
- register as a data holder in the appropriate CDR sector/s
- create, update and remove brands
- have their organisation's primary business contact invite other users with other roles within their organisation to manage their participation in CDR
- request certificates and update their brand details, endpoints and authentication details, and submit their endpoints and authentication details for review.

6.1 Complete data holder registration

Registration as a data holder on the Participant Portal will only be accepted if an applicant is a data holder under section 56AJ of the *Competition and Consumer Act 2010,* including accredited persons to whom reciprocal data holder obligations apply.

A primary business contact or authorised business contact can initiate data holder registration on the CDR Participant Portal by following the steps below:

1. Log into the Participant Portal at https://portal.cdr.gov.au and select the **Applications** button.
2. Click the **Register** button to open the data holder registration application form.



3. Select an appropriate CDR sector.
4. Complete the declaration and click the **Register** button to submit the form.
5. Once submitted, you will be shown a message confirming your registration.
6. Following registration, data holders must complete on-boarding activities before becoming active in the CDR ecosystem. You will receive an email detailing these activities. Further

information about on-boarding can be found in the https://www.cdr.gov.au/for-providers/on-boarding-for-data-holders .

6.2 Reciprocal data holder obligations

If you are an accredited data recipient and are seeking to register as a data holder, when you click the **Register** button, you will need to check the **check box** confirming that your organisation is registering as a data holder in the banking sector based on reciprocity obligations under the CDR Rules.

Once registered as a data holder, you will receive a message confirming your submission and advice that the CDR Team will follow up to discuss details of your application or to request additional information.

7 Data recipients

7.1 Accreditation levels

There are currently two accreditation levels: Unrestricted and Sponsored.

7.1.1 Unrestricted

An unrestricted accreditation allows a data recipient to obtain consent from consumers and collect data from Data Holders without any restrictions for all designated sectors.

There are two types of unrestricted accreditation applications:

1. Full unrestricted accreditation application
    a. All applicants who are not ADIs will be required to complete the full unrestricted accreditation application.
    b. A sample full unrestricted application form can be viewed on the Consumer Data Right website under sample application forms.
2. Streamlined application
    a. Existing Data Holders who are ADIs meet the criteria for streamlined accreditation and may instead complete the streamlined accreditation form. This application requires reduced information than full unrestricted accreditation application.
    b. A sample streamlined application form can be viewed on the Consumer Data Right website under sample application forms.

7.1.2 Sponsored

An applicant intending to participate in CDR via a sponsorship arrangement with an unrestricted accredited data recipient (ADR) will be required to complete the sponsored accreditation application.

A sample sponsored accreditation application form can be viewed on the Consumer Data Right website under sample application forms.

7.2 Accreditation application

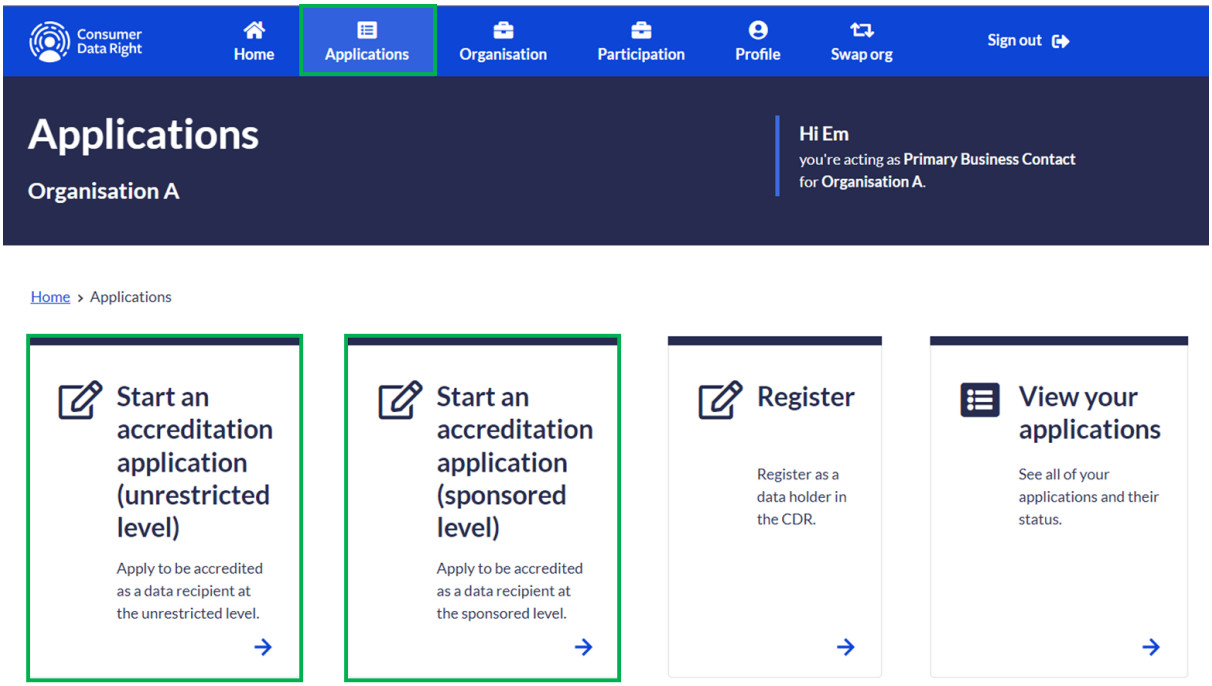
7.2.1 Start an accreditation application

We recommend you read the following guidance before commencing your application to better assist you with understanding the requirements of accreditation.

1. Accreditation Guidelines
2. Supplementary Accreditation Guidelines: Insurance
3. Supplementary Accreditation Guidelines: Information Security
4. Accreditation Controls Guidance

Only a Primary Business Contact can start and submit an accreditation application. To do this, the Primary Business Contact will need to:

1. Log in to the Participant Portal at https://portal.cdr.gov.au. Select **Applications** from the top navigation menu.
2. Select the relevant **Start an accreditation application** tile based on the accreditation level you wish to apply for.



3. Follow the prompts to complete the application.

Once an application has been started, other users with certain roles can view and update the draft accreditation application. For more information on user roles and permissions, please refer to the User roles and permissions in this guide.

For all application types, you will need to:

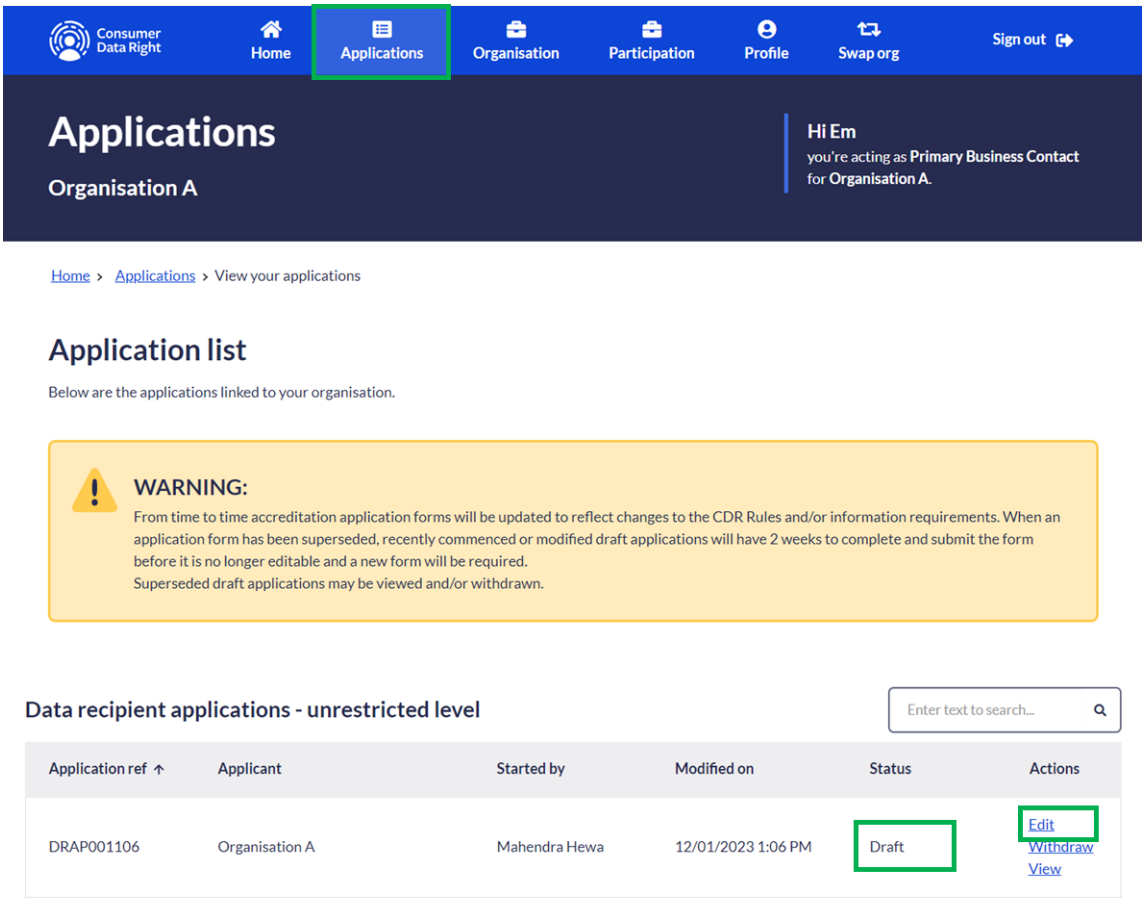
1. Confirm and agree with the way your personal information, provided in your application, will be used and handled.
2. Give general background information about your legal entity.
3. Provide details about all the products/services you will be offering to consumers if accredited.
4. Provide, under the information security section:
   a. a self-assessment and attestation form if you are a sponsored accreditation applicant
   b. an assurance report if you are a full unrestricted accreditation applicant
5. Complete the remainder of the form.

7.2.2 Edit your application

An accreditation application with a status of 'draft' can be edited. An application cannot be edited once submitted.

To edit an application with a draft status:

1. Log in to the Participant Portal at https://portal.cdr.gov.au. Select **Applications** from the top navigation menu followed by the **View your applications** tile.
2. Find the relevant application and under the **Actions** column select **Edit** for the application you want to edit.
3. Select **Save and continue** button during navigation of each of the sections that are edited.



7.2.3 Finalise and submit your application

Depending on the application type and your responses to questions on the application form, you will be shown a tailored list of documents that you need to upload before submitting your application.

Upon submission, you will be shown a success screen confirming your application has been submitted.

You will also receive an email with your application number.

To check the status of your application at any time, log in to the Participant Portal at https://portal.cdr.gov.au and select **Applications** from the top navigation menu then **View your applications**.

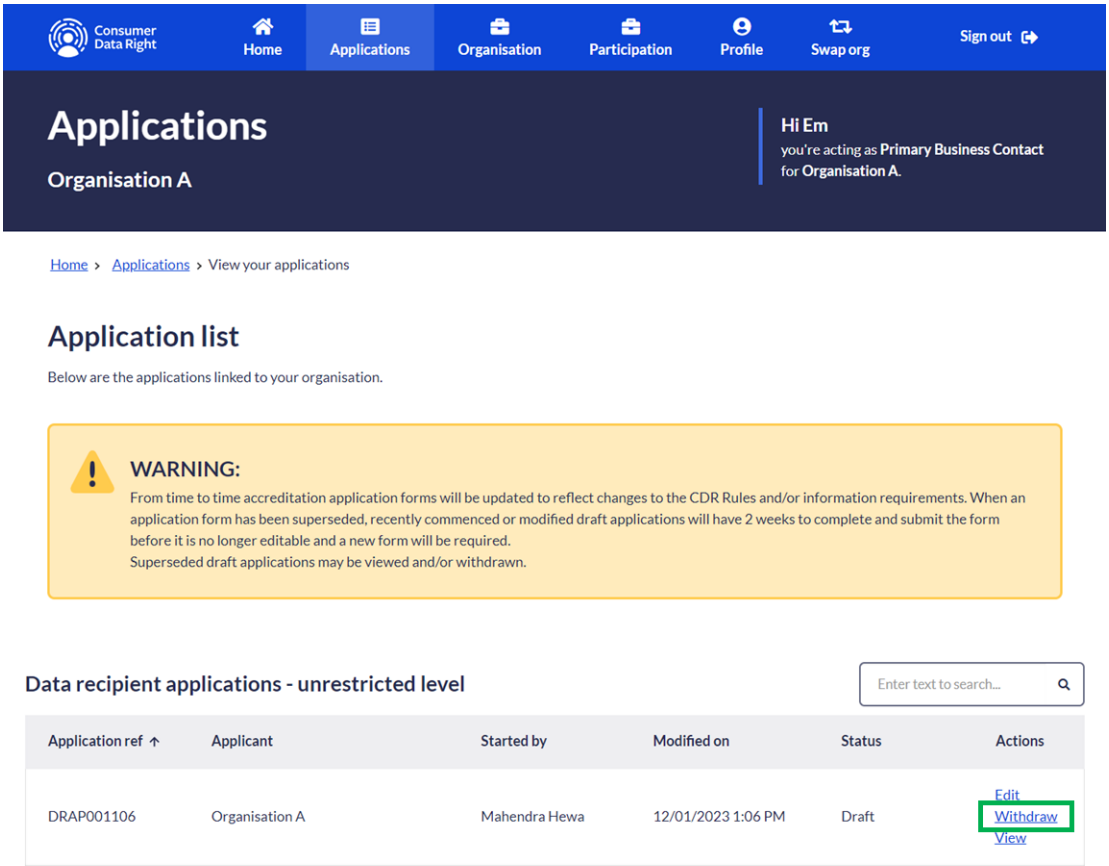
If you have any questions about your application, please contact us via the CDR Technical Operations mailbox CDRtechnicaloperations@accc.gov.au.

7.2.4 Withdraw a draft application

If you no longer wish to continue with your accreditation application, and the application has a status of 'draft', it can be withdrawn by a Primary Business Contact.

To withdraw a draft application:

1. Log in to the Participant Portal at https://portal.cdr.gov.au and select **Applications** from the top navigation menu followed by the **View your applications** tile.
2. Find the relevant application and under the **Actions** column select **Withdraw**.



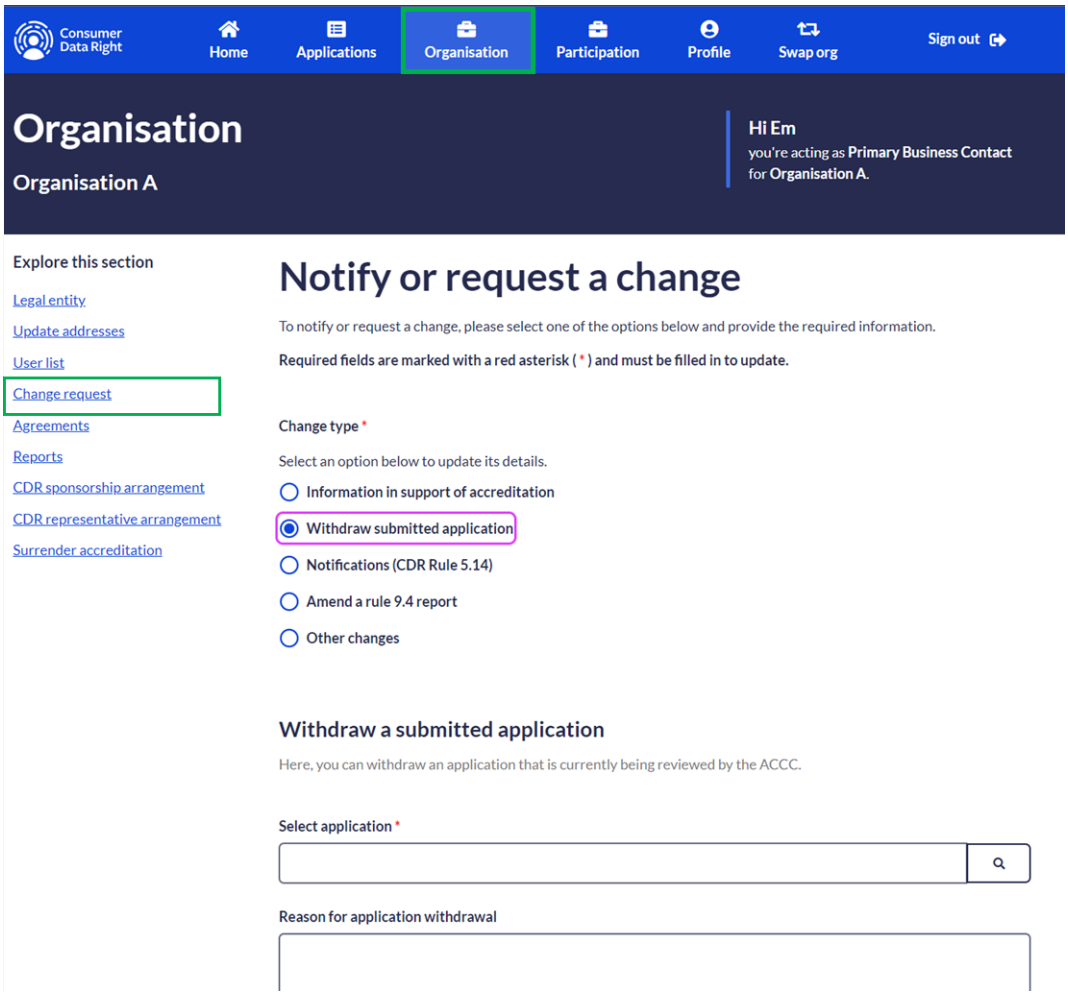
7.2.5 Withdraw a submitted application

A Primary Business Contact can withdraw a submitted accreditation application by submitting a change request.

To withdraw a submitted application:

1. Log in to the Participant Portal at https://portal.cdr.gov.au and select **Organisation** from the top navigation menu.
2. Select **Change request** from the left-hand navigation menu and select **Notify or request a change**.

3. Under **Change type** select **Withdraw submitted application**.
4. Select the application that you would like to withdraw and select **Submit request**.



7.2.6 Incomplete applications

An application will be returned to you as a draft if it is considered to be incomplete. You will be advised which areas of the application are incomplete and afforded an opportunity to provide the missing information and resubmit your application.

Applications that have been returned to draft status are displayed in the **Application list** section of the Participant Portal which can be edited to provide requested missing information.

The Primary Business Contact who submitted the application will also receive an email notification advising the application is incomplete and has been returned as a draft.

7.3 Other change requests

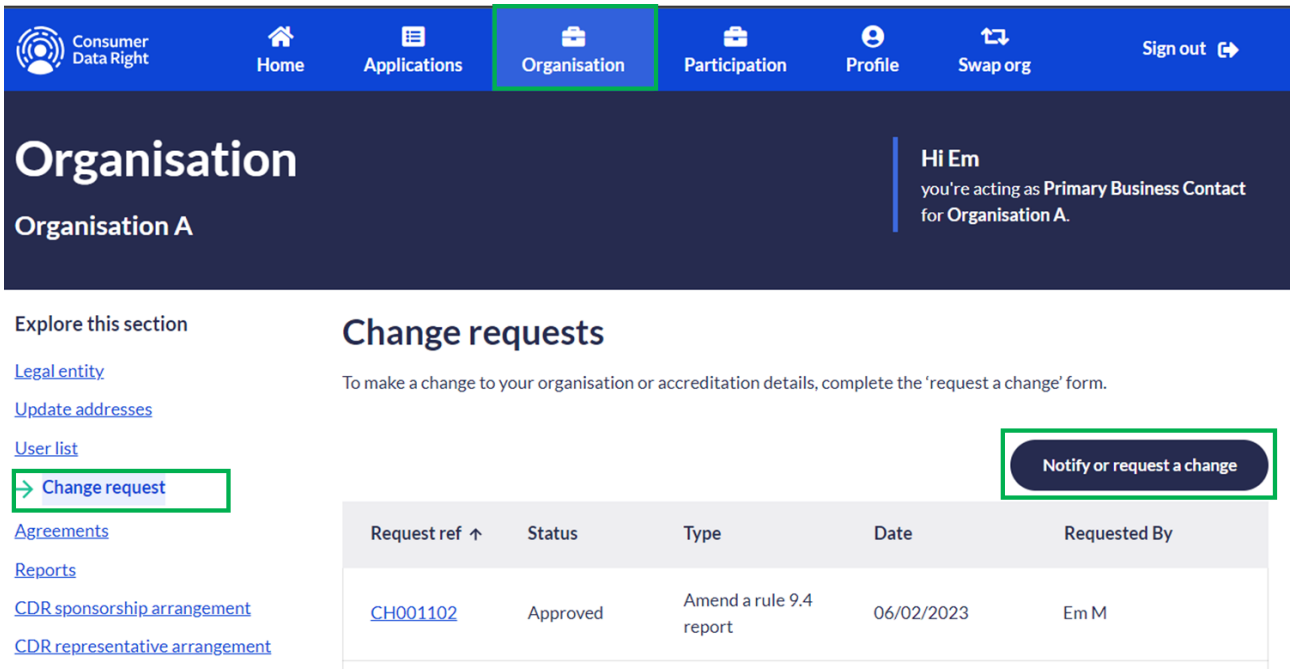
Once an application has been submitted, a Primary Business Contact can view the submitted accreditation application and provide further information in support of the application, request

to withdraw a submitted application, and notify or request other changes by raising a change request from the Participant Portal. Any additional information submitted in relation to an application for accreditation will be considered by the Data Recipient Accreditor alongside the original information contained in the application.

Once accredited, this capability can also be used by the accredited data recipients to notify the Data Recipient Accreditor of any notification requirements required under rule 5.14 of the CDR Rules.

To access change requests:

1. Log in to the Participant Portal at https://portal.cdr.gov.au and select **Organisation** from the top navigation menu.
2. Select **Change request** from the left side navigation menu.
3. Click on the **Notify or Request a change** button.
4. Select the relevant change type:
    a. information in support of accreditation
    b. withdraw submitted application
    c. notifications (CDR Rule 5.14)
    d. amend a rule 9.4 report
    e. other changes.
5. Complete supporting information and upload documents if required.
6. Click on the **Submit request** button.

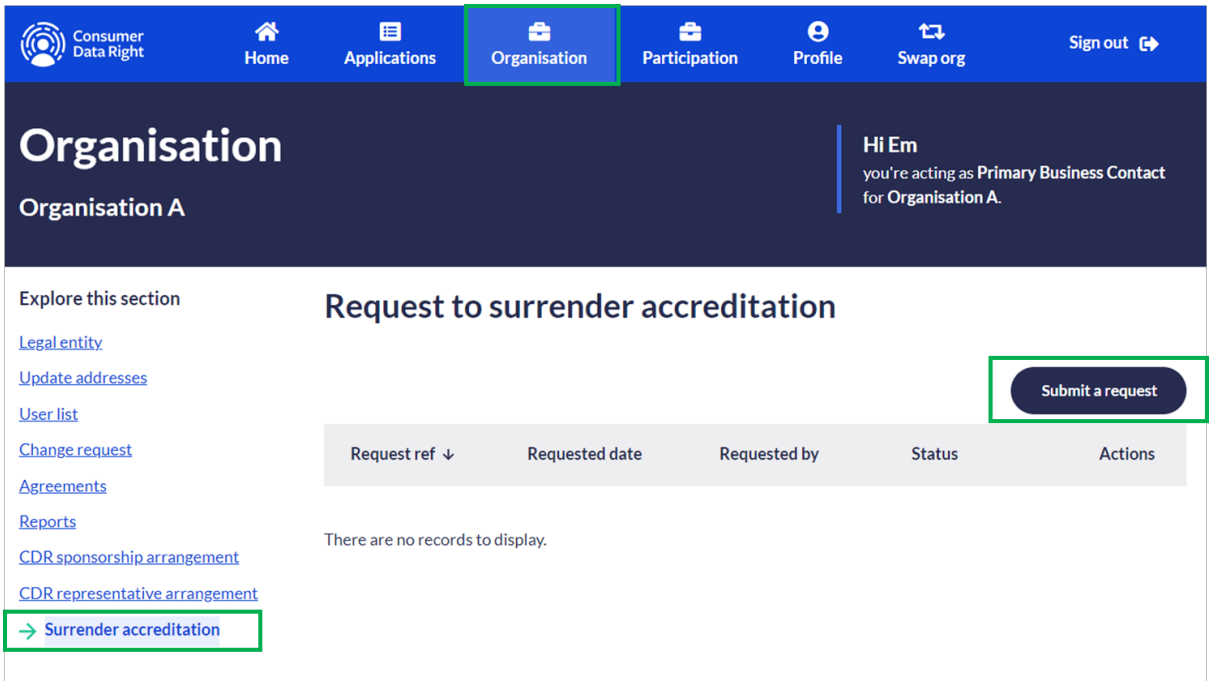


7.4 Surrender accreditation

7.4.1 Submit a request to surrender accreditation

A Primary Business Contact can submit a request to surrender accreditation from the Participant Portal. Please note that surrendering accreditation is a significant action. Once a request to surrender accreditation has been accepted by the Data Recipient Accreditor, it cannot be reversed.

1. Log in to the Participant Portal at https://portal.cdr.gov.au and select **Organisation** from the top navigation menu.
2. Select **Surrender accreditation** from the left side navigation menu, and then select **Submit a request** button to open up the form.

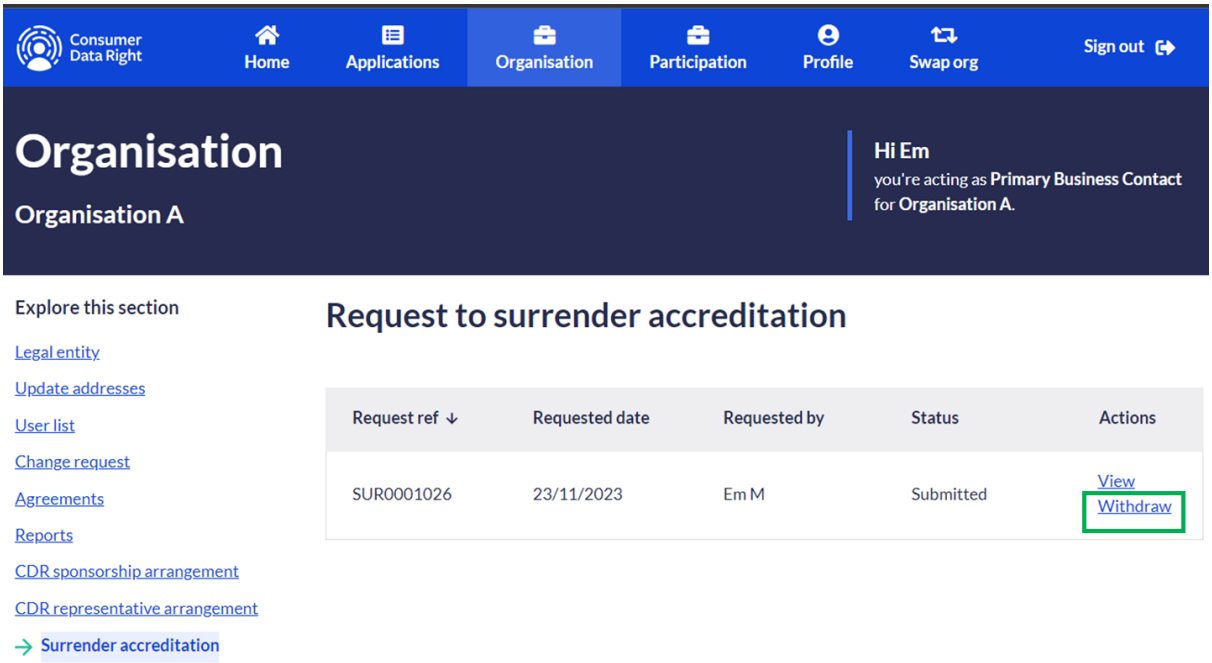


3. Complete all mandatory fields and select the **Submit request** button to submit the form.
4. Upon submission, a confirmation will be displayed.

7.4.2 Withdraw your request to surrender accreditation

Before the surrender request is processed and accepted by the Data Recipient Accreditor, you can withdraw the request from the Participant Portal.

1. From the **Surrender accreditation** landing page, select the **Withdraw** action to open the form.



2. Provide reason for withdrawal and submit the form.
3. Upon submission, a confirmation will be displayed.

8 Post accreditation or registration

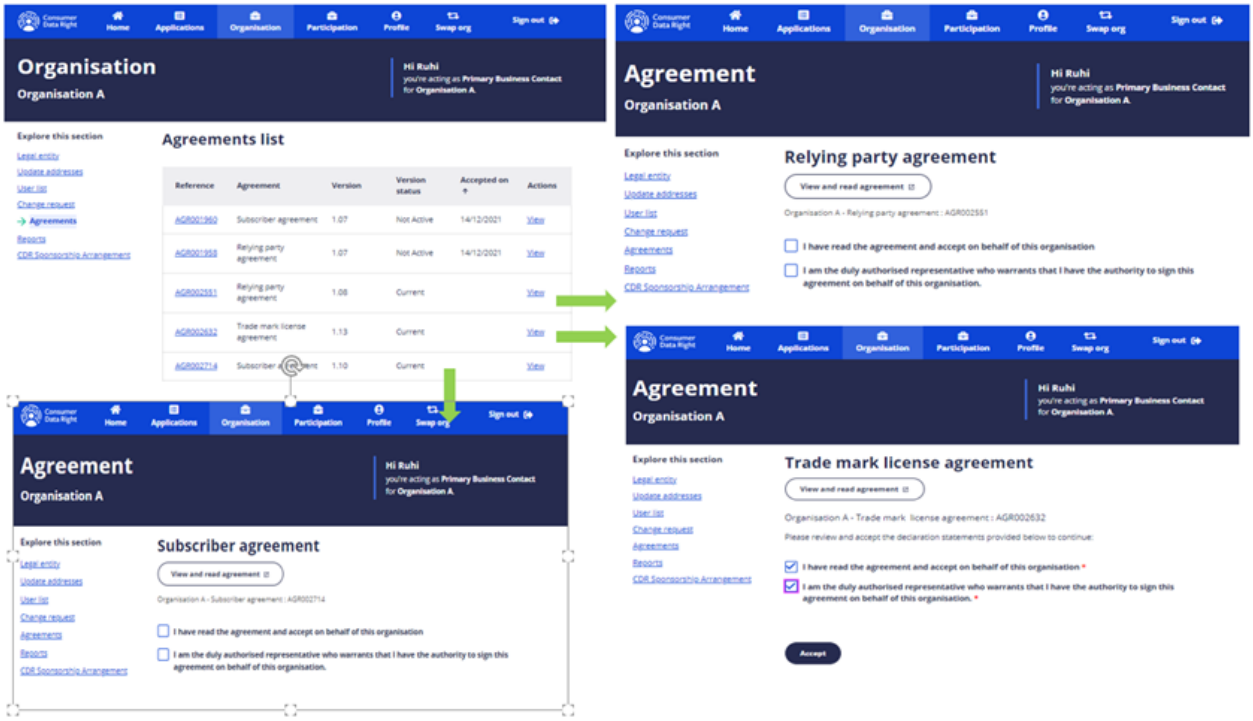
Following accreditation or registration, participants must be on-boarded before they become active participants in the CDR ecosystem. As part of the on-boarding process, participants must accept the following agreements:

- Subscriber Agreement
- Relying Party Agreement

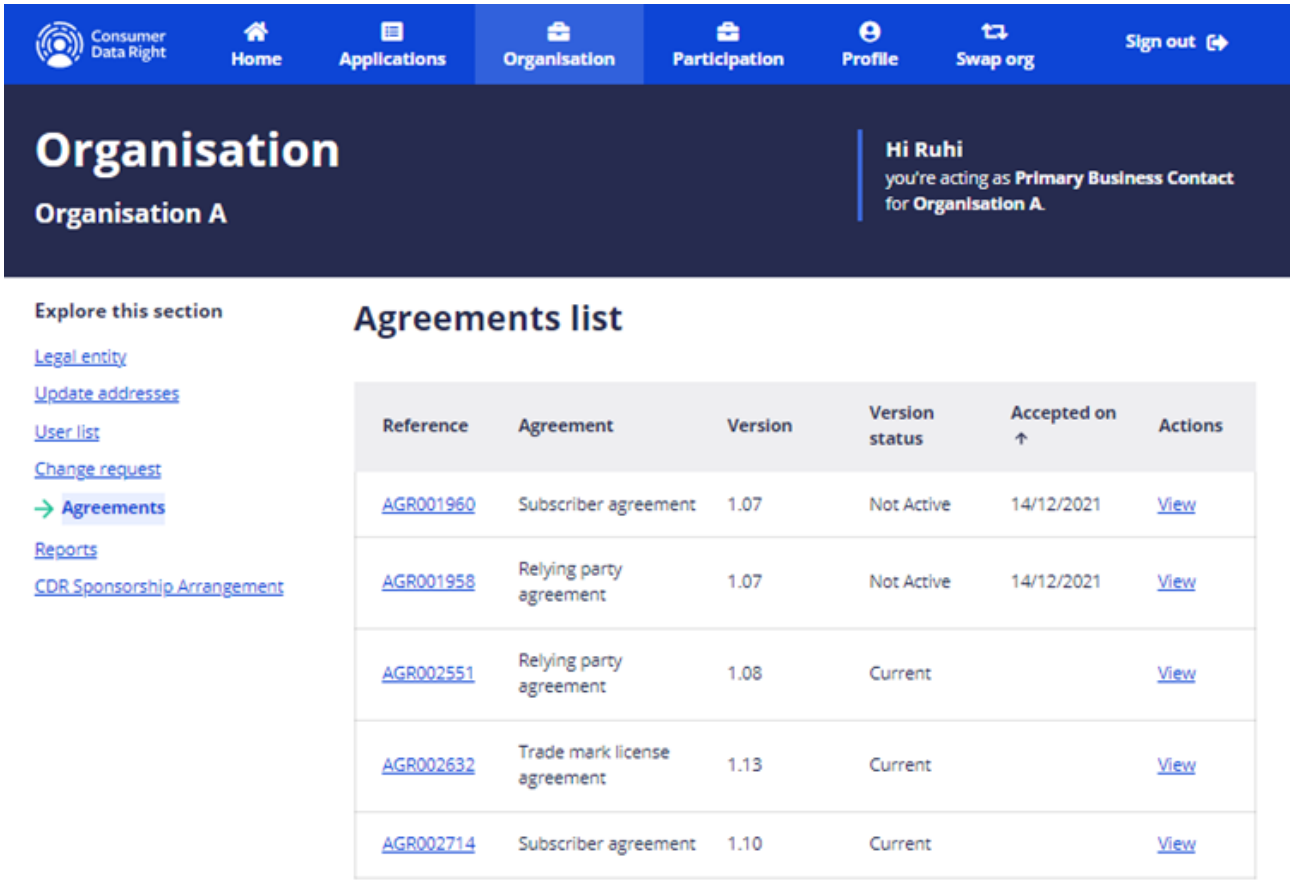
The following agreement is required in order to use the CDR Trademark:

- CDR Trademark Licence Agreement

The Trademark Licence agreement is mandatory to be signed if the participant is a Data Recipient or both Data holder and Data Recipient.



Participants can view both signed and latest version of the agreements in the participant portal at all times. Select Organisation in the primary navigation> click Agreement in the left navigation panel



Acceptance of the Subscriber Agreement and the Relying Party Agreement is required once only, and not subsequently when a new agreement is published.

A sponsored Accredited data recipient will only receive and accept the CDR Trademark Licence Agreement.

If an agreement requires action, a notification will be displayed when the participant signs in. All users within the organisation will be able to see that action is required.

All users can view the agreements, but only the legal authority contact can accept or action the agreements within the Participant Portal.

For more information on user roles and permissions, please refer to User roles and permissions in this guide.

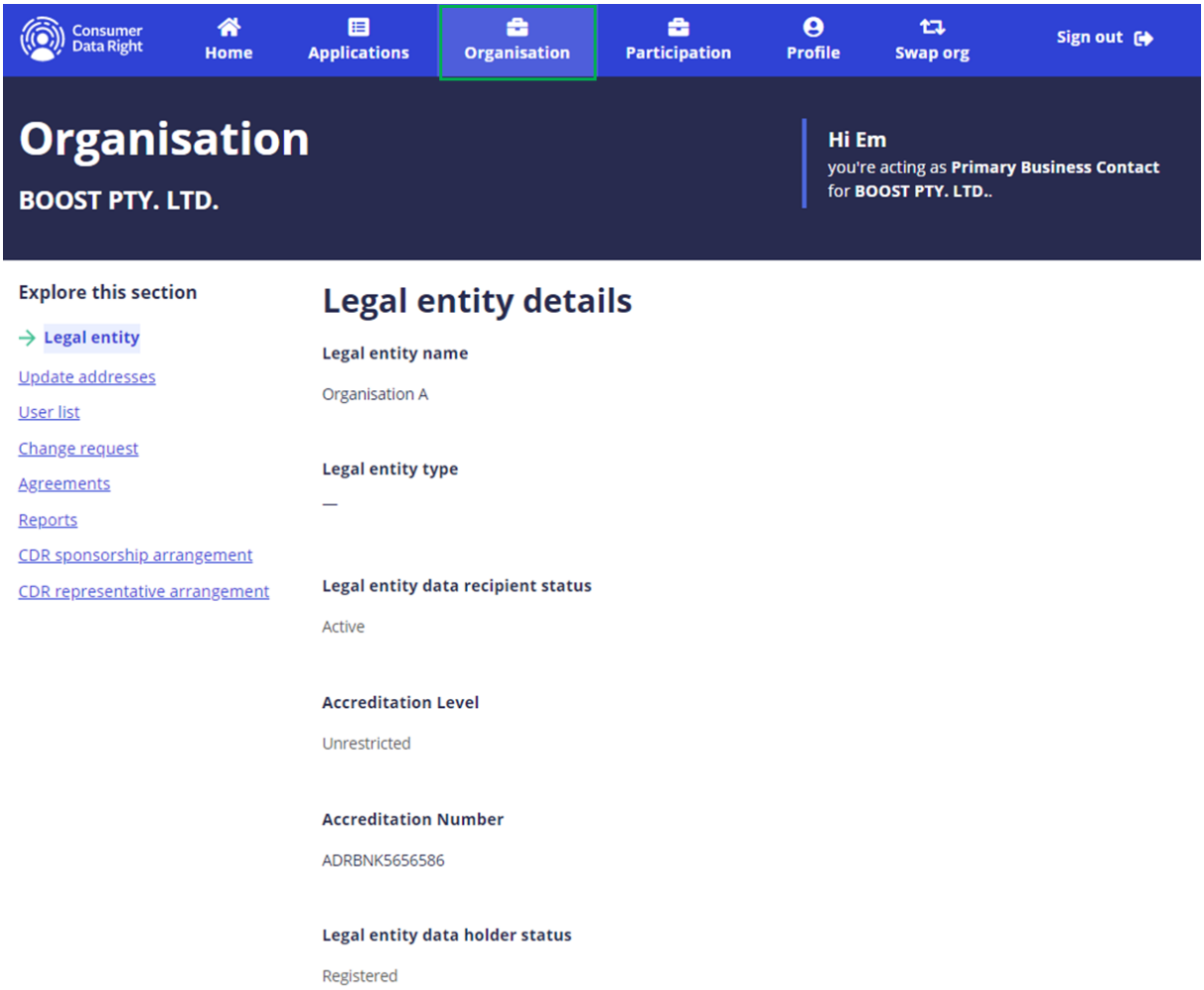
9 Manage organisation details

Details such as your organisation details, reports, agreements and CDR arrangements can be viewed and maintained by selecting **Organisation** from the primary navigation.

9.1 Maintain organisation details

Only a primary business contact has the ability to update all of your legal entity's organisation details. An authorised business contact, primary IT contact and authorised IT contact can view organisation details and update selected entries. Once updated, the participant's information on the CDR Register will be updated with the new information.

1. Log in to the Participant Portal at https://portal.cdr.gov.au and select **Organisation.**



2. The landing page displays the Organisation details in which you can update your legal entity details:
   a. logo URI
   b. website URL
   c. CDR policy URL

These details can be updated by a user who has been assigned a primary business contact or an authorised business contact role.

1. If you need to update your address, select **Update addresses** in the left side navigation menu to update your registered business addresses, registered address for service or local agent address for service and select **Update** to save.

The registered business address can be updated by a user who has been assigned a primary business contact or authorised business contact role.

The addresses for service for a local agent can only be updated by a primary business contact.

> **Note:** More information regarding the definitions of the organisation's details can be found in the Consumer Data Right participant on-boarding guide.

9.2 CDR representative arrangement notification

The CDR representative arrangement model allows eligible participants to access and use CDR data without the need for accreditation in circumstances where they offer CDR-related services to consumers as a representative of an unrestricted accredited data recipient.

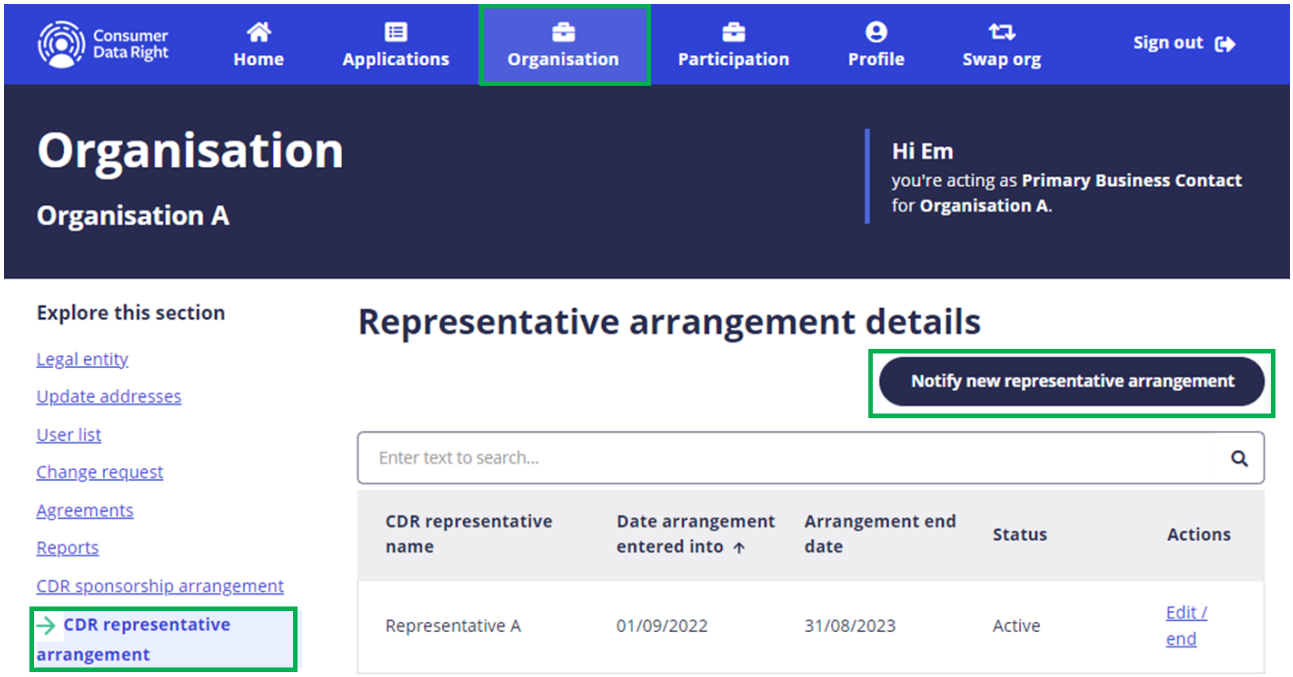
The principal (an unrestricted accredited data recipient) must notify the Data Recipient Accreditor as soon as practicable, and within 5 business days, of entering into a new CDR representative arrangement. Likewise, the principal must also notify the Data Recipient Accreditor if the arrangement terminates or otherwise ends as soon as practicable, but no later than 5 business days after the event. Once notified, the Data Recipient Accreditor will verify the arrangement and the Registrar will publish details of the arrangement on the CDR Register.

Only a primary business contact or a legal authority contact of an unrestricted accredited data recipient has the ability to notify a new CDR representative arrangement on the CDR Participant Portal and edit / end an existing arrangement.

9.2.1 Notify a new CDR representative arrangement

To notify a new CDR representative arrangement, follow the steps below:

1. Log in to the CDR Participant Portal at https://portal.cdr.gov.au and select **Organisation** from the top navigation menu.
2. Select **CDR representative arrangement** from the 'Explore this section' menu.
3. From the landing page, select the **Notify new representative arrangement** button to launch the notification form.
4. Complete all mandatory questions and submit the form.
5. Once submitted, the representative arrangement details will be displayed on the page.



9.2.2 Edit or end a representative arrangement

Certain details of a representative arrangement can be updated, this includes the end date of the arrangement.

To edit or end a representative arrangement, follow the steps below:

1. Log in to the CDR Participant Portal at https://portal.cdr.gov.au and select **Organisation** from the top navigation menu.
2. Select **CDR representative arrangement** from the 'Explore this section' menu.
3. From the landing page, find the relevant arrangement that needs to be updated and select **Edit / end** to launch the form.
4. Update the necessary information and submit the update.

> **Note:** Once an arrangement has expired, the edit functionality will no longer be available.

9.3 CDR sponsorship arrangement notification

A sponsorship arrangement is a written contract between an unrestricted accredited data recipient (the sponsor) and another person (the affiliate) and provides for the sponsor to disclose CDR data to its affiliate in response to a consumer data request.

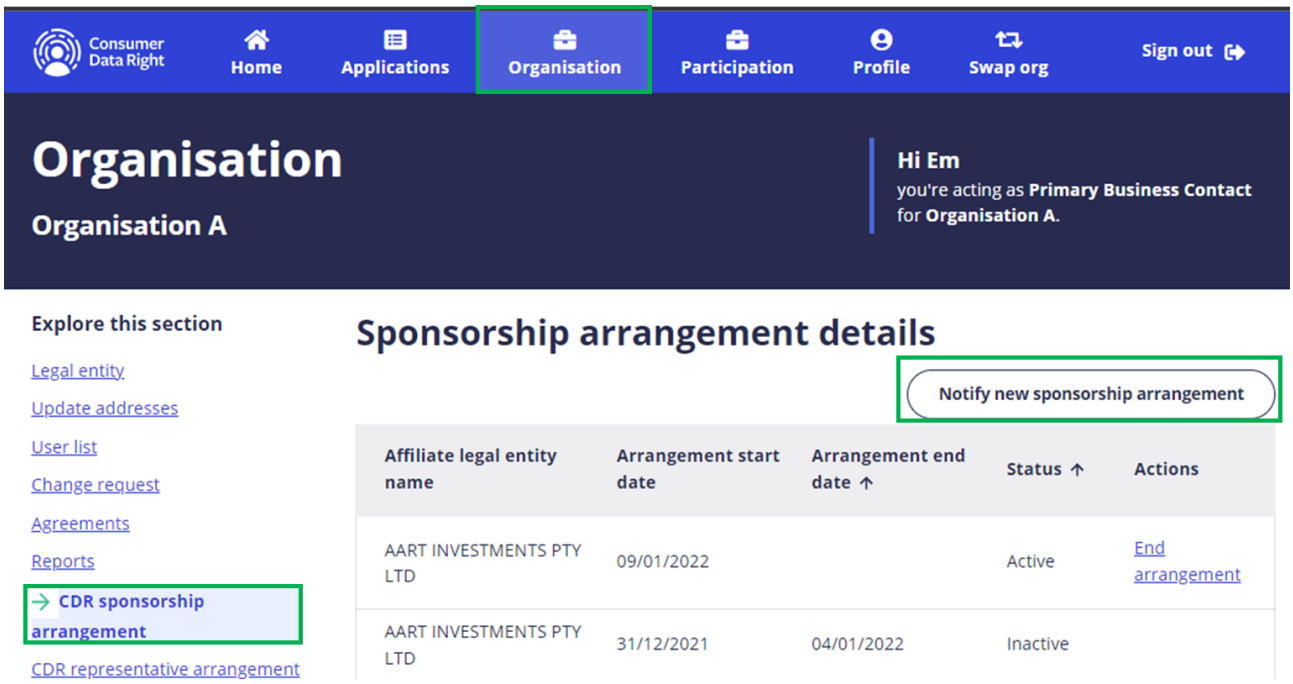
The sponsor must notify the Data Recipient Accreditor of becoming a sponsor of an affiliate, or the suspension, expiration or termination of a sponsorship arrangement, and must do so as soon as practicable, and in any event, within 5 business days.

Only a primary business contact or a legal authority contact of an unrestricted accredited data recipient has the ability to access the CDR sponsorship arrangement notification process on the CDR Participant Portal.

9.3.1 Notify a new sponsorship arrangement

To notify a new CDR sponsorship arrangement, follow the steps below:

1. Log in to the CDR Participant Portal at https://portal.cdr.gov.au and select **Organisation** from the top navigation menu.
2. Select **CDR sponsorship arrangement** from the 'Explore this section' menu.
3. From the landing page, select the **Notify new sponsorship arrangement** button to launch the notification form.
4. Complete all mandatory questions and submit the form.
5. Once submitted, the sponsorship arrangement details will be displayed on the page.



9.3.2 Notify the end date of a sponsorship arrangement

To notify the end date of a sponsorship arrangement, follow the steps below:

1. Log in to the CDR Participant Portal at https://portal.cdr.gov.au and select **Organisation** from the top navigation menu.
2. Select **CDR sponsorship arrangement** from the 'Explore this section' menu. You will be directed to the CDR sponsorship arrangement details page where you can notify the end date of an arrangement by selecting **End arrangement** from the 'Actions' column.

9.3.3 View sponsorship arrangements

If you are a sponsor, i.e. data recipient accredited at the unrestricted level:

- A list of associated sponsorship arrangements will be available under ‘Explore this section’ menu --> ‘CDR sponsorship arrangement’ with corresponding affiliate details

If you are an affiliate, i.e. data recipient accredited at the sponsored level:

- A list of associated sponsorship arrangements will be available under ‘Explore this section’ menu --> ‘CDR sponsorship arrangement’ with corresponding sponsor details

10 Manage participation details

> **Note:** The Participation section only displays when a legal entity has applied to be either a data holder or data recipient.

10.1 Maintain brand details

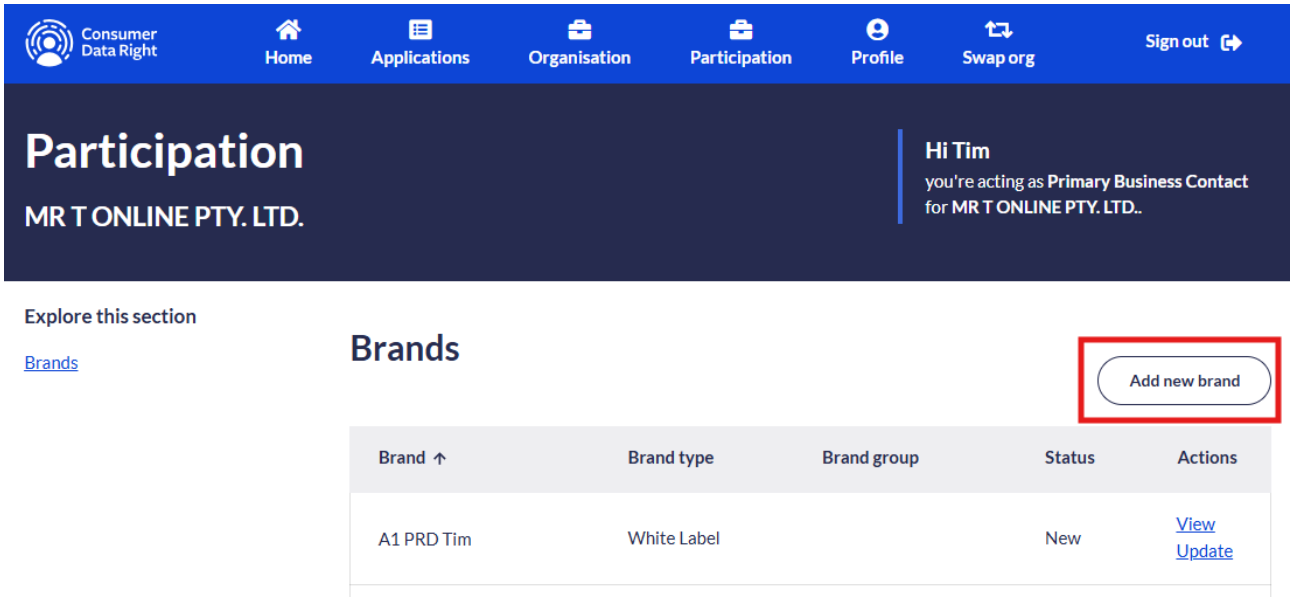
10.1.1 Add a new brand

A brand is a specific name that is used to collectively identify a set of products and services offered by a participant. This will be aligned to, and may or may not be the same as, a business name that is registered to the participant's organisation.

Participants would typically have one or more brands within the CDR. Brands can be added or removed.

Brand can be added following accreditation (for Data Recipients) or registration (for Data Holders). To add a brand, follow the steps below:

1. Log in to the Participant Portal at https://portal.cdr.gov.au and select **Participation** from the top navigation menu.
2. Select the **Add new brand** button and complete the form.
3. To add additional brands, select **Add new brand** and complete the form.



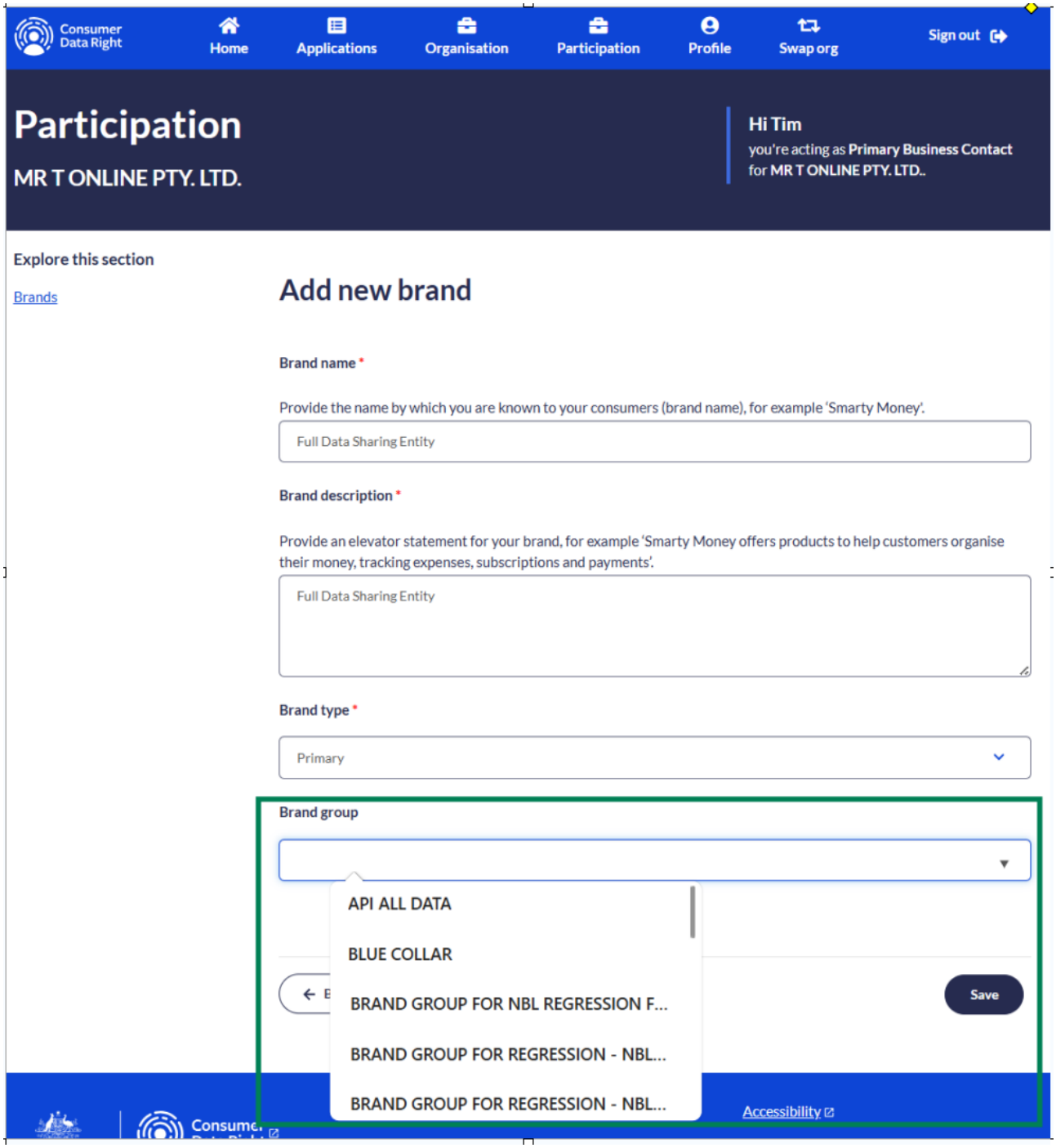
Brand groups

Brand group is an optional field designed to help manage complex "white label" or multi-brand arrangements, particularly in the banking and non-bank lending sectors.

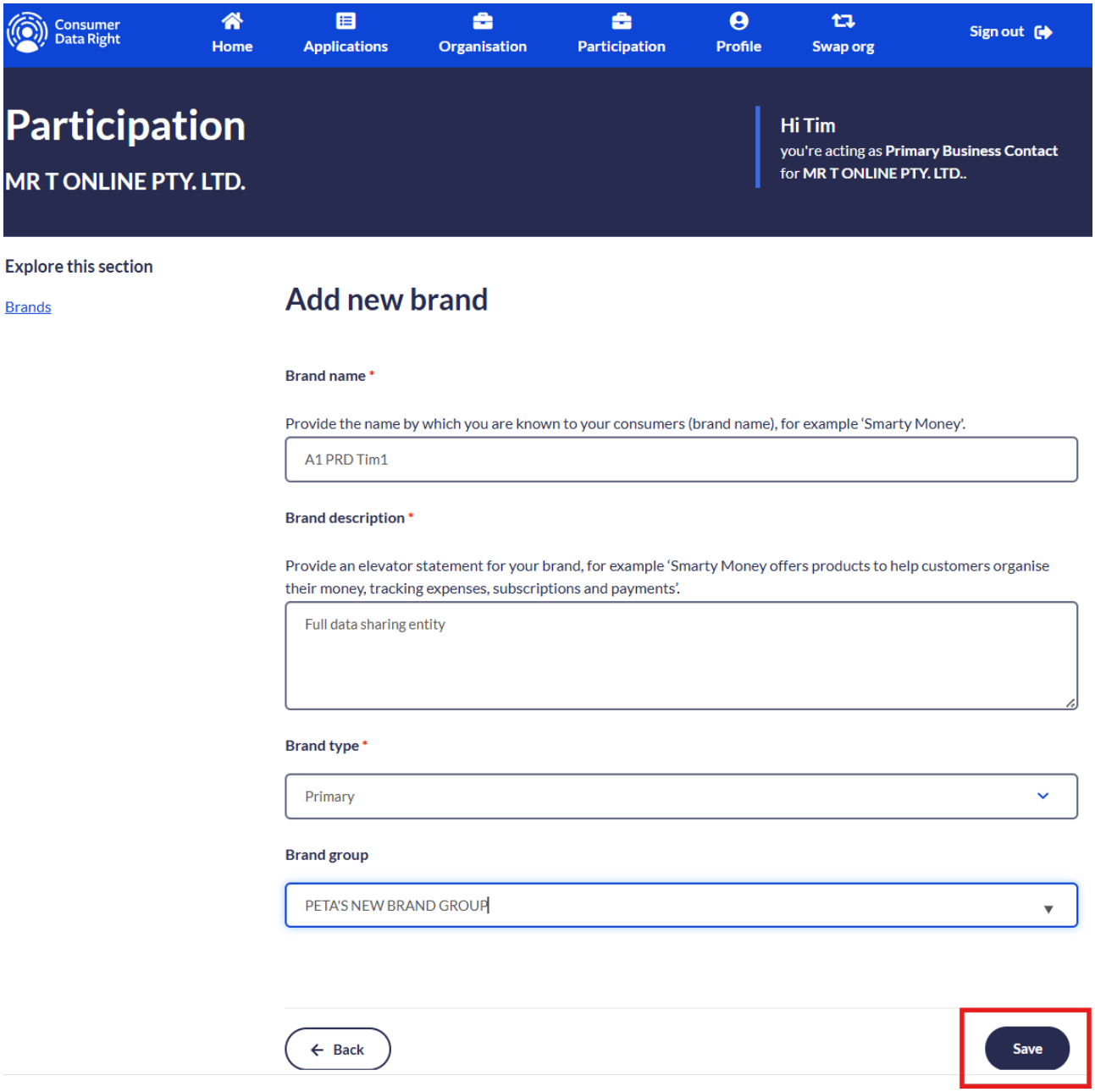
When adding a new brand, you can associate it with an existing brand group or create a new brand group for it.

If a brand group is used, all relevant data holder brands should use the same value to maintain consistency in the CDR Register.

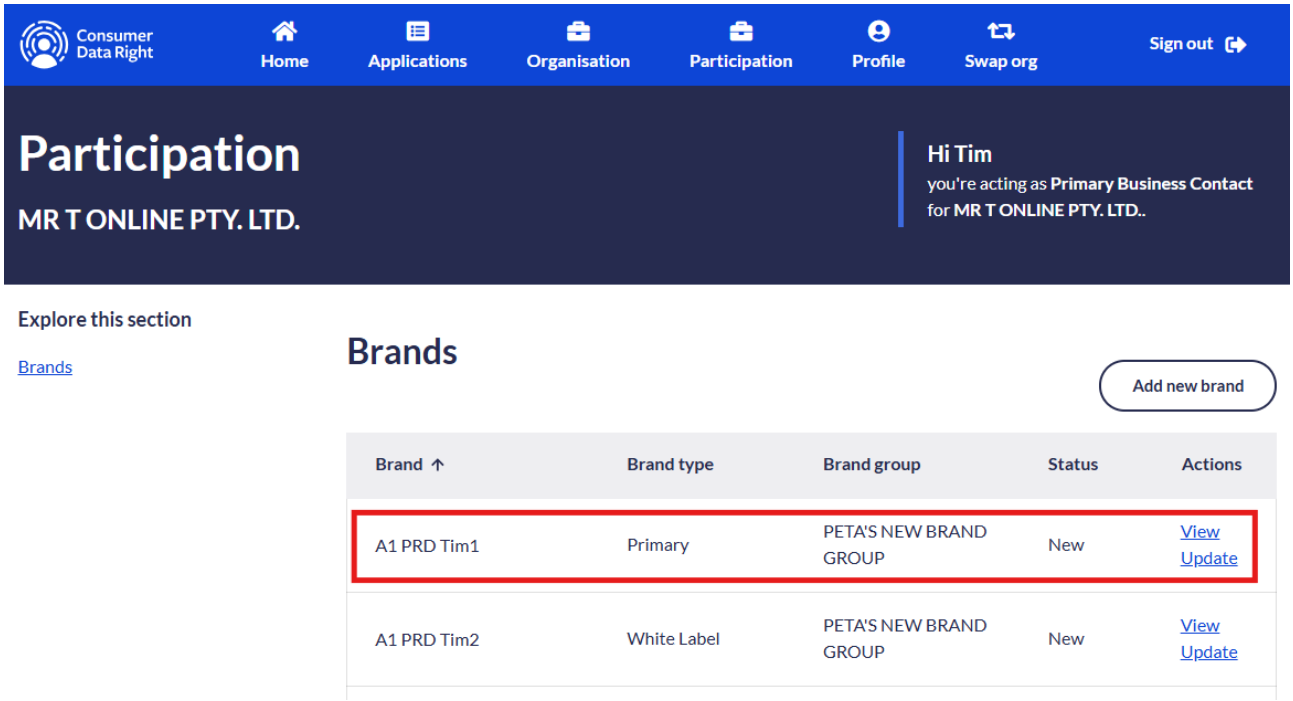
The brand group dropdown will show you existing brand groups. Start typing to alphabetically select from existing groups. If you create a new brand group, it will be added to the list of existing brand groups and can be selected from the dropdown in future updates. Please note that existing brand groups are visible in the dropdown to all participants.



4. Complete the form and select **Save**.



5. The system will create the new Brand.

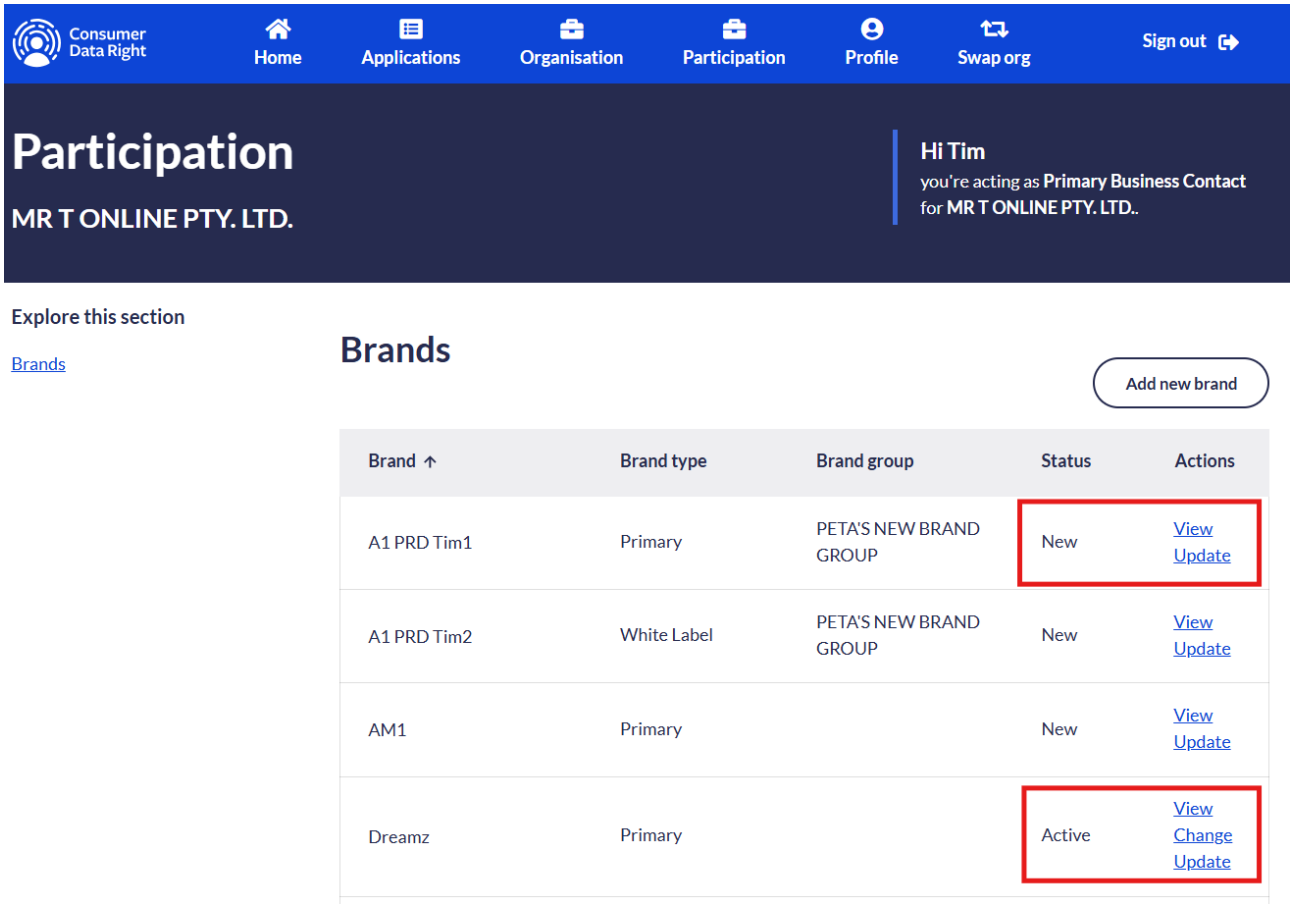


10.1.2 Modify an existing brand

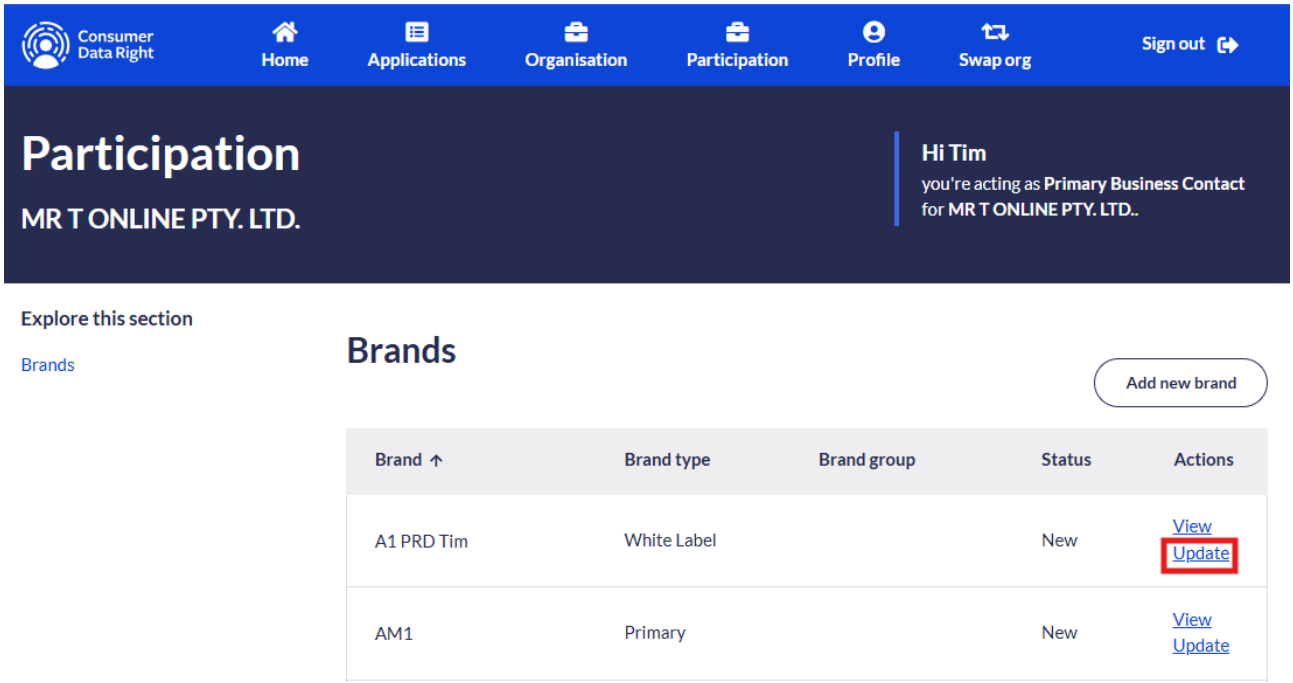
To edit existing brand details, please follow the steps below:

1. Log in to the Participant Portal at https://portal.cdr.gov.au and select **Participation** from the top navigation menu.

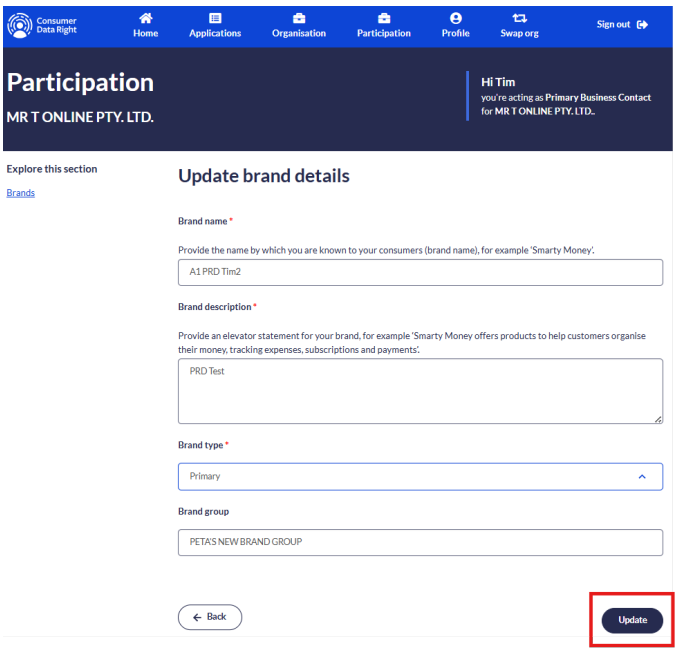
Different statuses offer different change options.



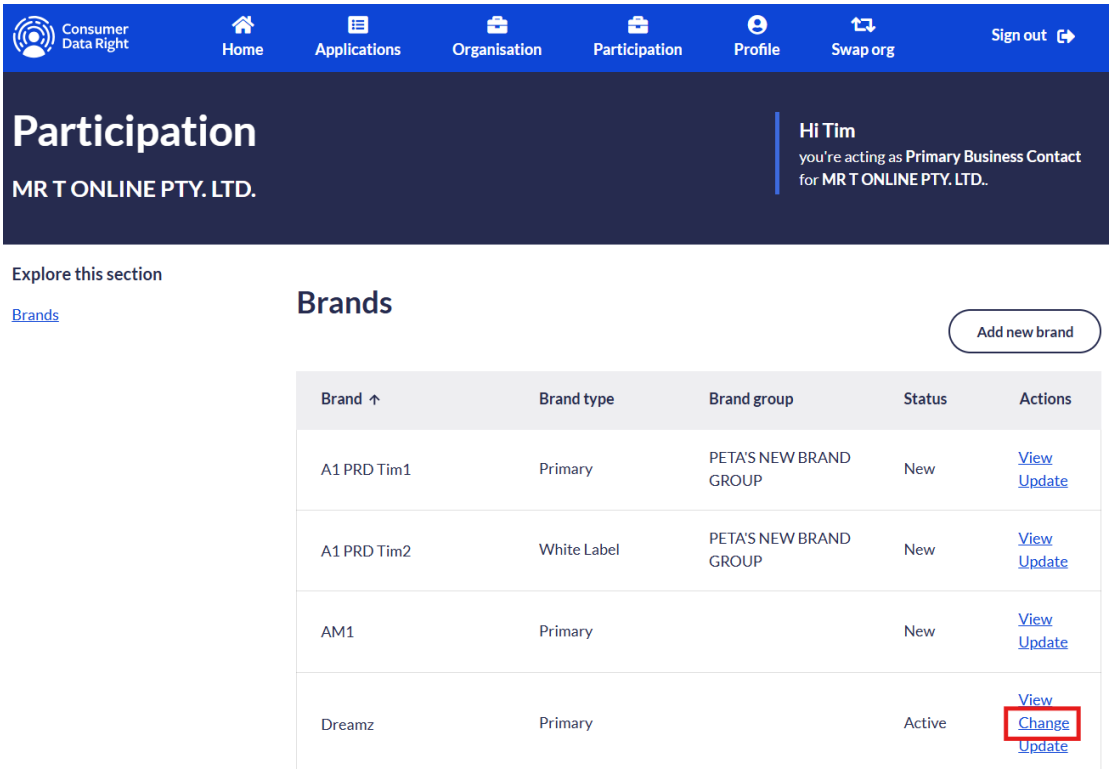
- If the Status is **New**, all details can be updated by clicking on the update link. Select **Update** against the brand that you wish to edit.



- Once updated details have been inputted, select **Update** button to finalise changes.



- If the Status is **Active**
  - to change the Brand name and/or Description you need to submit a Change Register request using the **Change** link.



- Once Brand name and/or Description details have been updated with reason for proposed change, select **Submit Request** button to submit the proposed change to ACCC for approval. You will be notified via email once the changes are applied.

Consumer Data Right | Home | Applications | Organisation | Participation | Profile | Swap org | Sign out

Participation

MR T ONLINE PTY. LTD.

Hi Tim
you're acting as Primary Business Contact for MR T ONLINE PTY. LTD..

Explore this section

Brands

Change brand name and description

Note: Changes to brand details

Changes to brand details are subject to an approval process, and as such will not be reflected immediately on the Public register. We endeavour to process these approvals as quickly as possible, you will be notified via email when your changes are applied.

Brand name *

Provide the name by which you are known to your consumers (brand name), for example 'Smarty Money'.

Dreamz

Brand description *

Provide an elevator statement for your brand, for example 'Smarty Money offers products to help customers organise their money, tracking expenses, subscriptions and payments'.

Test Brand 2

12 of 2000 characters

Reason for brand change *

Please provide a reason for changing brand details.

I want to

9 of 2000 characters

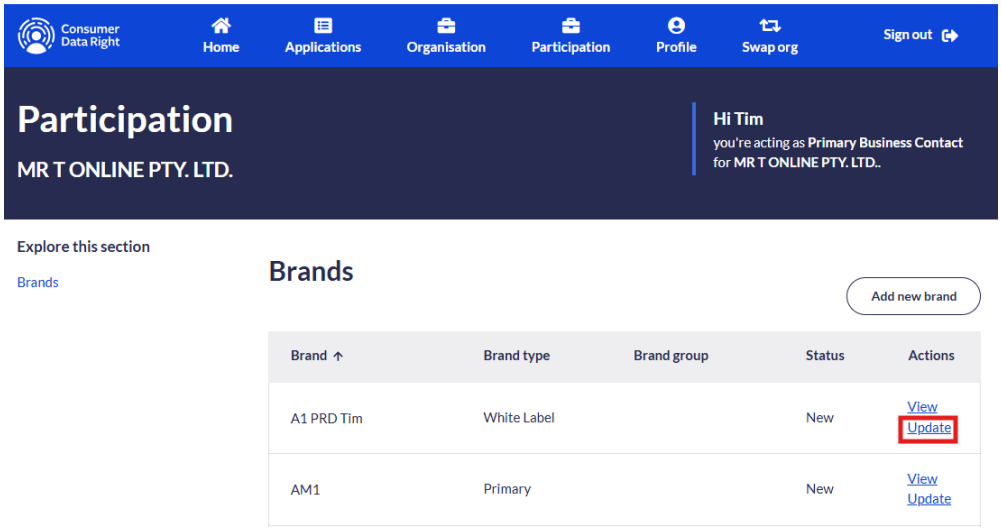
Proposed publication date (optional)

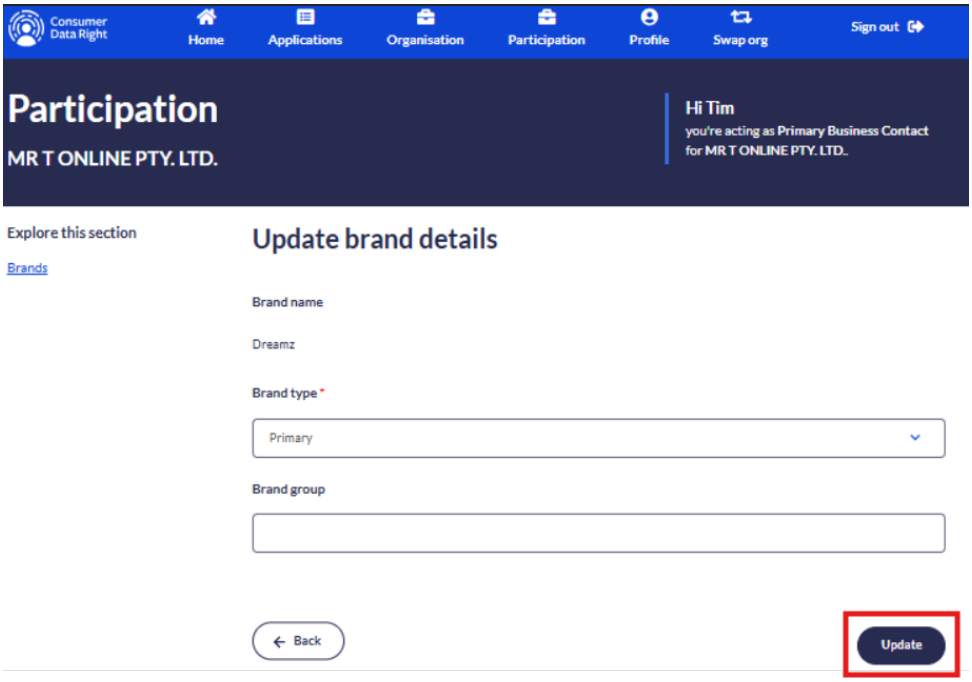
ACCC will publish your changes as soon as possible following our approval procedures. Should you require publication of your changes to be delayed beyond this, please enter your preferred date of publication below.

DD/MM/YYYY

Back | Submit request

- To update Brand type and Brand group use the **Update** link. Once the new details have been entered, click on **Update** to finalise the changes.





10.2 Maintain brand participation details

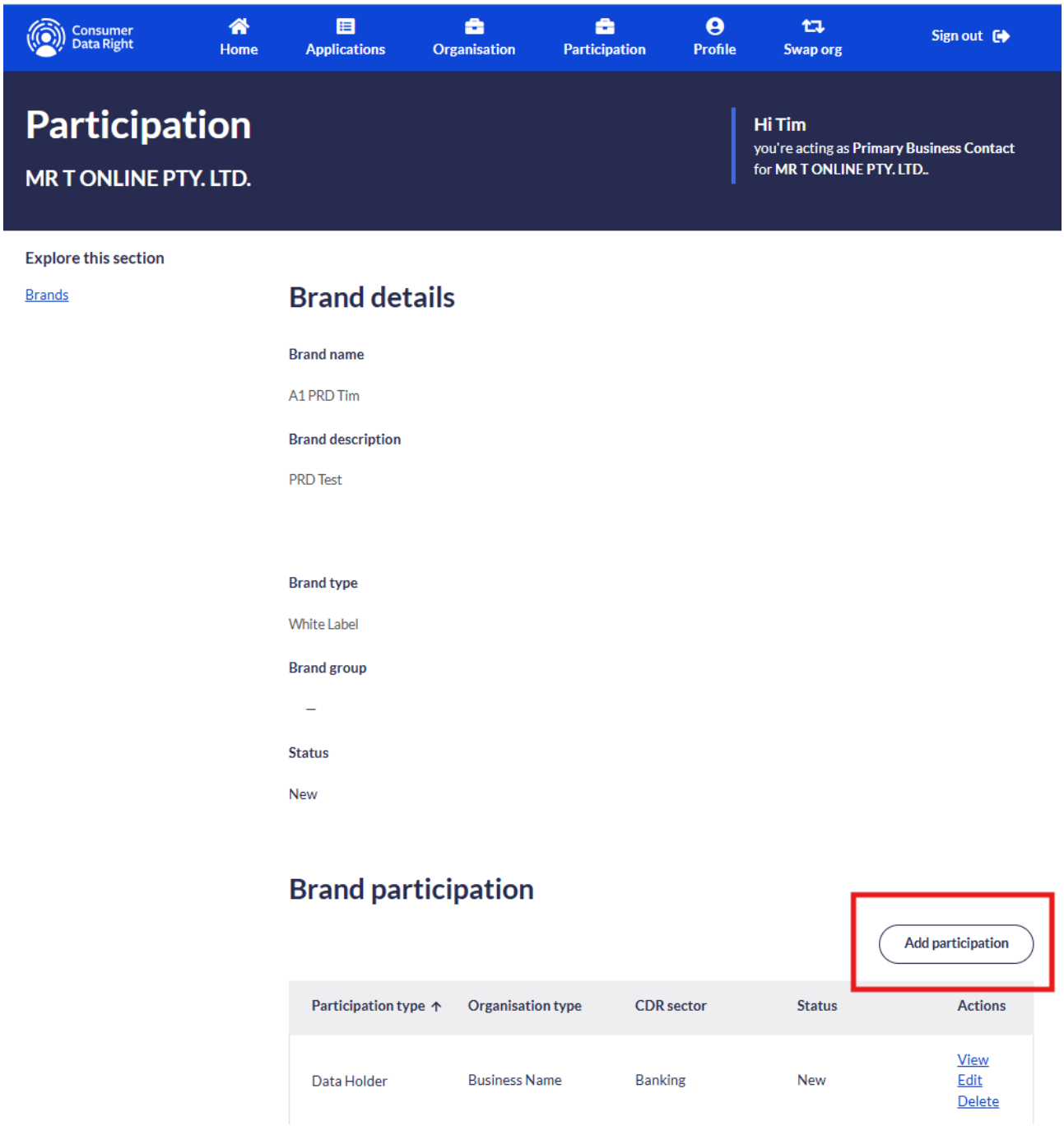
10.2.1 Add new brand participation

Brand participation details allow participants to publish information about their brands on the CDR Register, including details related to:

- product reference data sharing
- progress a brand from product reference data sharing purpose to consumer data sharing purpose
- manage brand-specific participation details, such as the industry sectors for which a brand acts as a data holder
- manage data recipient brand details and progress to activation

To add brand participation details, follow the steps below:

1. Log in to the Participant Portal at https://portal.cdr.gov.au and select **Participation** from the top navigation menu.
2. Select **View** against the brand that you wish to update.
3. Select **Add participation** and fill in the form.
4. Complete the form by providing your information in the required fields and save.



Fields:

- **Participation type** - For brand participation, can be a data holder or data recipient.
- **CDR Sector** - Industry sector.
- **Data Sharing Purpose** - Select the data sharing purpose applicable to the brand as a data holder. This field is not applicable for a data recipient.
    - **Product Reference Data**: Choose this option if the brand is required to participate in product reference data sharing.

  - **Consumer Data Sharing**: Choose this option if the brand is required to participate in the consumer data sharing journey. This option can also be selected for brands that are transitioning from the product reference data journey to the consumer data sharing journey.

Participants are provided with the flexibility to nominate separate brands for product reference data and consumer data sharing purposes for each industry sector. Once a brand has been activated, the participation cannot be changed back to product reference data purpose through the portal.

- **Logo URI** - Brand logo URI.
- **Website URL** - Publicly available website or web resource URI.
- **Public Base URI** - Base URI for the Consumer Data Standard public endpoints. This should encompass endpoints not requiring authentication that do not have a dedicated base URI.
- **Product Base URI** - Base URI for the Consumer Data Standard product reference data endpoints. **MAY** be the same as **Public Base URI.**
  When filling out the form, this value will default to the same value as **Public Base URI** (where Public Base URI has been added previously). This can be changed, or no value can be entered. The form will require a reason where the user has removed this value.
  Data Holders designated for the Energy sector are not required to expose energy product reference endpoints, but **MAY** provide an alternate base URI of the product reference endpoint hosted by the designated data holder.
- **Publish brand** - Can be selected to publish immediately. This will determine the status of the brand - if not published the Status will be **New**, if published the Status will be **PRD Active**. By selecting **Publish brand**, the brand information will be discoverable by Data Recipients via CDR APIs.
- Select **Add Participation** to continue.

Consumer Data Right | Home | Applications | Organisation | Participation | Profile | Swap org | Sign out

Participation

BOC

Hi Harsha
you're acting as **Primary Business Contact** for **BOC**.

Explore this section

Brands

Brand details

Brand participation details

Participation type *

Data Holder

CDR Sector *

Banking

Data Sharing purpose *

Select

Logo URI *

https://portal.preprod.cdr.gov.au/

Website URL *

https://portal.preprod.cdr.gov.au/

Public Base URI *

https://portal.preprod.cdr.gov.au/

Product Base URI

https://portal.preprod.cdr.gov.au/

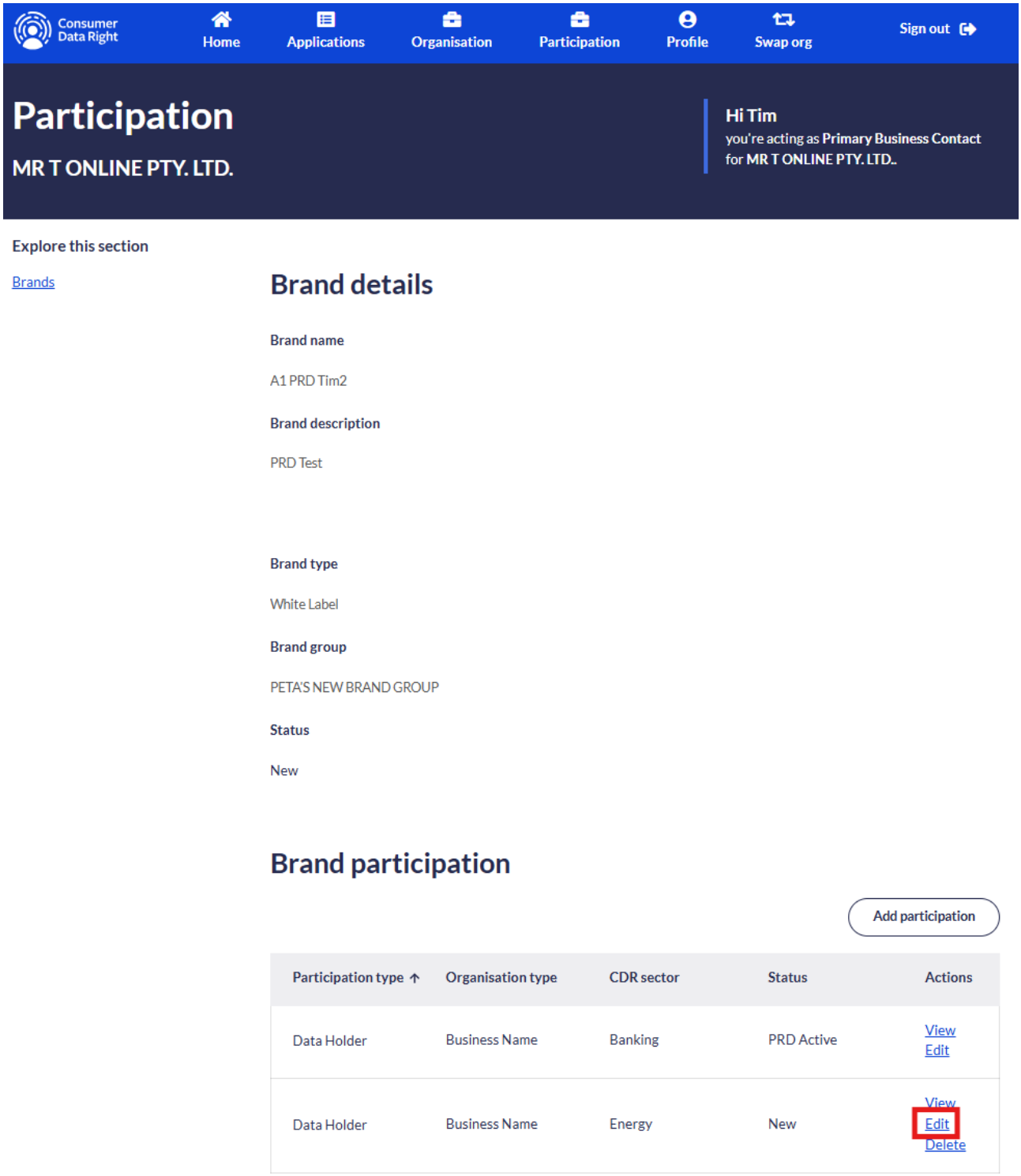
By selecting **Publish brand**, the brand information will be discoverable by Data Recipients via CDR APIs.

☑ **Publish brand**

← Back | Add participation

10.2.2 Modify existing brand participation details

To update the existing brand participation details, click on the edit link as shown below.



Update the fields as required and click update participation to save the changes successfully.

If a brand's current data sharing purpose is product reference data sharing and it needs to be progressed to consumer data sharing journey, update the **Data Sharing Purpose field from Product Reference Data Sharing to Consumer Data Sharing** before saving the changes. This

change will enable participants to provide production-related details for their brands, including certificates, endpoints, and authentication information, as well as submit requests for brand activation.

Consumer Data Right | Home | Applications | Organisation | Participation | Profile | Swap org | Sign out

Participation

Agrium SP Holdings Pty Ltd

Hi Harsha
you're acting as **Primary Business Contact** for **Agrium SP Holdings Pty Ltd.**

Explore this section

Brands

Brand details

Brand participation

Brand

Harsha Brand UAT Banking

Brand GUID

2c9178a0-5f9f-f111-85cf-000d3a6a45c5

Status

PRD Active

Participation type

Data Holder

CDR Sector

Banking

Data Sharing purpose *

Product Reference Data Sharing

Logo URI *

https://portal.preprod.cdr.gov.au/

Website URL *

https://portal.preprod.cdr.gov.au/

Public Base URI *

https://portal.preprod.cdr.gov.au/

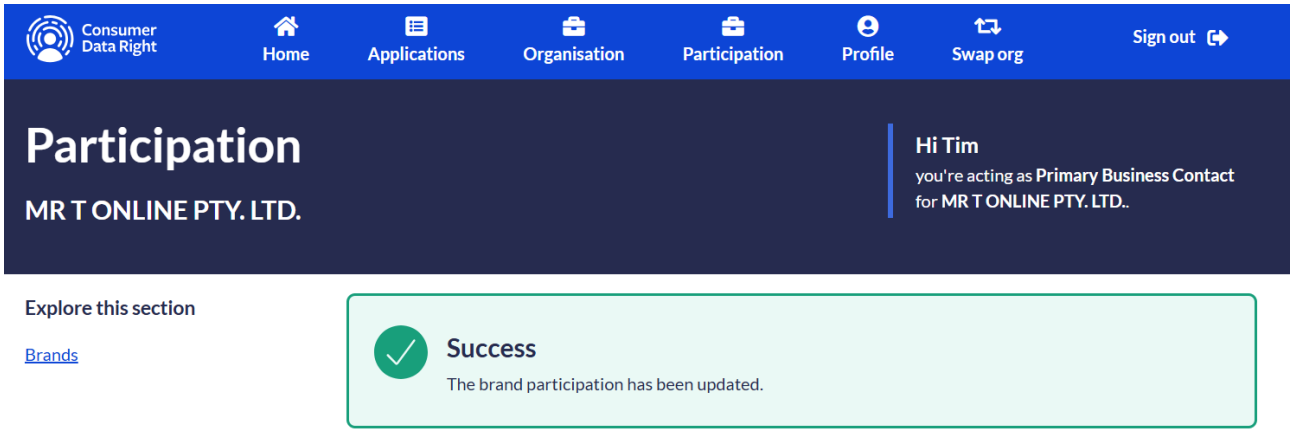
Product Base URI

https://portal.preprod.cdr.gov.au/

Back

Update participation

4. A Success screen will be displayed.



10.3 Progression to consumer data sharing

To progress a brand to consumer data sharing, click on the view link against the brand and follow the below steps:

1. After data sharing purpose is set to consumer data sharing for the brand, the data holder will need to enter relevant information on the **Production details** screens. When you view the brand, you can access production details at the bottom of the screen.

Consumer Data Right | Home | Applications | Organisation | Participation | Profile | Swap org | Sign out

Participation

MR T ONLINE PTY. LTD.

Hi Tim
you're acting as Primary Business Contact for MR T ONLINE PTY. LTD..

Explore this section

Brands

Brand details

Production and CTS details

Brand name

A1 PRD Tim1

Brand GUID

aa6516ee-8622-f111-9730-000d3a6afe8c

Participation type

Data Holder

CDR Sector

Banking

Data Sharing purpose

Consumer Data Sharing

Logo URI

https://www.logo

CDR Policy URL

Website URL

https://www.website

Status

New

Production details

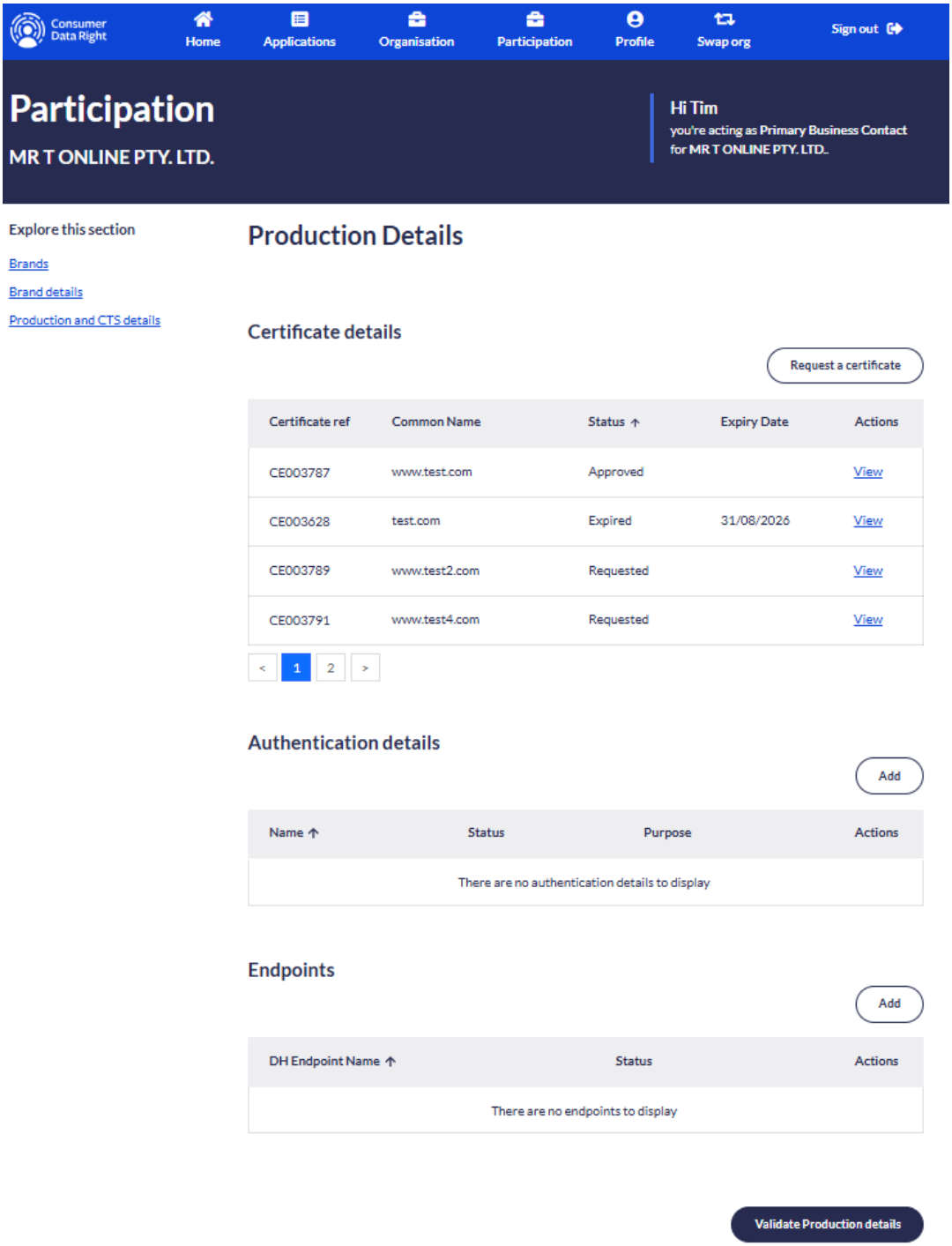
Access certificate details, authentication details and endpoints

CTS Details

Access CTS enrolment, certificate details, authentication details, endpoints and the final report

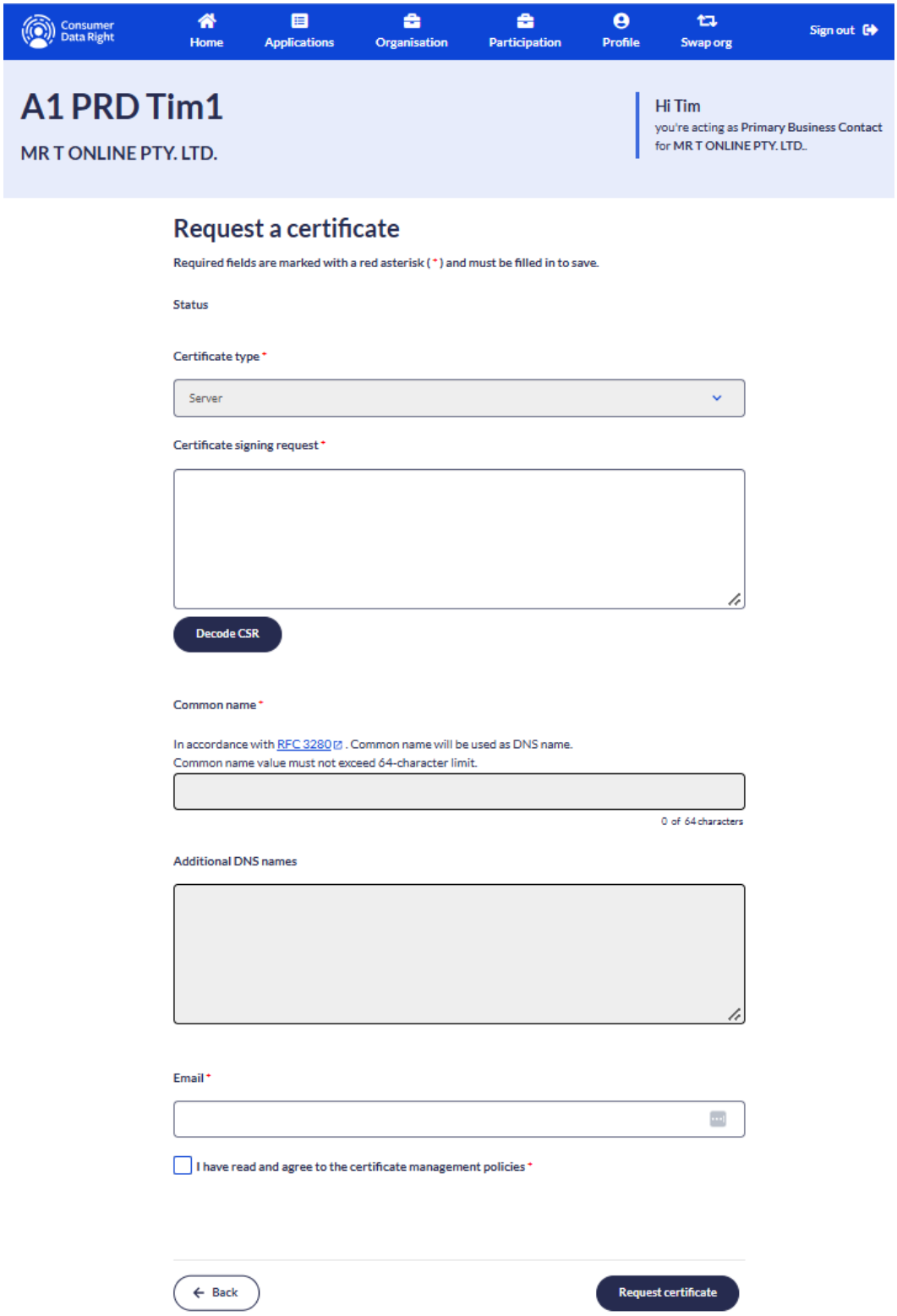
2. The Production details screen allows you to enter your details for 3 important areas - **Certificate details, Authentication details** and **Endpoints**.

> **Note:** This information will enable data holders to continue progress towards active consumer data sharing. If you need more information, please consult the Participant on-boarding guide or contact our Compliance team at accc-cdr@accc.gov.au.



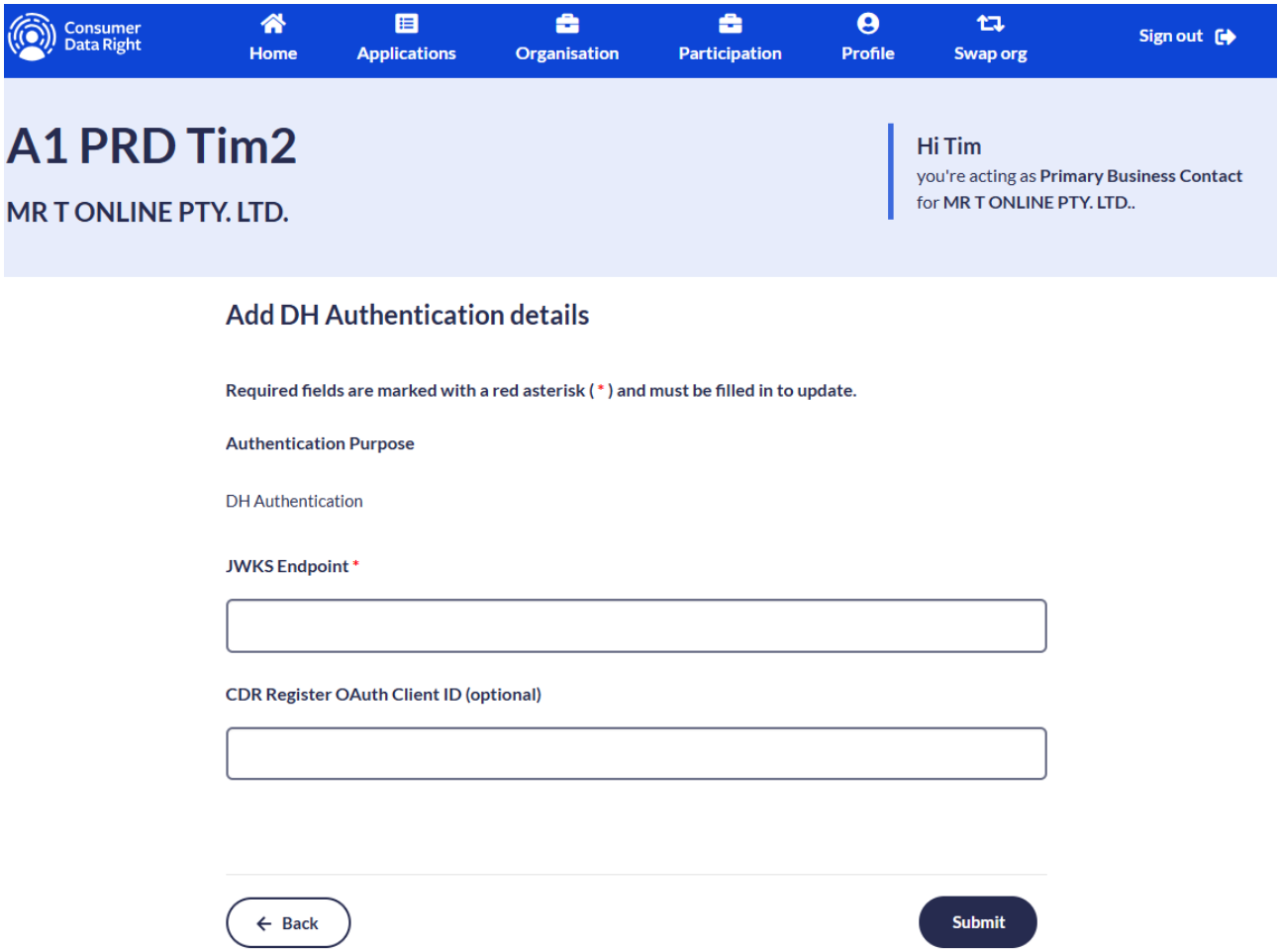
10.3.1 Certificate details

Complete the form to give the necessary details to request your certificate.



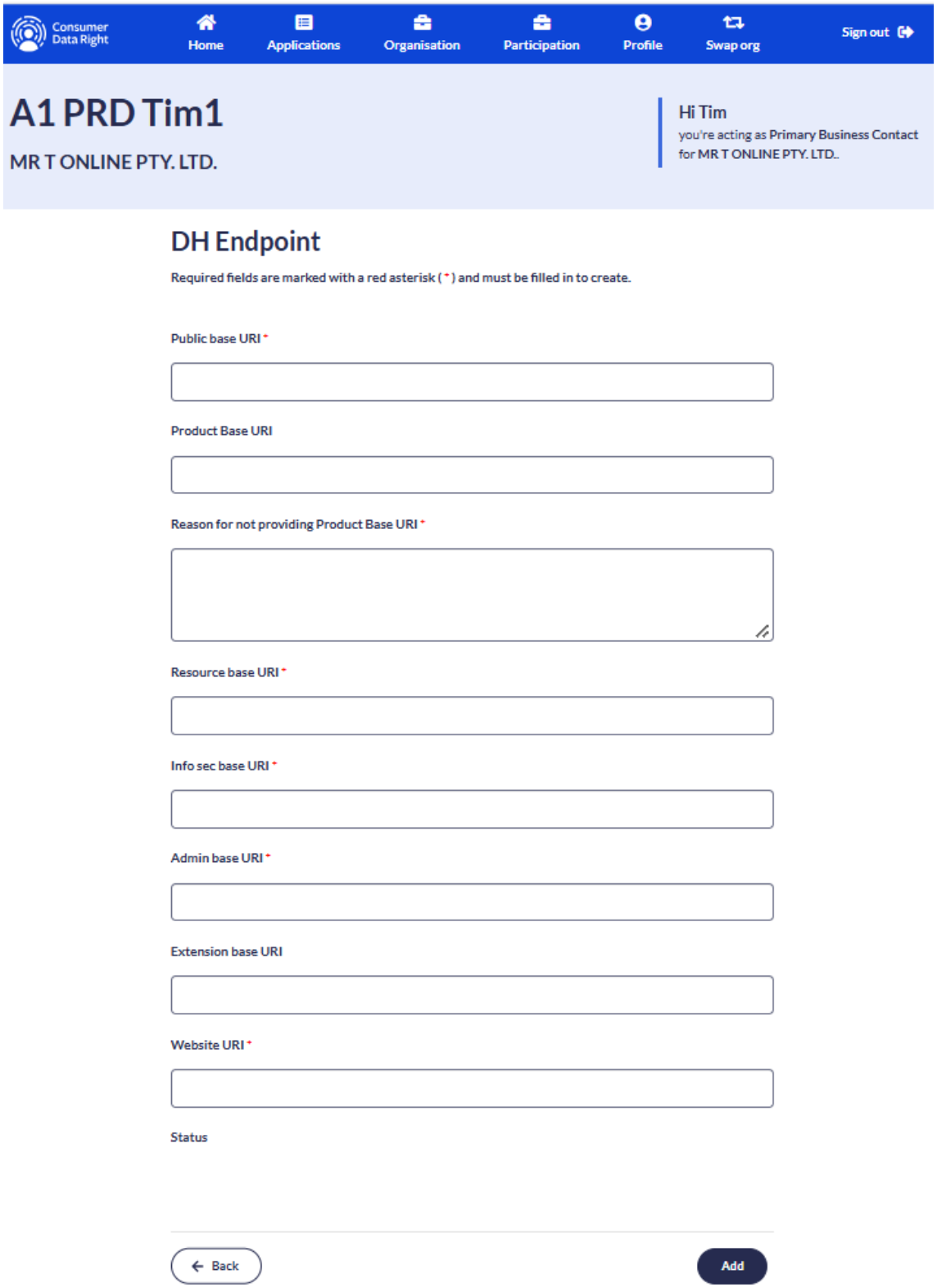
10.3.2 Authentication details

Complete the form to give authentication details.



10.3.3 Endpoints

Enter the details of your endpoints. Note that the form will prefill any values that you have entered while completing Brand Participation.


Consumer Data Right
Home
Applications
Organisation
Participation
Profile
Swap org
Sign out
A1 PRD Tim1
MR T ONLINE PTY. LTD.
Hi Tim
you're acting as Primary Business Contact for MR T ONLINE PTY. LTD..
DH Endpoint
Required fields are marked with a red asterisk (*) and must be filled in to create.
Public base URI *
Product Base URI
Reason for not providing Product Base URI *
Resource base URI *
Info sec base URI *
Admin base URI *
Extension base URI
Website URI *
Status
Back
Add

Fields:

Public base URI * - Base URI for the Consumer Data Standard public endpoints. This should encompass endpoints not requiring authentication that do not have a dedicated base URI.

Product Base URI - Base URI for the Consumer Data Standard product reference data endpoints. **MAY** be the same as the *publicBaseUri*.
Data Holders designated for the Energy sector are not required to expose energy product reference endpoints, but **MAY** provide the base URI of the product reference endpoints hosted by the designated data holder.

Reason for not providing Product Base URI - Product Base URI is not a mandatory field, but where it is not supplied a reason must be given - the reason becomes mandatory when Product Base URI does not have a value.

Resource base URI * - Base URI for the Consumer Data Standard resource endpoints. This **MUST** encompass all CDS resource endpoints requiring authentication.

Info sec base URI * - Base URI for the OIDC Discovery endpoint only.

Admin base URI * - Base URI for the Consumer Data Standard admin endpoints called by the CDR Register.

Extension base URI - Base URI for the Data Holder extension endpoints to the Consumer Data Standard (optional).

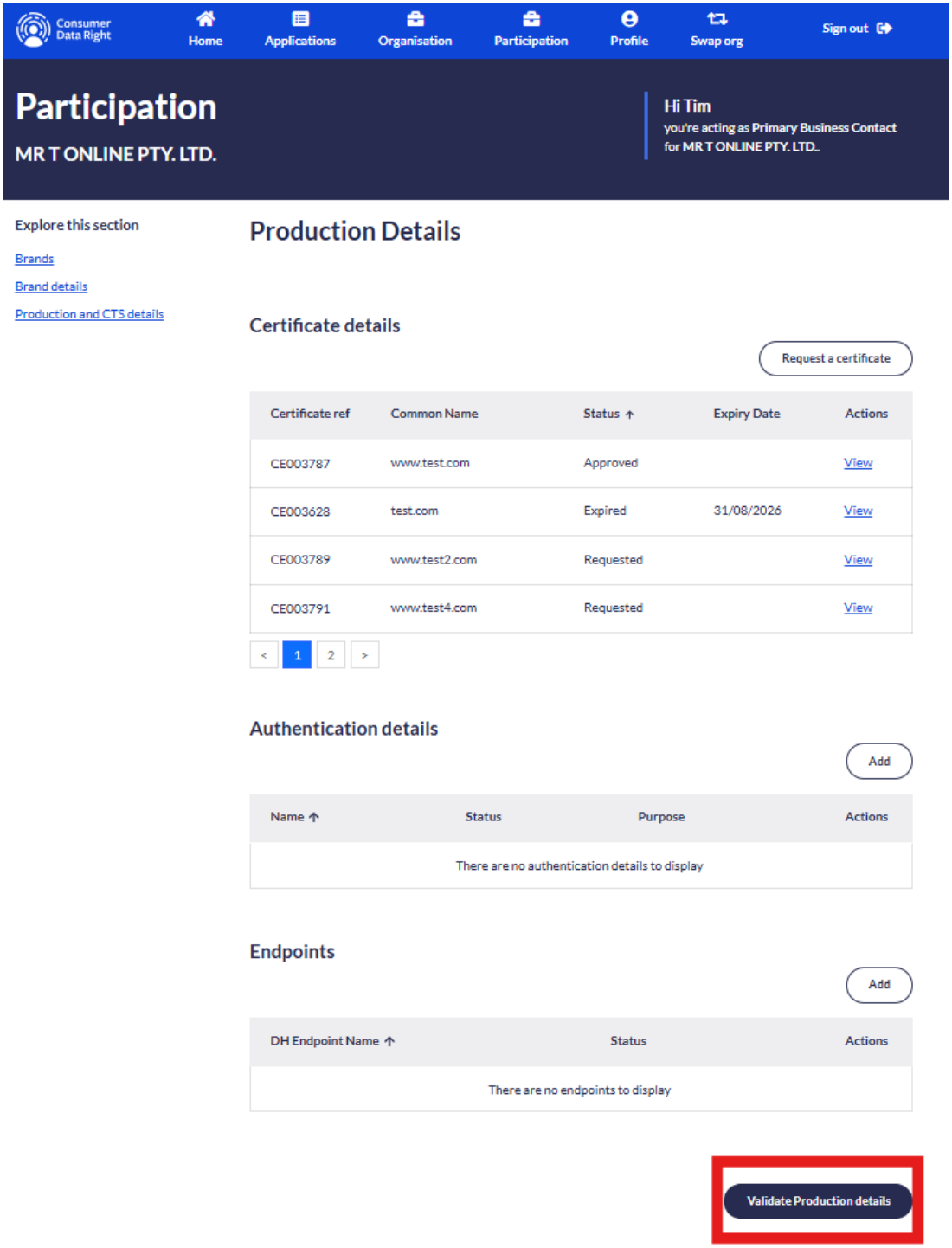
- TLS: for public endpoints.
- MTLS: for authenticated endpoints.

Website URI * - Publicly available website or web resource URI.

> **Note:** If you need any changes to endpoints after they are in production please contact our **Tech Ops** team at CDRTechnicalOperations@accc.gov.au

10.3.4 Validate Production Details

Once all required **Endpoints** and **Authentication details** have been added for the brand, and a valid certificate is in place, the participant can select **Validate Production Details** from the bottom-right corner of the page. This validation option is currently available only for **Data Holder** brand activations. **Data Recipient** brand activations must continue to be requested through the existing activation process.



If any above required information is missing, the system will display an error message identifying the missing details that must be provided before validation can proceed.

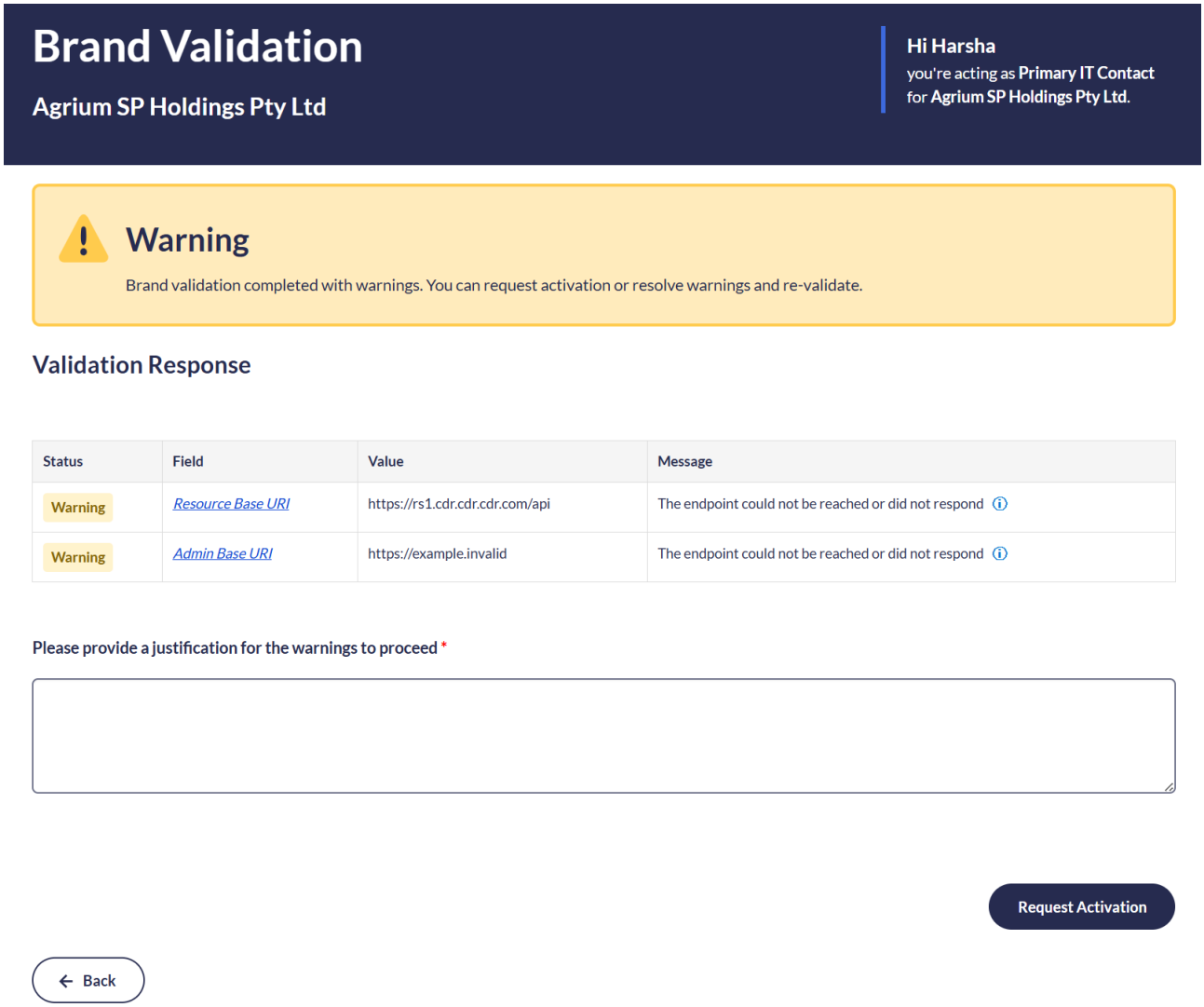
When **Validate Production Details** is selected, the system performs a resource validation. Resource validation is an automated assessment that checks whether the Data Holder's technical configuration is ready for activation.

As part of this process, the system reviews the participants:

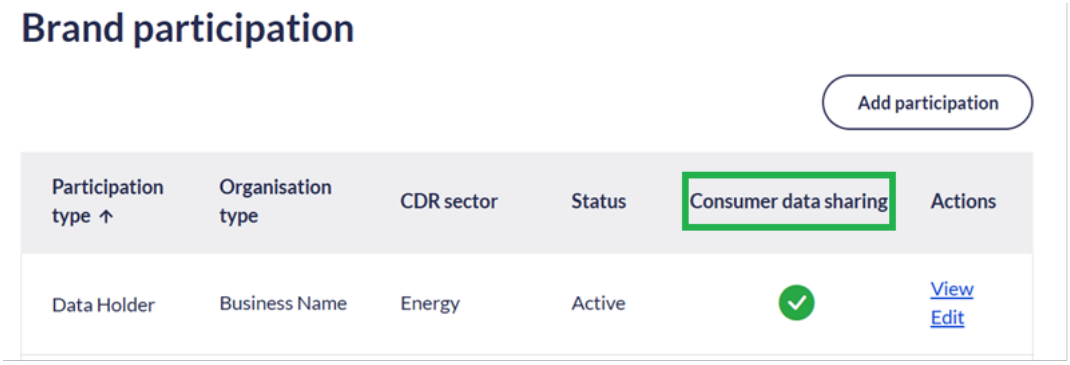
- Authentication details
- Endpoints
- Certificates
- Metadata
- Supporting URIs

These details are checked against a set of validation rules to ensure the configuration is ready for activation. Once all required validations have passed, the participant can submit a brand activation request through the Participant Portal by selecting **Request Activation**.

If any **warnings** are returned, the participant must provide a reason before submitting the request. If any **errors** are returned, the participant must correct the issues and re-run the validation before a request can be submitted for approval.



Brand activation is not automatic. CDR follows an internal assessment and approval process before approving a brand for Consumer Data Sharing. Users can monitor the status of their activation request in the **Consumer Data Sharing** column within the **Brand Participation** grid.



If an activation request is rejected, an automated email detailing the reasons for rejection is sent to the requestor, primary business contact, and primary IT contact. Participants can update the endpoint and authentication details and then resubmit the request for brand activation.

If the activation request is approved and scheduled by CDR, an automated notification is sent to the requestor, primary business contact, and primary IT contact. Once CDR completes the activation, a confirmation email is issued to notify participants that the brand has been successfully activated.

10.4 Maintain software product details

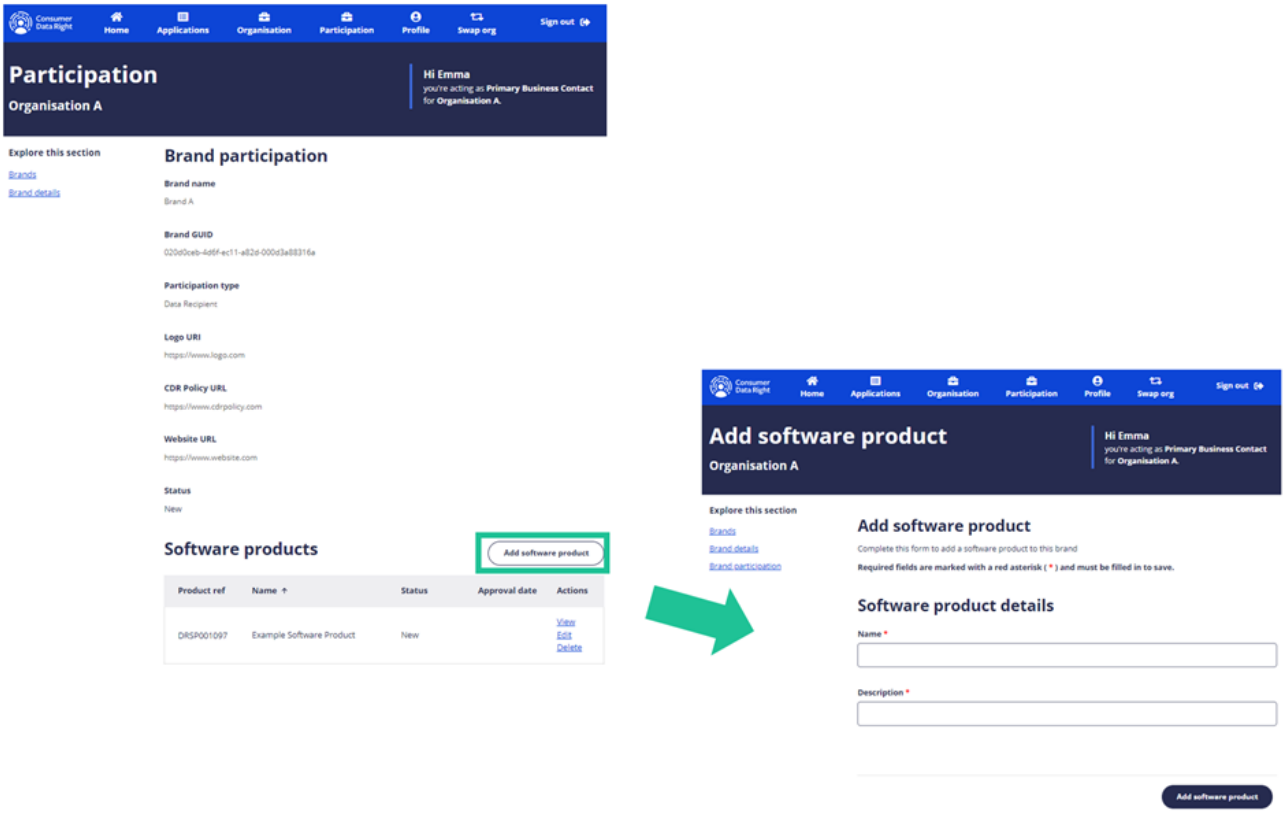
Unrestricted data recipients can create software products which will enable the collection of data from data holders.

> **Note:** Only a primary IT contact and authorised IT contact can add or edit software product details

10.4.1 Adding new software products

To add new software products, please follow the steps below:

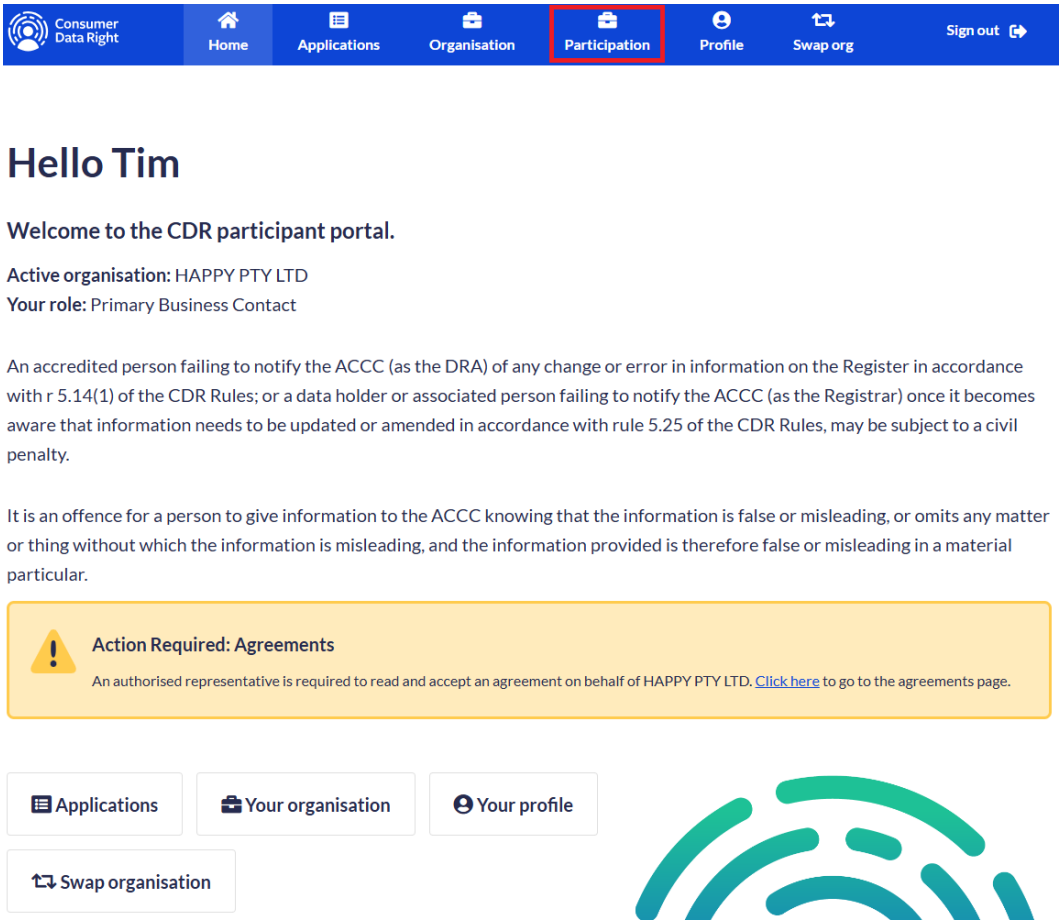
1. As a primary IT contact or authorised IT contact, log in to the Participant Portal at https://portal.cdr.gov.au and select **Participation** from the top navigation menu.
2. Select the **View** action on the brand that the software product that you wish to update.
3. Select the **View** action on the brand participation that the software product that you wish to update.
4. Select the **Add software product** button and fill in the form.



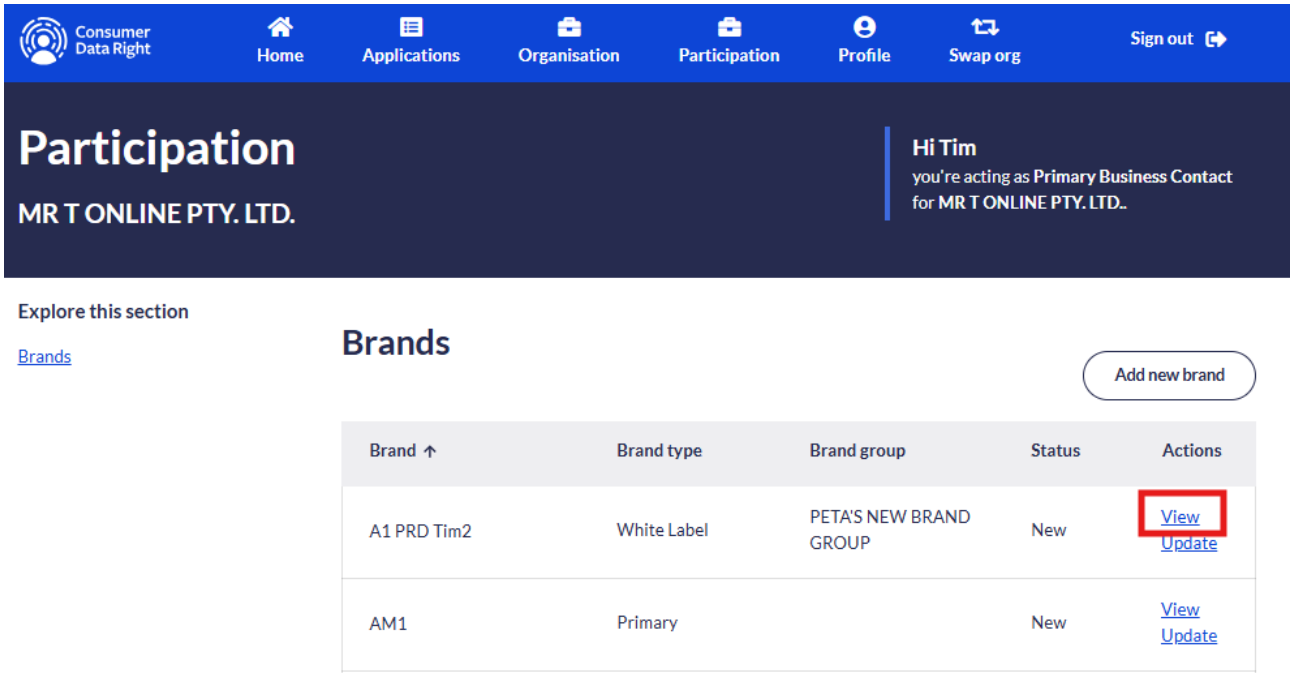
10.4.2 Maintaining existing software products

To maintain existing software products, please follow the steps below:

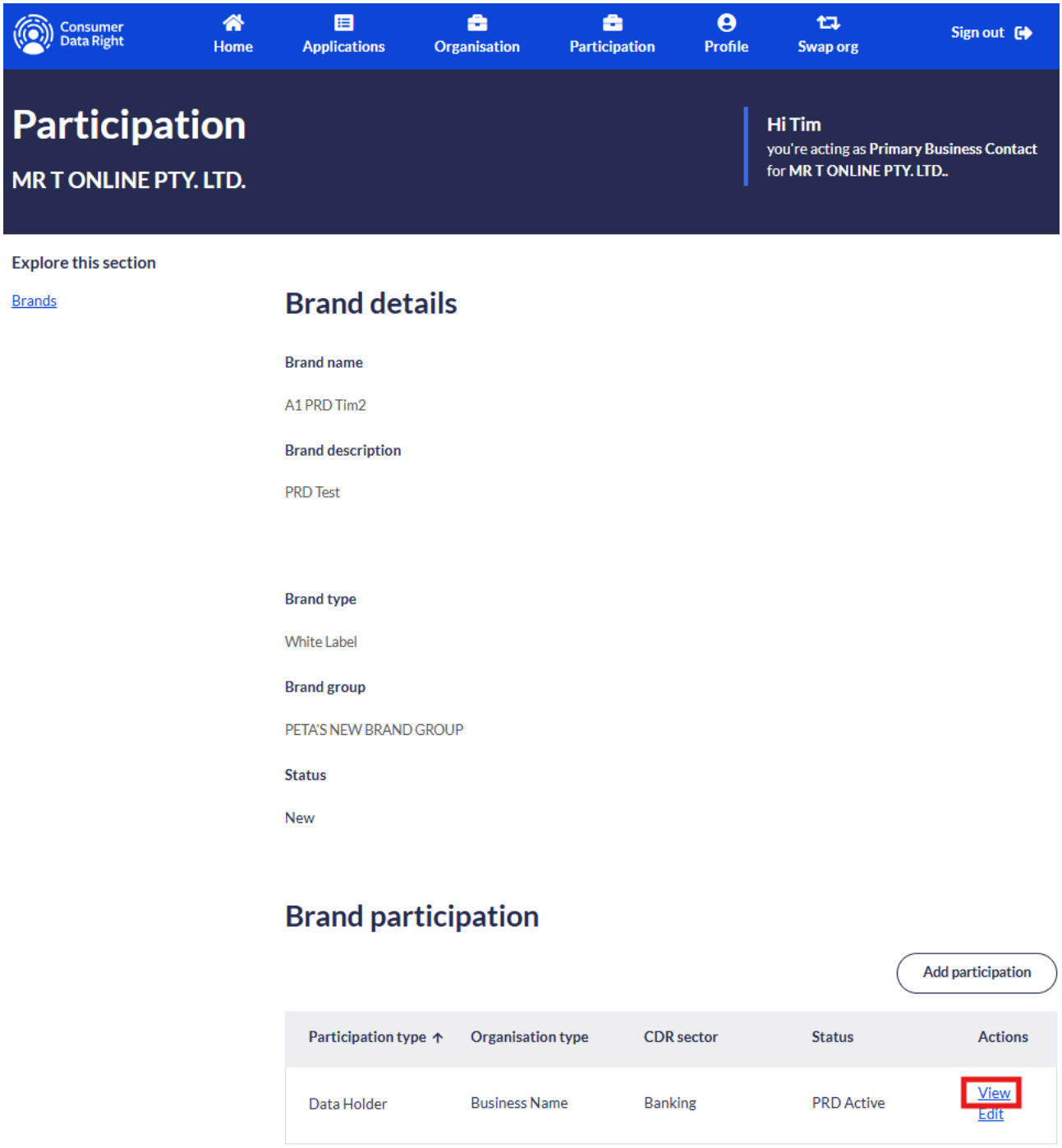
1. As a primary business contact, primary IT contact or authorised IT contact, log in to the Participant Portal at https://portal.cdr.gov.au and select **Participation** from the top navigation menu.



2. Select the **View** action on the brand for the software product that you wish to update



3. Select the **View** action on the brand participation for the software product that you wish to update



4. Select the **Edit** action for the software product you wish to update and fill in the form

Consumer Data Right | Home | Applications | Organisation | Participation | Profile | Swap org | Sign out

Participation

MR T ONLINE PTY. LTD.

Hi Tim
you're acting as Primary Business Contact for MR T ONLINE PTY. LTD..

Explore this section

Brands

Brand details

Brand participation

Brand name

Tim's brand test demo no pub date

Brand GUID

fb9673fc-ad09-ee11-a81c-000d3ad110d4

Participation type

Data Recipient

Logo URI

https://www.eee

CDR Policy URL

https://www.eee

Website URL

https://www.eee

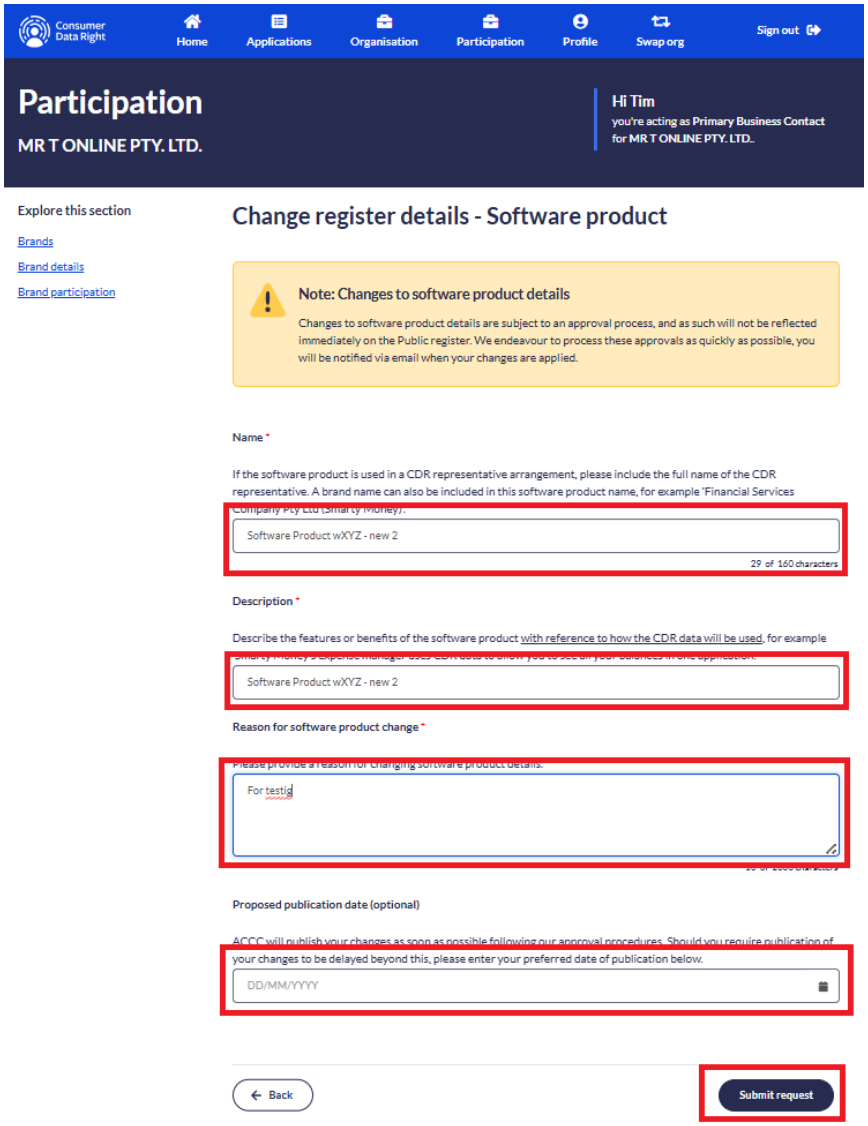
Status

Inactive

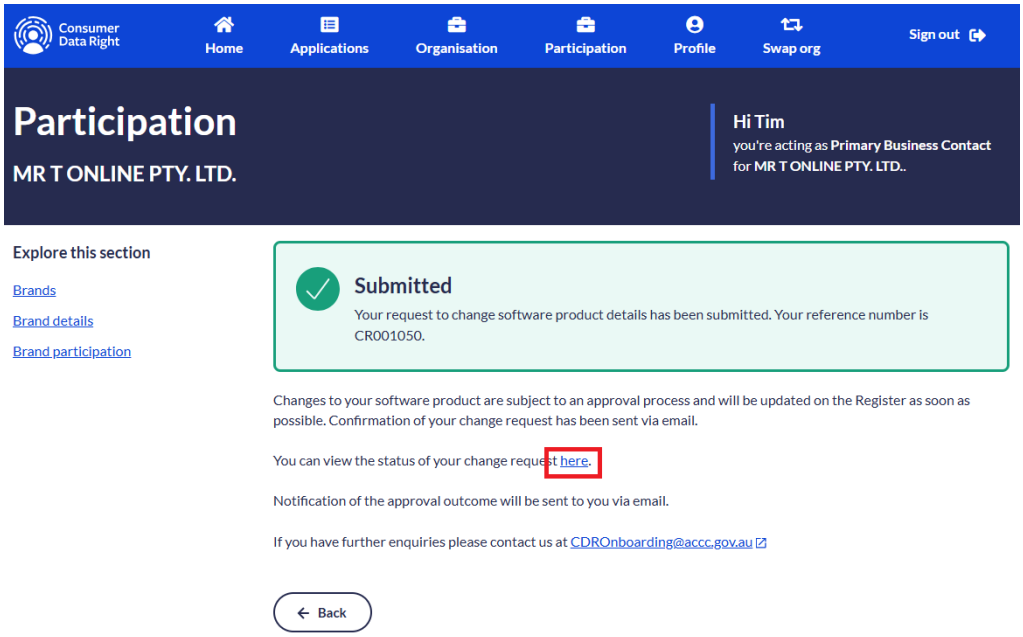
Software products

Add software product

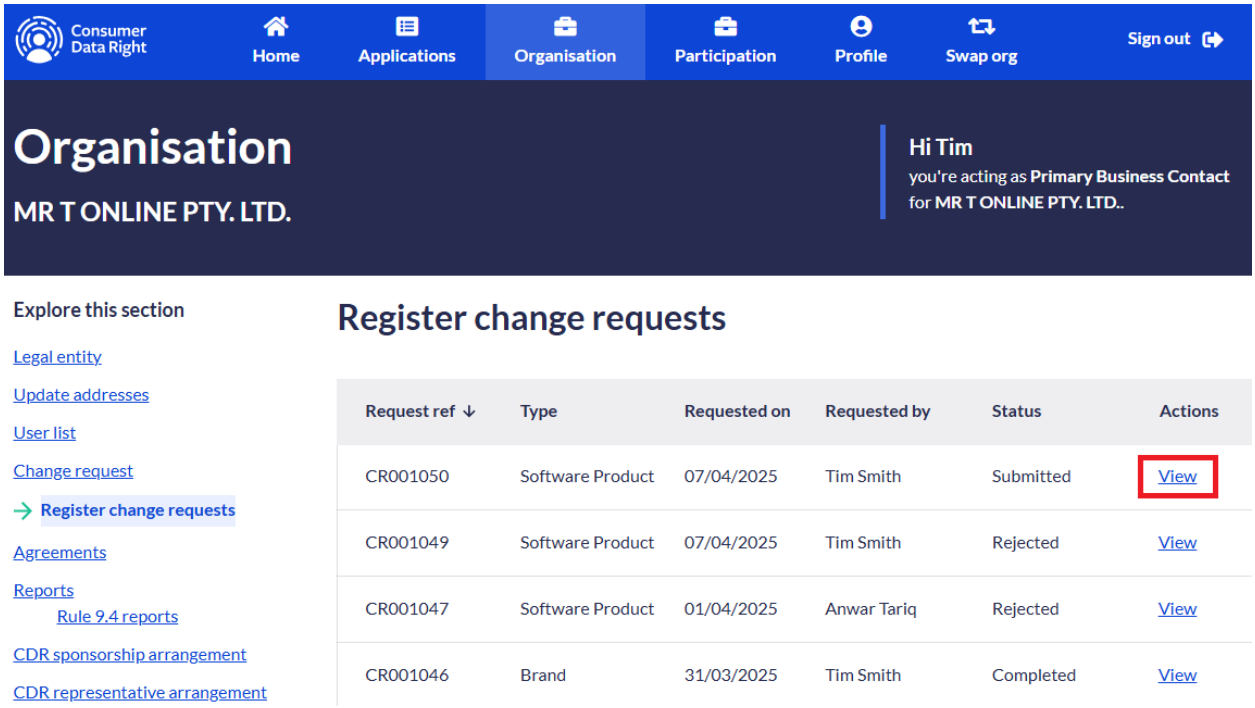
Product ref	Name ↑	Status	Approval date	Actions
DRSP004143	Software Product UAT new	Inactive		View Edit
DRSP001281	Software Product wXYZ - new 1	Active		View Edit



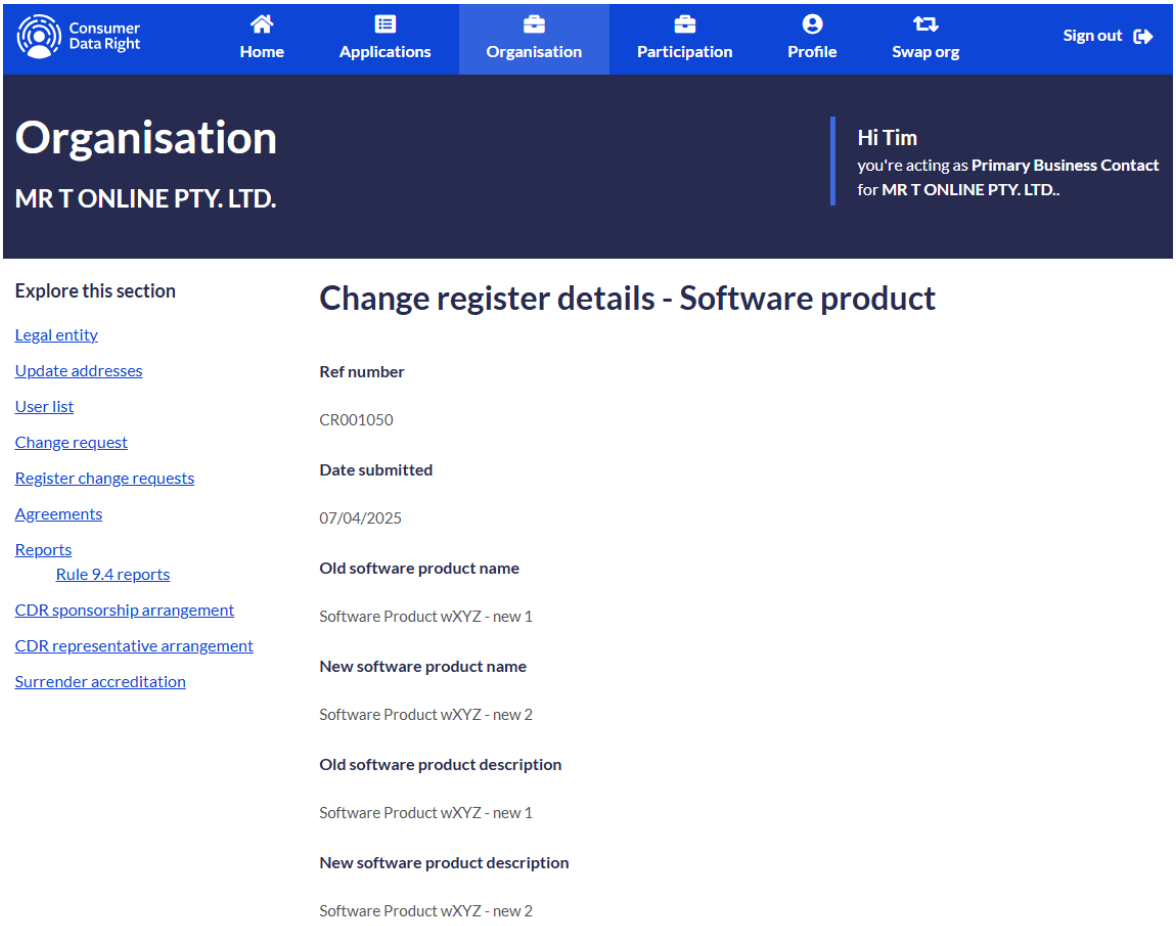
5. The system will return a Success Page.



6. The “here” link in the Success Page will take the user to a list of the current Change Requests



7. The “View” link will take the user to a page that contains details of the status of the change request.



10.5 Maintain Public Key Infrastructure (PKI) certificates

Public Key Infrastructure (PKI) certificates are a key component used in the CDR ecosystem to provide secure and private communications between participants. The ACCC, as the Registrar, is responsible for issuing PKI certificates to participants. Participants will be asked to request certificates – one for the environment the participant will test in, and one for the production environment, as part of the on-boarding process.

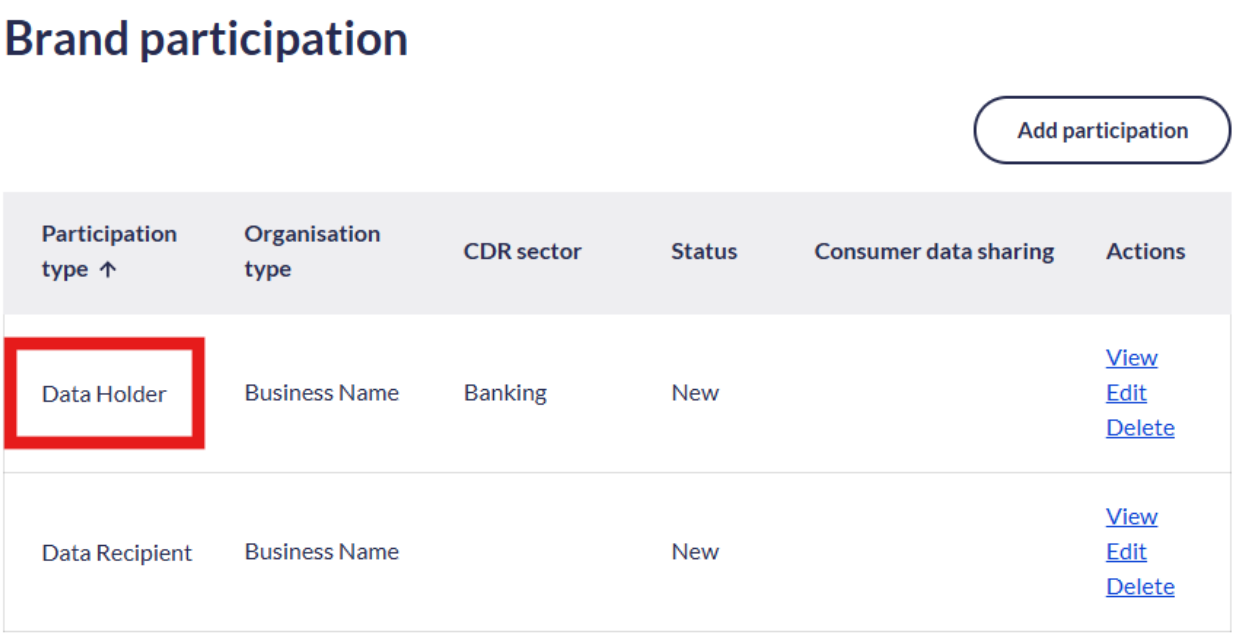
> **Note:** Only a primary business contact, primary IT contact and authorised IT contact can request, revoke and renew certificates.

For detailed information about certificates and how to request test and production certificates, please refer to Certificate Policy on the Digital certificate agreements and the Participant on-boarding guide which can be found on the CDR website. The certificate management section of the Consumer data standards has useful information as well.

> **Note:** The ACCC is maintaining the existing certificate management approach where they are applied ONLY at the Brand level. The update to the supporting Explanatory Document clarifies that there is no committed date for any change and that current arrangements continue to operate as is. Any future changes to certificate policy will be communicated separately following appropriate governance and consultation. If you have any queries on this matter, please contact the ACCC technical support team at CDRTechnicalOperations@accc.gov.au

10.6 Server certificates

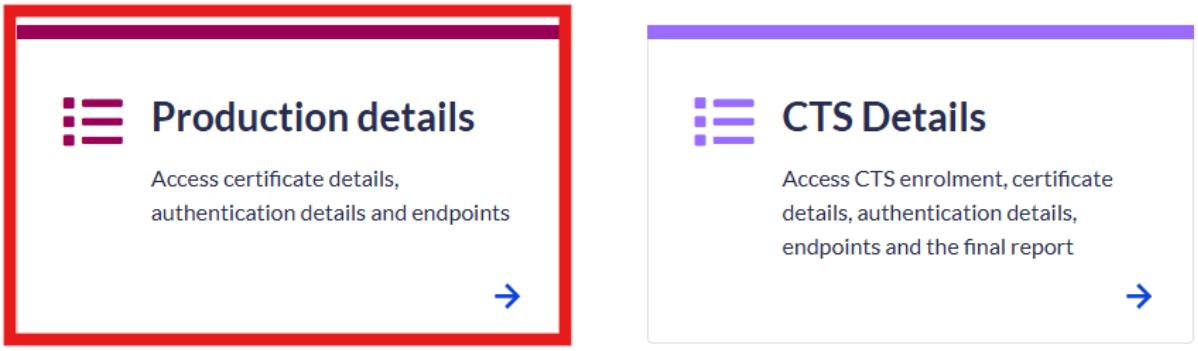
Server certificates are required for a Data Holder. When you manage a certificate as a Data Holder:



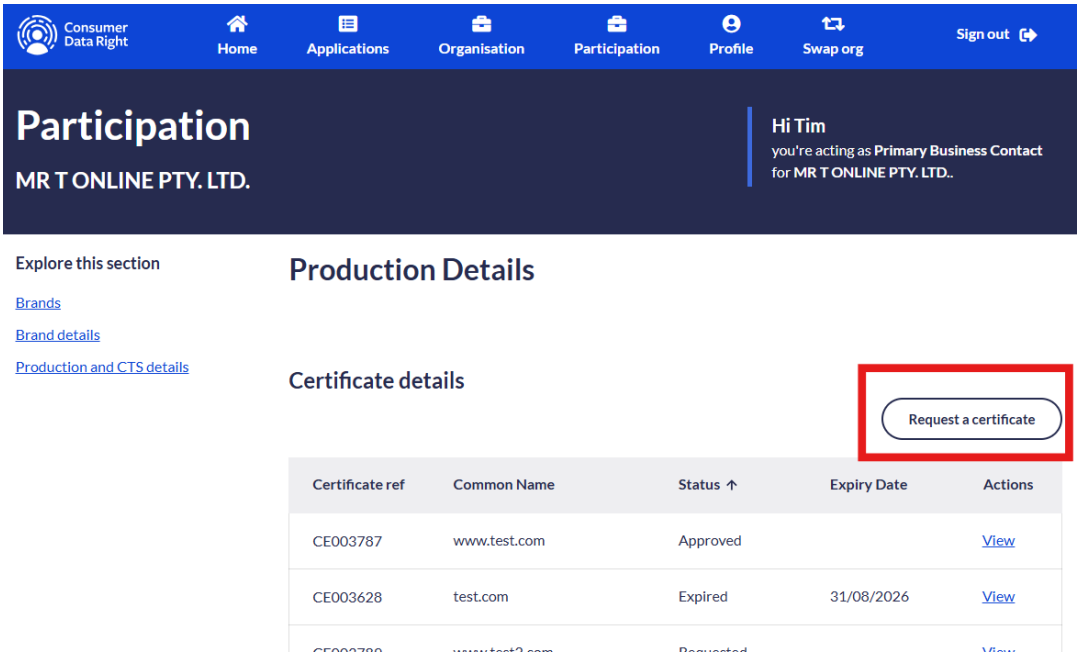
10.6.1 Request a server certificate

To manage Production certificates for a brand, please follow the instructions below:

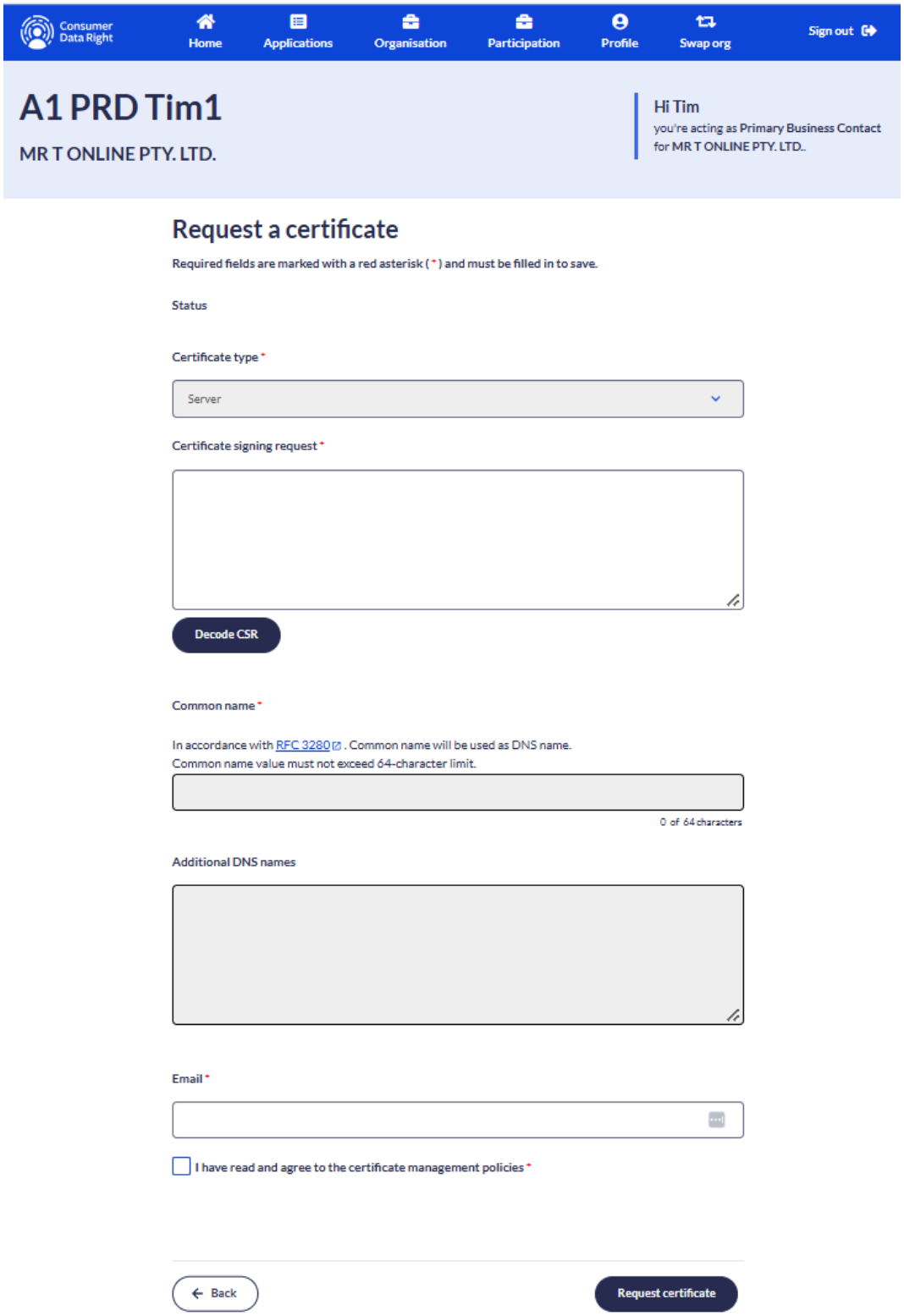
1. Log in to the Participant Portal at https://portal.cdr.gov.au and select **Participation** from the top navigation menu.
2. Select the **View** action on the brand that you wish to update.
3. Select the **View** action on the brand participation for the brand that you wish to update.
4. Select the **Production details** tile towards the bottom of the page to navigate to the relevant details page for the brands that the certificate is required for.



Click Request a certificate



Complete the form to request a certificate.



1. The system selects Server certificate as certificate type.

2. CSR is entered in the certificate signing request window and select decode CSR to decode and validate the CSR. A valid CSR is decoded.
3. Certificate common name and any SANs are decoded from the CSR and displayed.
4. Your email* address is then entered and after selecting the read and agree certificate management policies, we can select Request certificate.
5. A new certificate request is then submitted to technical operations team, and appears in the header tile with certificate status as submitted.

Note: the certificate approval and certificate renewal reminder emails are sent to the email address specified here.

10.6.2 Server certificate - CSR Validation

This change aims to enhance the current CSR decoding and validation capability in the Participant Portal by introducing additional validation rules aligned with Consumer Data Right (CDR) certificate standards. These validations include mandatory CSR attributes, Fully Qualified Domain Name checks, and cryptographic requirements to ensure certificate requests comply with the required standards before progressing through the issuance process.

The system will check the fields that are decoded from the CSR and display diagnostics where validations fail.

```
⚠ CSR successfully decoded with warnings/errors

== Subject ==
countryName: ZZ
organizationName: CAR LOANS
organizationalUnitName: Wrong Unit
commonName: 122.22.33.2

== Public Key ==
Algorithm: RSA
Key Size: 2048 bits

== Signature Algorithm ==
sha256WithRSAEncryption

== Fingerprints ==
MD5: F2F778AE313D57F4DEFA4ADAED566EBA
SHA1: 42B59FBF48083DC49B0259767CEE0BB2657B5151
SHA256: A8233A4B9FF121F34F8D8CC43494DF29EC955A0F05F9FE59632448626E2EE397
```

Validation Review

✕ Errors must be corrected before the certificate request can be submitted. If you need to change any certificate details i.e. Organization (O), Common Name (CN), Subject Alternate Name (SAN), Locality, State and Country or private key, please create a new Certificate Signing Request and update above before submitting.

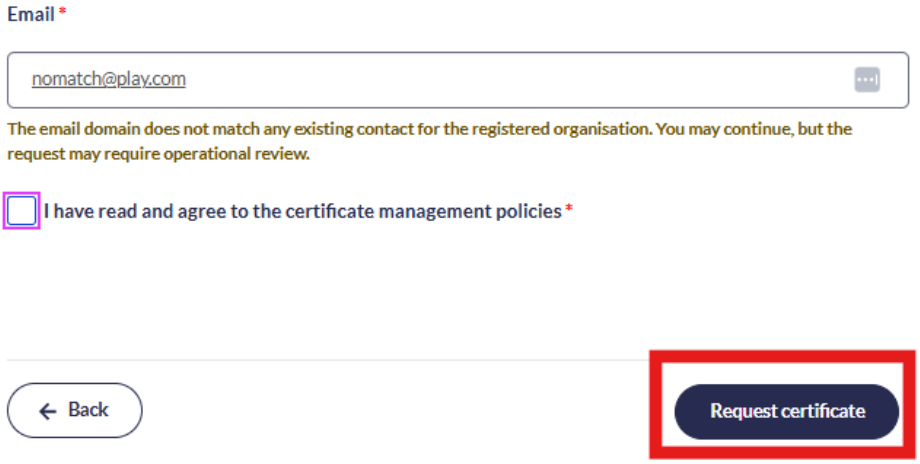
⚠ Warnings do not prevent submission. Requests submitted with warnings only will be subjected to review and may be rejected

Status	Message
Error	Common Name (CN) is not valid. A valid FQDN contains only letters (a-z, A-Z), numbers (0-9), hyphens and dots; no wildcards, IP addresses, URLs, paths, spaces, unsupported characters, or invalid DNS lengths.
Error	Organisation (OU) is not valid. Must be Consumer Data Right
Error	The country code value is invalid.
Warning	Organisation (O) does not match the registered Brand Name or Legal Entity (LE) Name. Submission is allowed but the request may be rejected on subsequent review.

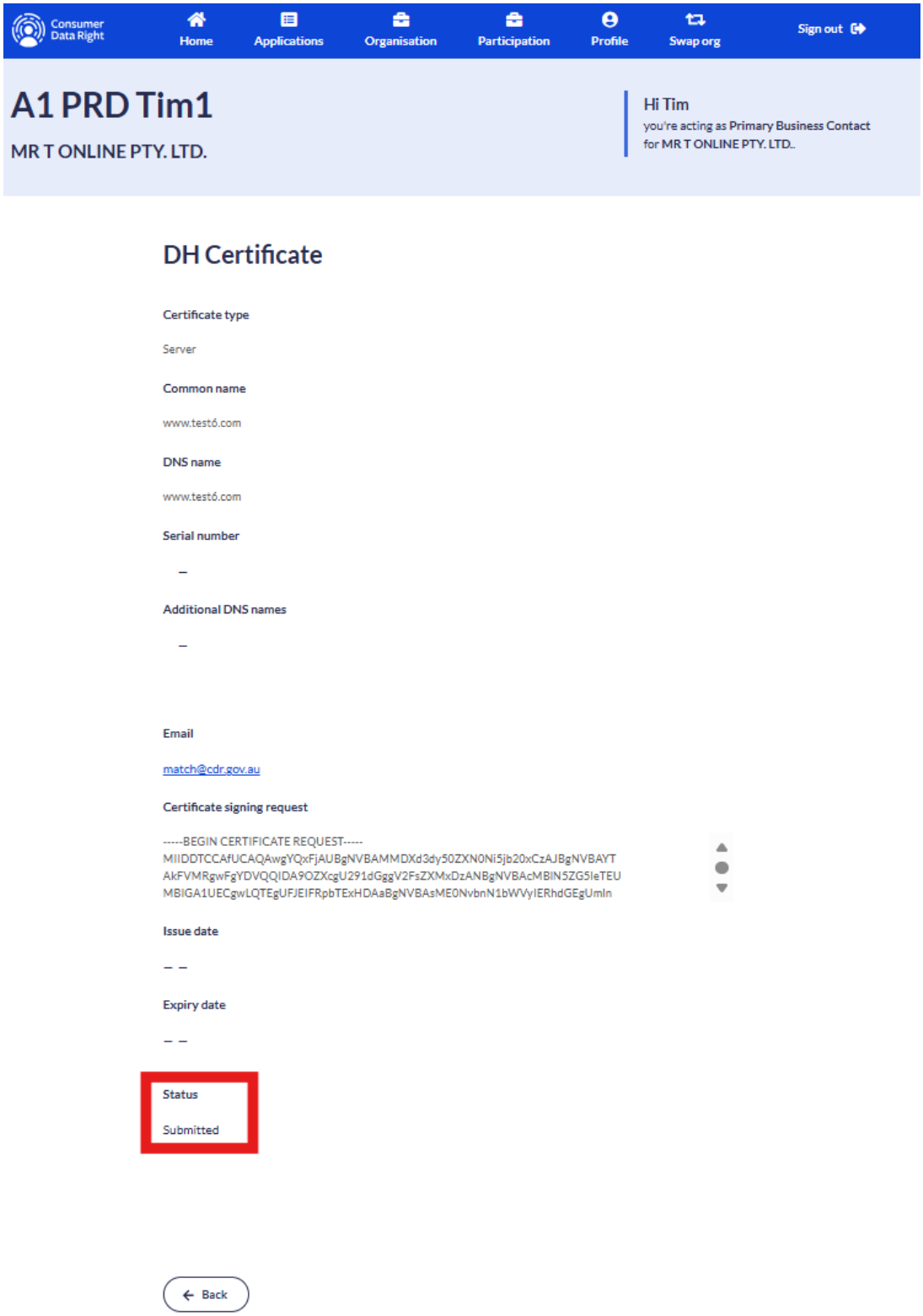
Errors will prevent a form from being submitted. This gives you the opportunity to fix the CSR errors and regenerate the CSR. Replace the CSR and decode it again until all of the errors are resolved. Warning messages will still allow submission, but may alert you to a problem with a field (i.e. a typo in an email address).

If the CSR decode is not displaying errors, submit the form to proceed.

An additional test is performed on your email address, where the email domain name is matched against other email domains associated with your account. This is for your information only and the form can still be submitted. We recommend that you use a shared mailbox so that renewals and reminders are less likely to be sent to people who are on leave or have left



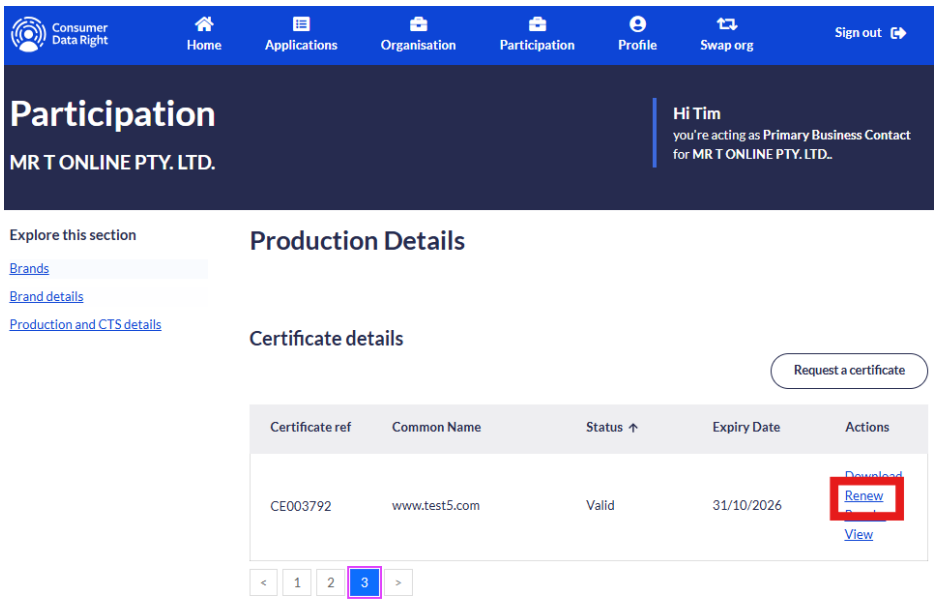
If the form is complete, you can Request a Certificate.



You will be presented with a success screen that shows a summary of your application. Your certificate will be provisioned as soon as we can process it.

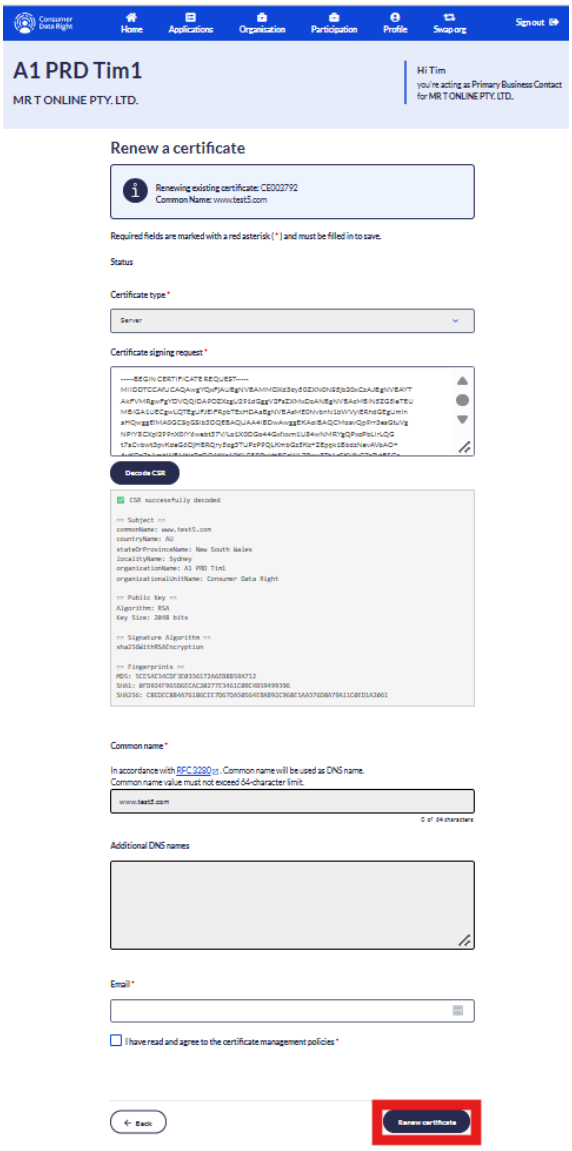
10.6.3 Server certificate - Renew a certificate

30 days before a valid certificate expires, a link will appear for that certificate allowing you to easily renew it.



When you renew a server certificate, the system will retrieve your existing CSR, decode it and apply it to the renewal request. It will automatically apply the existing validation rules.

> **Note** - there is a strong possibility that it will immediately pass these rules, since it has been scrutinised and evaluated before it was approved.

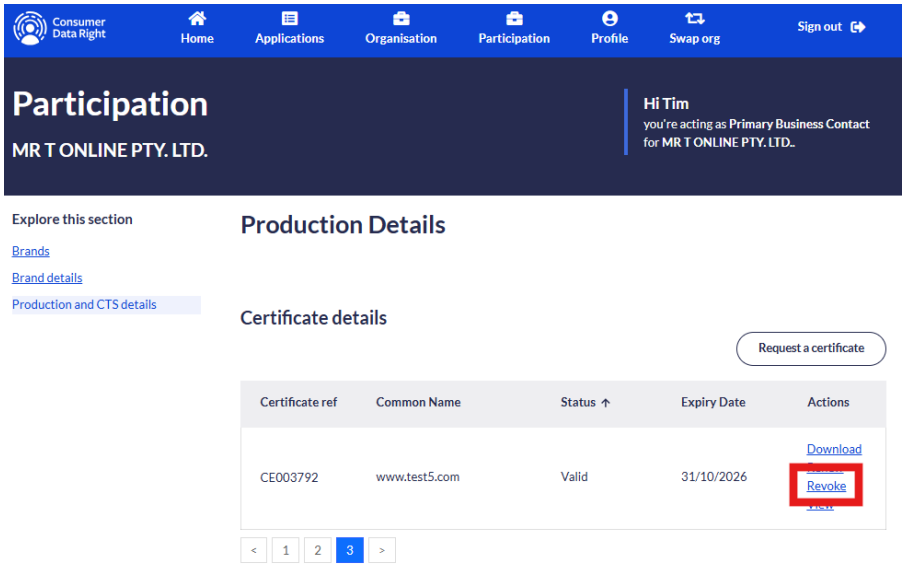


Please add/ensure the contact email is correct, check the acknowledgement box and click Renew Certificate.

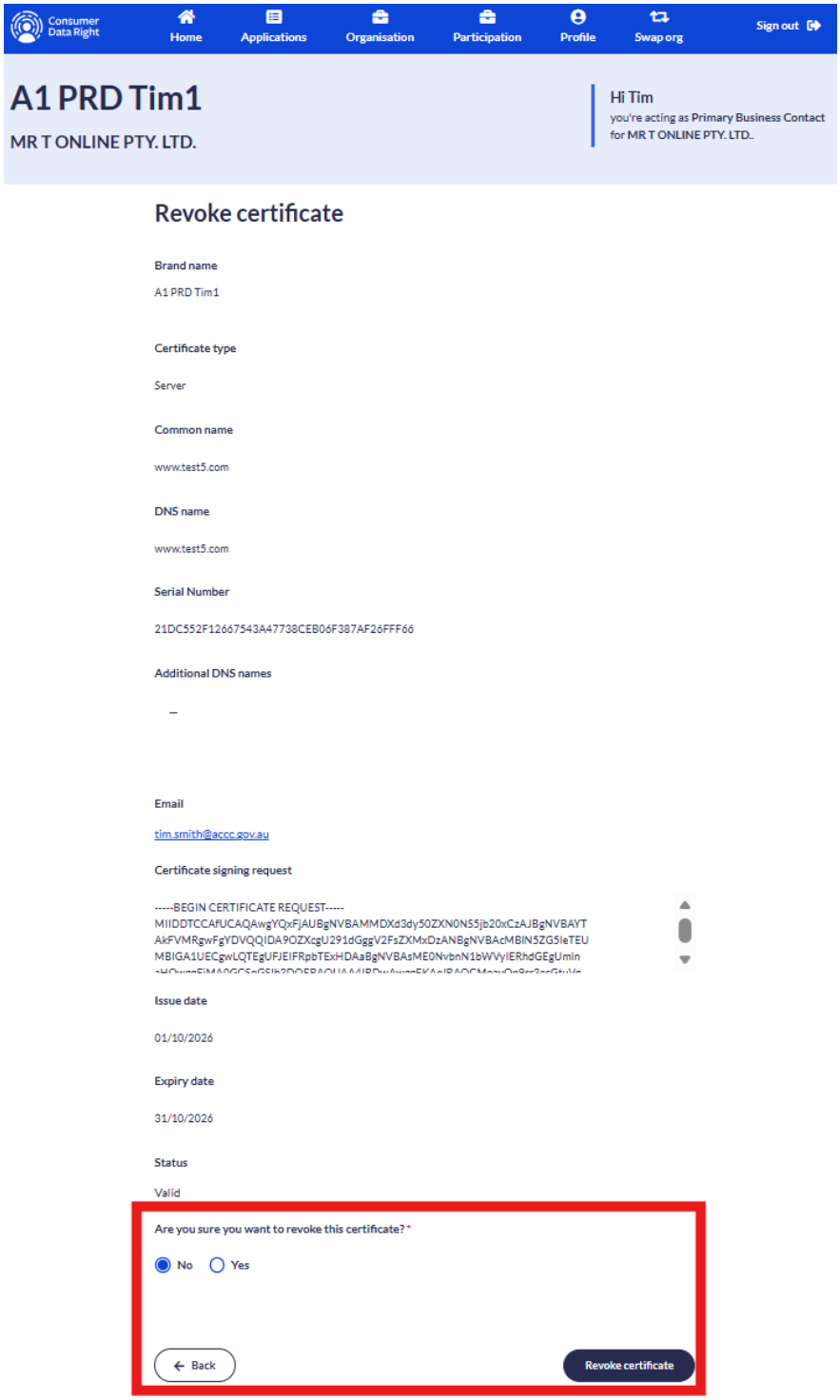
Should there be any errors, correct the errors in the CSR, regenerate and reapply the CSR as you would for a new one, then Submit.

10.6.4 Server certificate - Revoke a certificate

Any valid certificate provides a link from which it can be revoked.

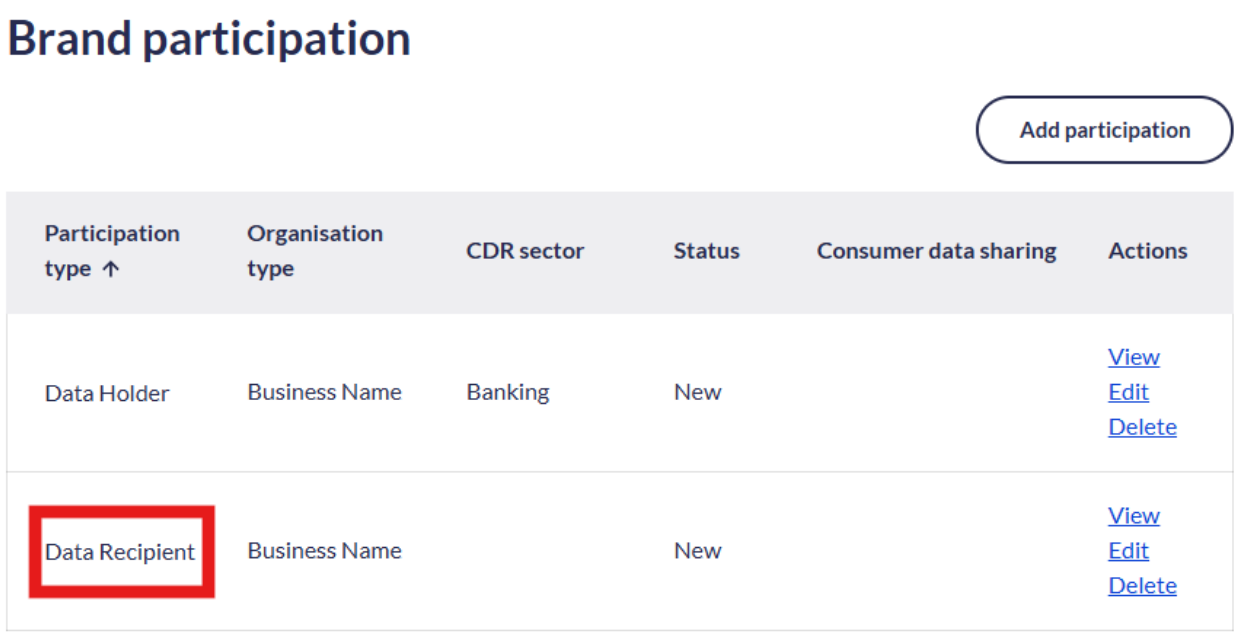


The system will present a summary page giving the details of that certificate and prompt you to confirm that you are sure - if so, click to revoke the certificate.


Consumer Data Right
Home
Applications
Organisation
Participation
Profile
Swap org
Sign out
A1 PRD Tim1
MR T ONLINE PTY. LTD.
Hi Tim
you're acting as Primary Business Contact for MR T ONLINE PTY. LTD.
Revoke certificate
Brand name
A1 PRD Tim1
Certificate type
Server
Common name
www.test5.com
DNS name
www.test5.com
Serial Number
21DC552F12667543A47738CEB06F387AF26FFF66
Additional DNS names
–
Email
tim.smith@accc.gov.au
Certificate signing request
-----BEGIN CERTIFICATE REQUEST-----
Issue date
01/10/2026
Expiry date
31/10/2026
Status
Valid
Are you sure you want to revoke this certificate? *
No
Yes
Back
Revoke certificate

10.7 Client certificates

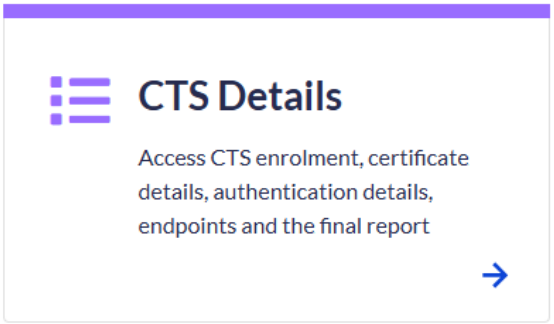
Client certificates are required for a Data Recipient. When you manage a certificate as a Data Recipient:



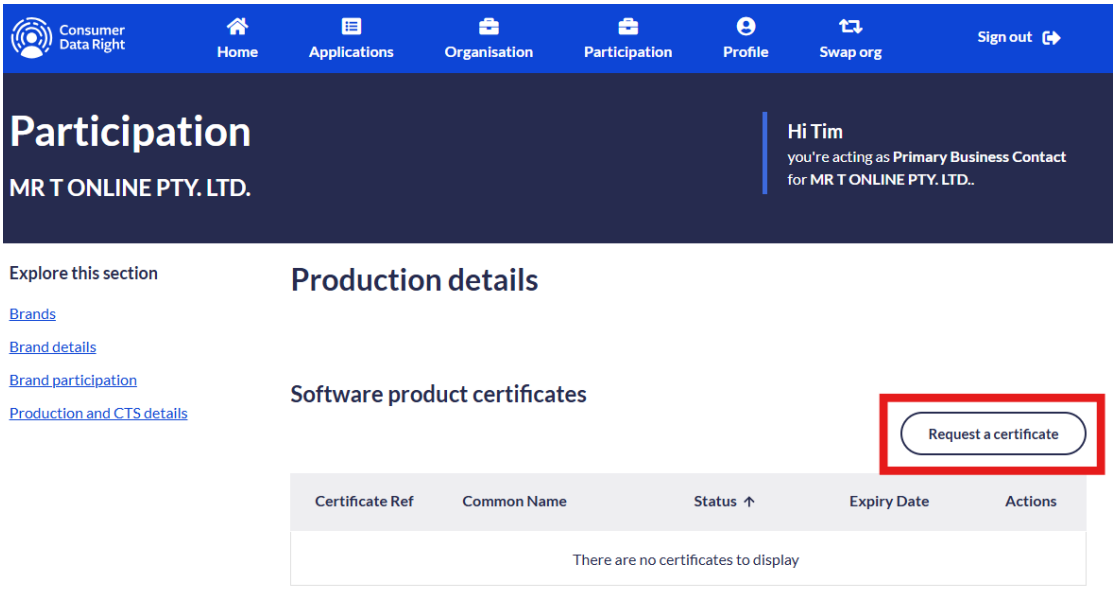
10.7.1 Request a client certificate

To manage Production or CTS certificates for a software product, please follow the instructions below:

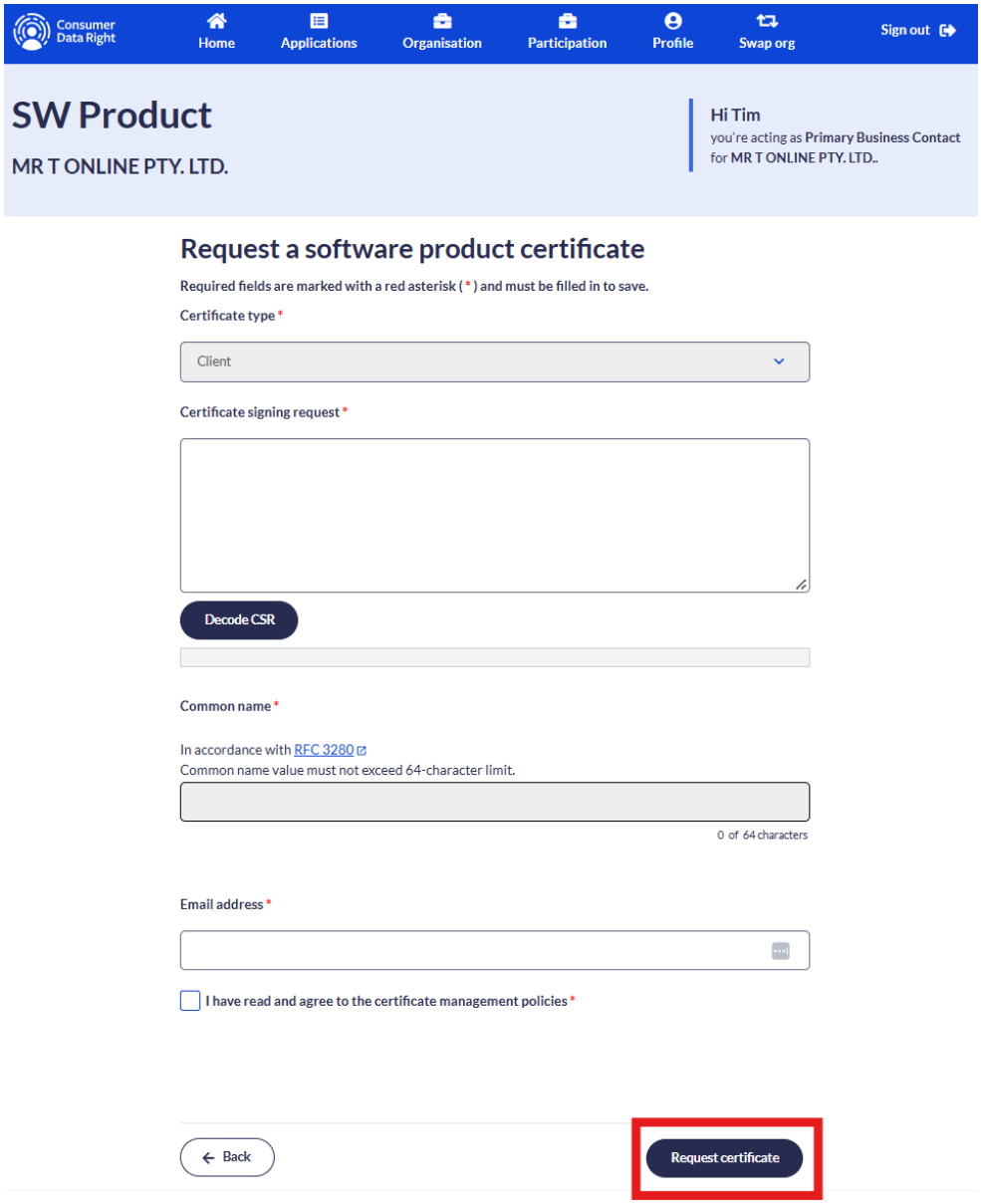
1. Log in to the Participant Portal at https://portal.cdr.gov.au and select **Participation** from the top navigation menu.
2. Select the **View** action on the brand of the software product that you wish to update.
3. Select the **View** action on the brand participation that the software product that you wish to update.
4. Select the **View** action on the software product that you wish to update.
5. Select either **Production details** tile towards the bottom of the page to navigate to the relevant details page for the software product that the certificate is required for.



Click Request a certificate



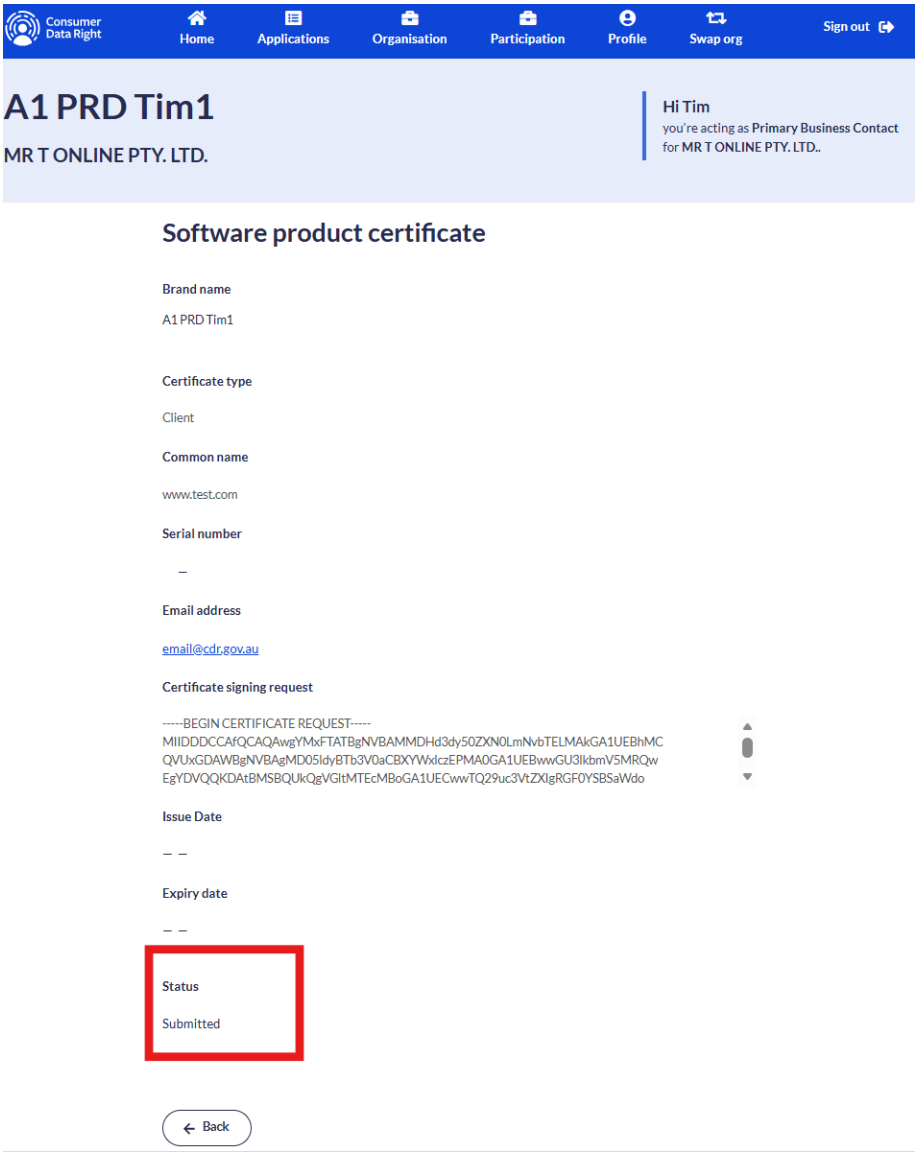
Complete the form to request a certificate.



After clicking Request a certificate

1. The system selects Client certificate as certificate type.
2. CSR is entered in the certificate signing request window and select decode CSR to decode and validate the CSR. A valid CSR is decoded.
3. Certificate common name and any SANs are decoded from the CSR and displayed.
4. Your email* address is then entered and after selecting the read and agree certificate management policies, you can select Request certificate.
5. A new certificate request is then submitted to technical operations team, and appears in the header tile with certificate status as submitted.

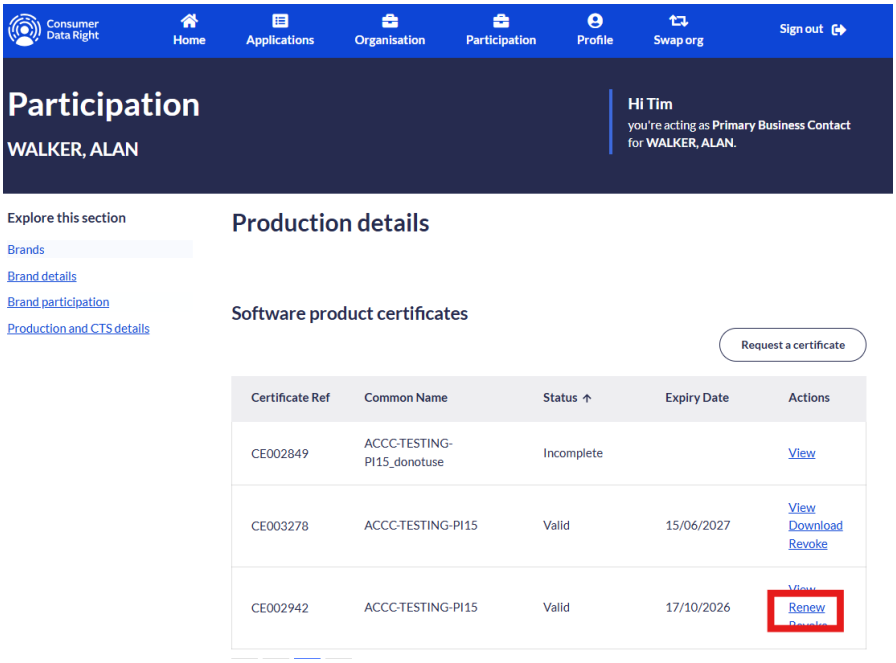
> **Note:** the certificate approval and certificate renewal reminder emails are sent to the email address specified here.



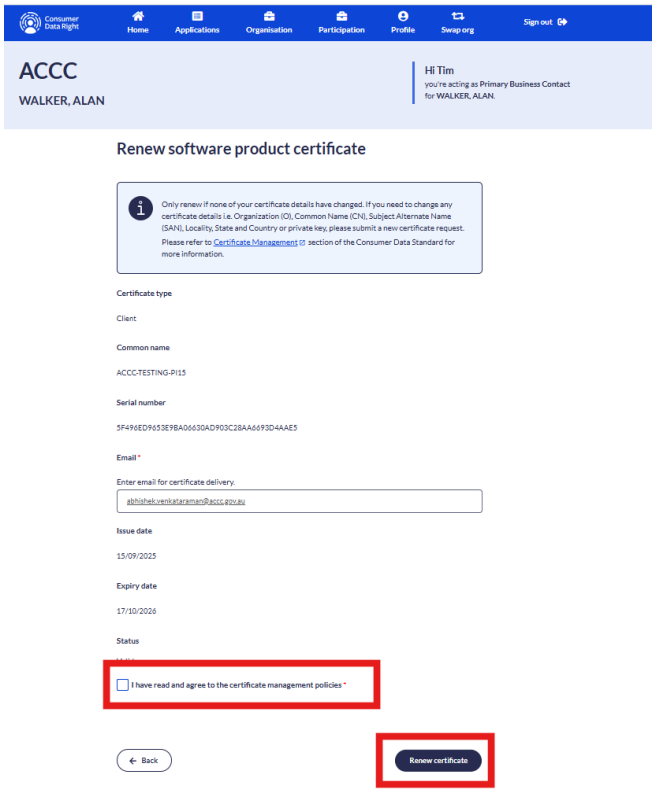
You will be presented with a success screen that shows a summary of your application. Your certificate will be provisioned as soon as we can process it.

10.7.2 Client certificate - Renew a certificate

30 days before a valid certificate expires, a link will appear for that certificate allowing you to easily renew it.



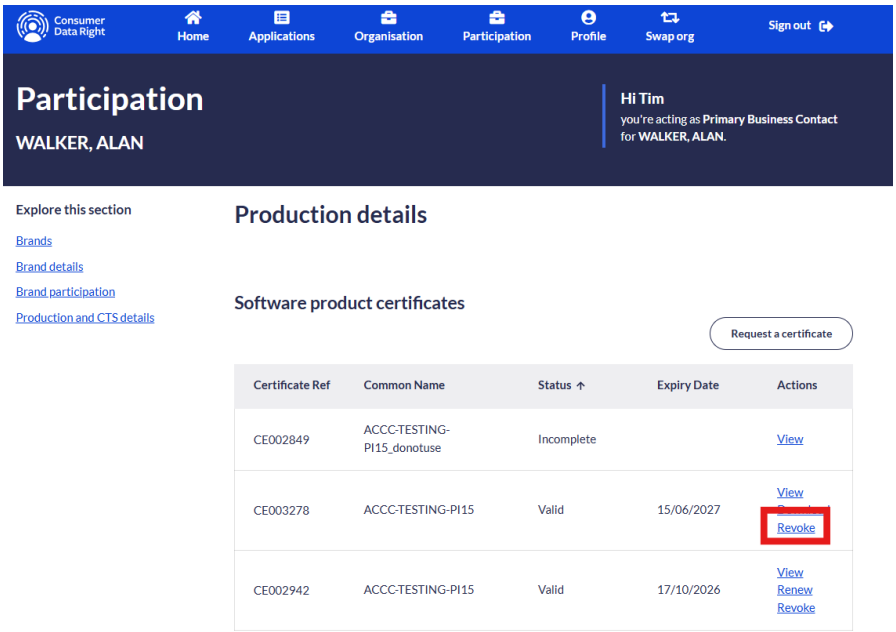
When you renew a client certificate, you will be required to paste your existing CSR, decode it and apply it to the renewal request.



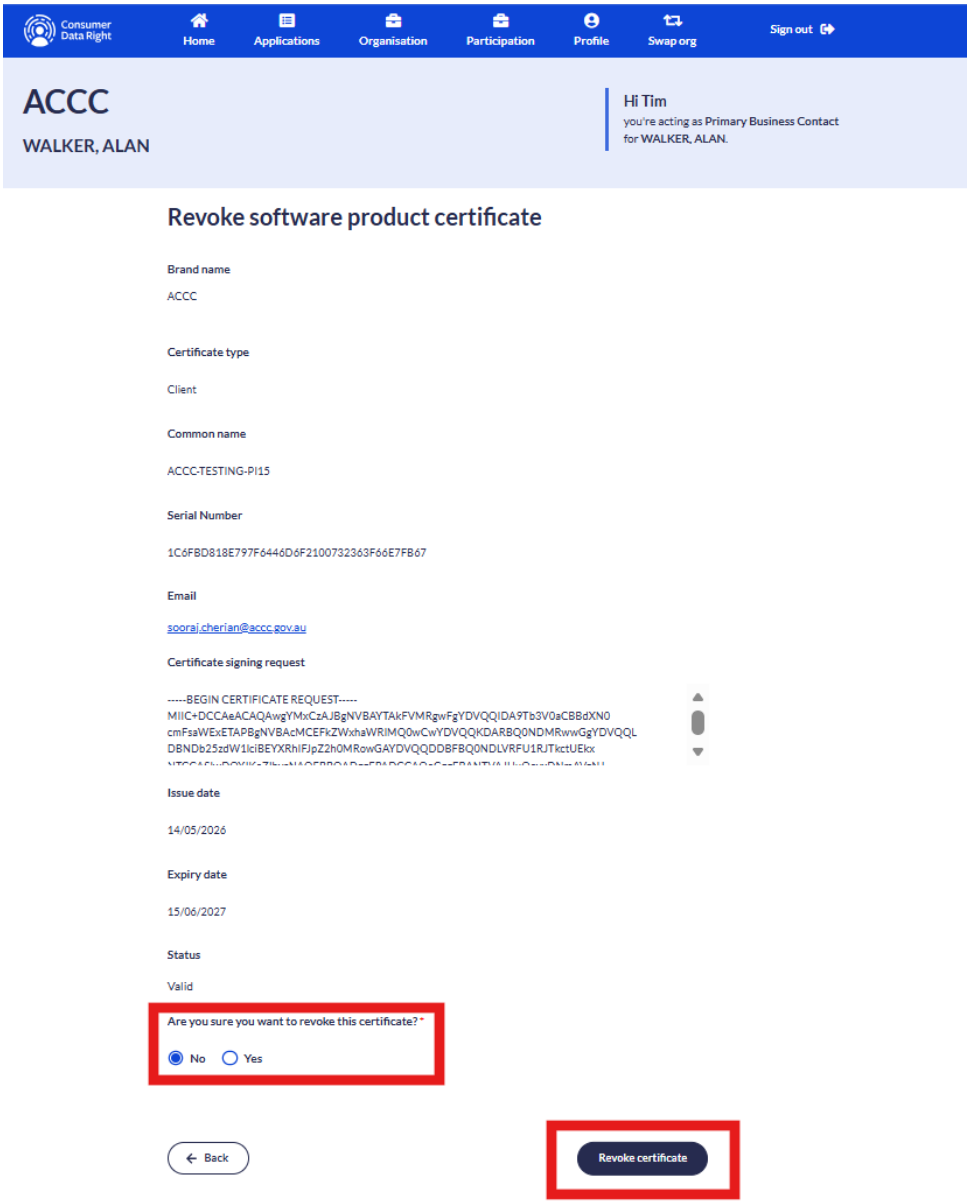
Please add/ensure the contact email is correct, check the acknowledgement box and click Renew Certificate.

10.7.3 Client certificate - Revoke a certificate

Any valid certificate provides a link from which it can be revoked.



The system will present a summary page giving the details of that certificate and prompt you to confirm that you are sure - if so, click to revoke the certificate.

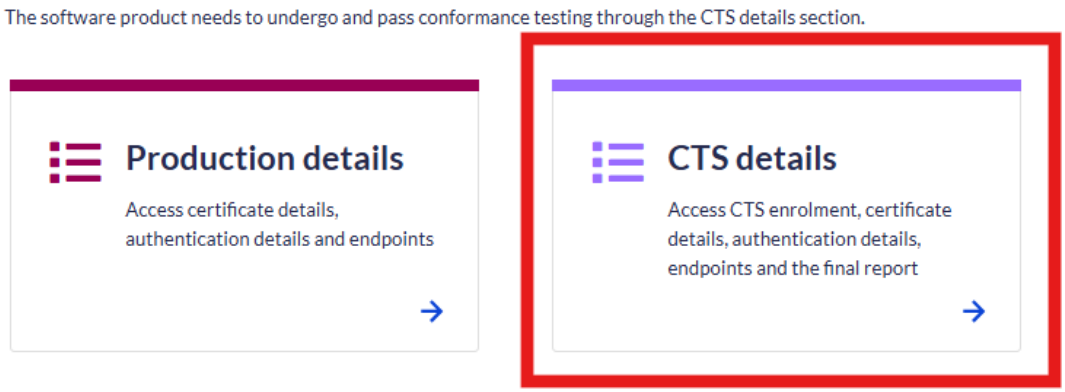


10.8 CTS Certificates

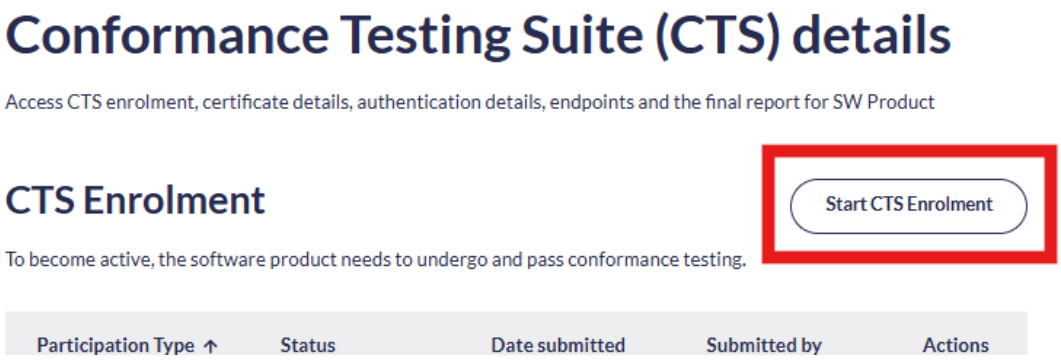
Further details on requesting and managing the CTS Certificate can be found on the Maintain CTS certificates page in this User Guide.

10.8.1 Request a CTS certificate

Data holder and data recipients can request a brand or software product CTS certificate via the Participant Portal once a data holder brand or data recipient software products is added.

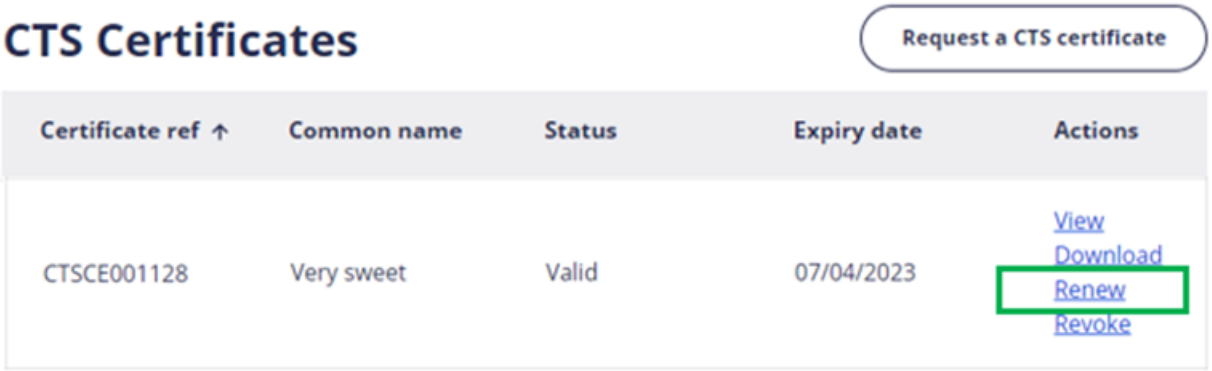


Simply select the button outlined in the image below to request a new CTS certificate.



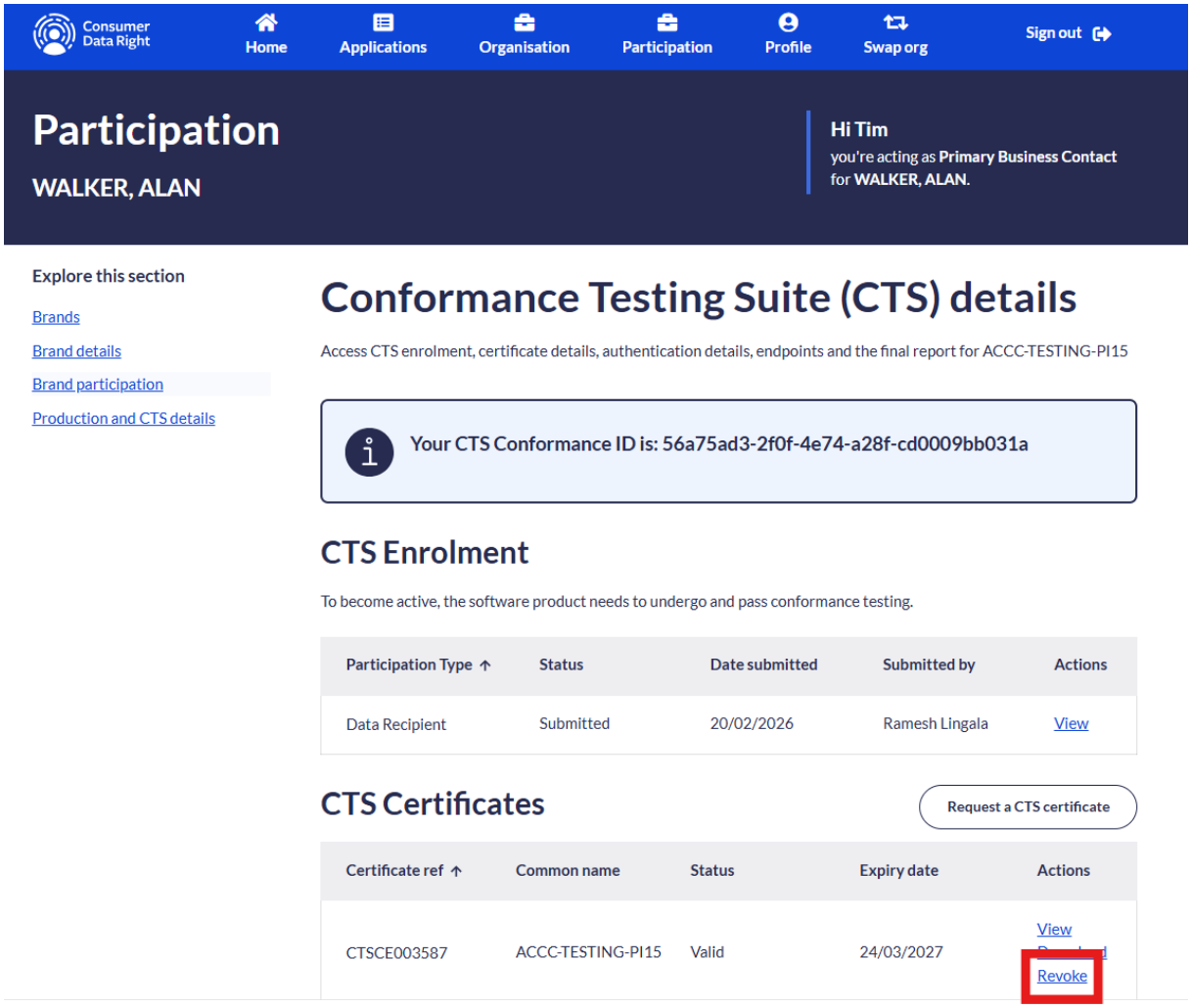
10.8.2 Renew a CTS certificate

Data holder and data recipients can renew an existing CTS certificate using the Participant Portal so that the brand or software product can continue to transfer data securely within the testing ecosystem. This option will become available 7 days before a valid certificate's expiry date. To renew a CTS certificate, select the **Renew** action and confirm the details of the certificate.



10.8.3 Revoke a CTS certificate

Data holders and data recipients can revoke their existing valid CTS certificate. Upon revocation, the system sends revocation data and reflects the change status in near real time to help participants better manage their brands and software products. To revoke a CTS certificate select the **Revoke** action and confirm your selection.



10.8.4 Obtain a valid production certificate

Consequent to the approval of the certificate request, a certificate approval email will be sent to the participant. The approval email will contain the certificate installation next steps and a link to obtain a valid certificate

The participant must click on the link in the email to obtain a valid production certificate. A sample email with masked data is reproduced below

From: noreply@digicert.com
Sent: Wednesday, 27 August 2025 2:26 PM
To: Email ID of Requestor
Subject: **DIGICERT-ONE PREPROD**- Consumer Data Right Certificate approved. Installation next steps.

You don't often get email from noreply@digicert.com. Learn why this is important
CAUTION: This email originated from outside of the organisation. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Action required

Consumer Data Right

DIGICERT-ONE PREPROD- Consumer Data Right Certificate approved. Installation next steps.

**This certificate has been requested for the PREPROD Environment **

Hello,

Your request for a certificate for **Chosen Certificate Name** has been approved. The certificate (including its issuing chain) can be downloaded from link provided below.

https://one.au.digicert.com/mpki/certificate-pickup/0a009d46-f16e-4334-8c27-
REDACTED LINK

Install this certificate on the device where you generated the CSR for this certificate. You may need to install the root CA to use this certificate. For your convenience, the Intermediate root CA is also provided.

Note: You will download the certificate as a .p7b file, which includes the certificates needed to use your device securely. You can choose to download it in either a text format or a binary format. Once it is downloaded, you will also be able to get it from the CDR Participant Portal https://portal.cdr.gov.au.

For installation instructions, refer to the vendor documentation for this device.

If you need help with certificate, contact CDR Technical Operations
CDRTechnicalOperations@accc.gov.au

Thank you,
CDR Technical Operations

Copyright© 2025 DigiCert, Inc. All rights reserved. DigiCert and its logo are registered trademarks of DigiCert, Inc. Other names may be trademarks of their respective owners.

10.8.5 Maintain authentication details

Primary business contacts, primary IT contacts and authorised IT contacts can maintain authentication details (software security token information) on the Participant Portal. For detailed technical information about authentication, please refer to the 'ACCC CDR Register Reference guide' which can be found on the Resources page on the CDR website.

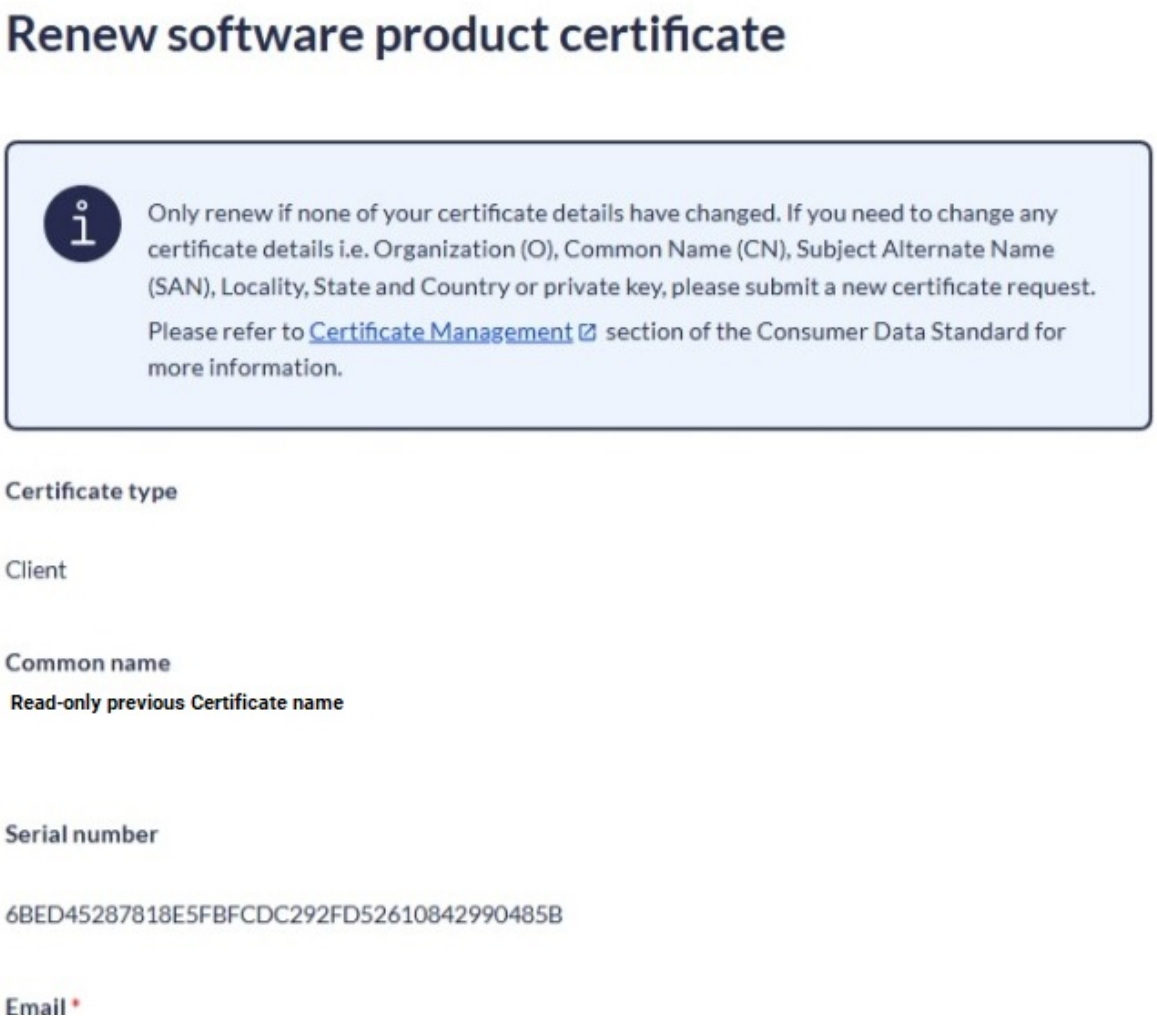
To manage production authentication details for a brand, please follow the instructions below:

1. Log in to the Participant Portal at https://portal.cdr.gov.au and select **Participation** from the top navigation menu.
2. Select the **View** action on the brand that you wish to update.
3. Select the **View** action on the brand participation for the brand that you wish to update.

4. Select the **Production details** tile towards the bottom of the page.
5. To update incomplete authentication details, select the **Edit** action.
6. To add new authentication details, select the **Add** button.

To manage production authentication details for software product, please follow the instructions below:

1. Log in to the Participant Portal at https://portal.cdr.gov.au and select **Participation** from the top navigation menu.
2. Select the **View** action on the brand or the software product that you wish to update.
3. Select the **View** action on the brand participation or the software product that you wish to update.
4. Select the **View** action on the software product that you wish to update.
5. Select the **Production details** tile towards the bottom of the page.
6. To update incomplete authentication details, select the **Edit** action.
7. To add new authentication details, select the **Add** button.



Enter email for certificate delivery.

Read only previous certificate email is shown here

Issue date

01/09/2025

Expiry date

02/10/2025

Status

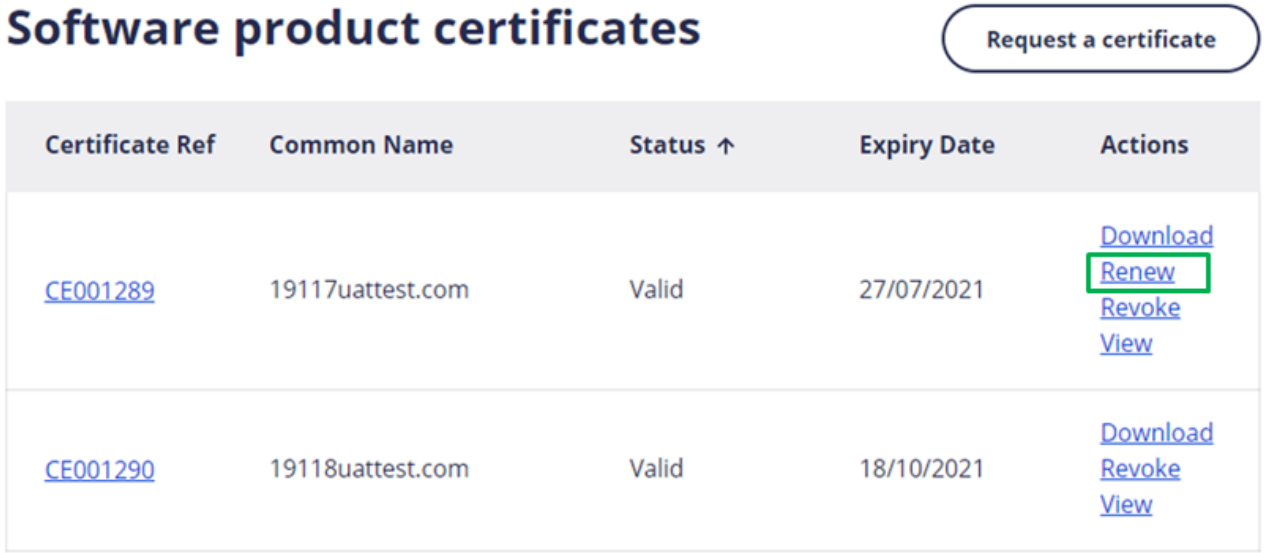
Valid

☑ I have read and agree to the certificate management policies *

If you renew this certificate, a new certificate request will be submitted.

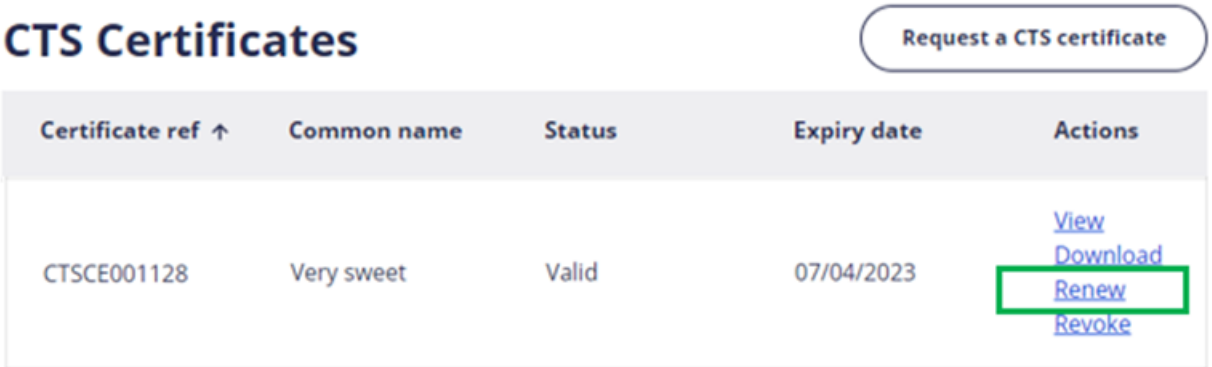
← Back

Renew certificate



10.8.5.1 Renew a CTS certificate

Data holder and data recipients can renew an existing CTS certificate using the Participant Portal so that the brand or software product can continue to transfer data securely within the testing ecosystem. This option will become available 7 days before a valid certificate's expiry date. To renew a CTS certificate, select the **Renew** action and confirm the details of the certificate.



10.8.6 Obtain a valid production certificate

Consequent to the approval of the certificate request, a certificate approval email will be sent to the participant. The approval email will contain the certificate installation next steps and a link to obtain a valid certificate

The participant must click on the link in the email to obtain a valid production certificate. A sample email with masked data is reproduced below

From: noreply@digicert.com
Sent: Wednesday, 27 August 2025 2:26 PM
To: **Email ID of Requestor**
Subject: **DIGICERT-ONE PREPROD**- Consumer Data Right Certificate approved. Installation next steps.

You don't often get email from noreply@digicert.com. Learn why this is important
CAUTION: This email originated from outside of the organisation. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Action required

Consumer Data Right

DIGICERT-ONE PREPROD- Consumer Data Right Certificate approved. Installation next steps.

**This certificate has been requested for the PREPROD Environment **

Hello,

Your request for a certificate for **Chosen Certificate Name** has been approved. The certificate (including its issuing chain) can be downloaded from link provided below.

https://one.au.digicert.com/mpki/certificate-pickup/0a009d46-f16e-4334-8c27-
REDACTED LINK

Install this certificate on the device where you generated the CSR for this certificate. You may need to install the root CA to use this certificate. For your convenience, the Intermediate root CA is also provided.

Note: You will download the certificate as a .p7b file, which includes the certificates needed to use your device securely. You can choose to download it in either a text format or a binary format. Once it is downloaded, you will also be able to get it from the CDR Participant Portal https://portal.cdr.gov.au.

For installation instructions, refer to the vendor documentation for this device.

If you need help with certificate, contact CDR Technical Operations
CDRTechnicalOperations@accc.gov.au

Thank you,
CDR Technical Operations

Copyright© 2025 DigiCert, Inc. All rights reserved. DigiCert and its logo are registered trademarks of DigiCert, Inc. Other names may be trademarks of their respective owners.

10.8.7 Maintain authentication details

Primary business contacts, primary IT contacts and authorised IT contacts can maintain authentication details (software security token information) on the Participant Portal. For detailed technical information about authentication, please refer to the 'ACCC CDR Register Reference guide' which can be found on the Resources page on the CDR website.

To manage production authentication details for a brand, please follow the instructions below:

1. Log in to the Participant Portal at https://portal.cdr.gov.au and select **Participation** from the top navigation menu.
2. Select the **View** action on the brand that you wish to update.
3. Select the **View** action on the brand participation for the brand that you wish to update.

4. Select the **Production details** tile towards the bottom of the page.
5. To update incomplete authentication details, select the **Edit** action.
6. To add new authentication details, select the **Add** button.

To manage production authentication details for software product, please follow the instructions below:

1. Log in to the Participant Portal at https://portal.cdr.gov.au and select **Participation** from the top navigation menu.
2. Select the **View** action on the brand or the software product that you wish to update.
3. Select the **View** action on the brand participation or the software product that you wish to update.
4. Select the **View** action on the software product that you wish to update.
5. Select the **Production details** tile towards the bottom of the page.
6. To update incomplete authentication details, select the **Edit** action.
7. To add new authentication details, select the **Add** button.

11 Maintain Conformance Test Suite (CTS) details

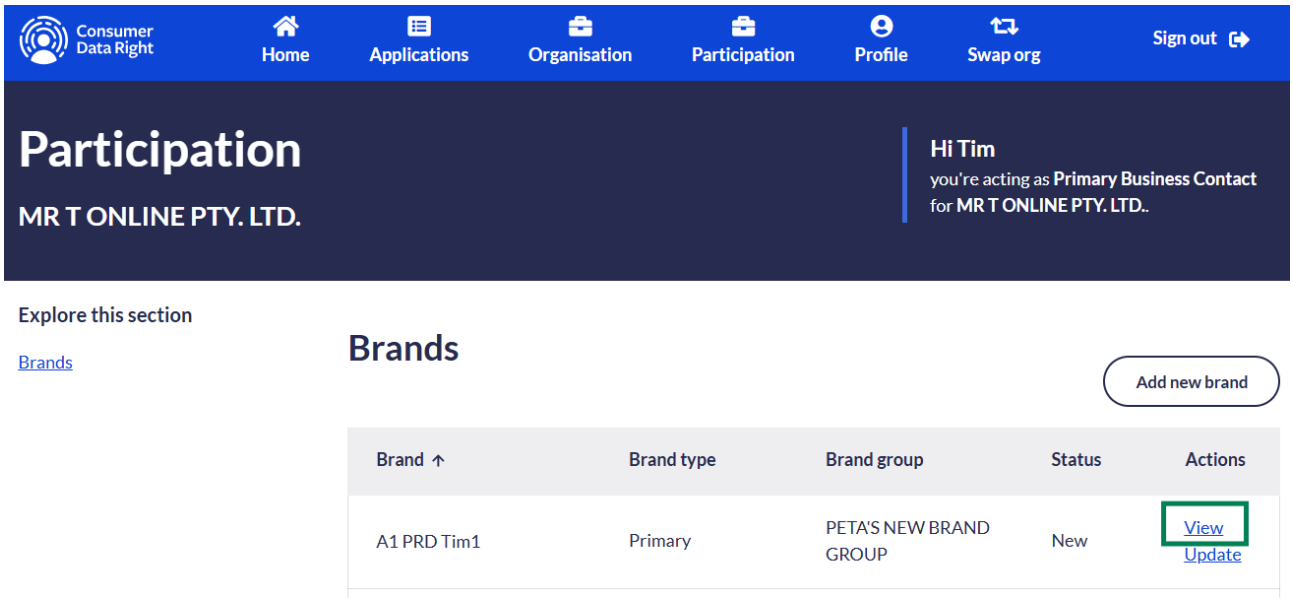
- View CTS details
- Submit CTS Enrolment

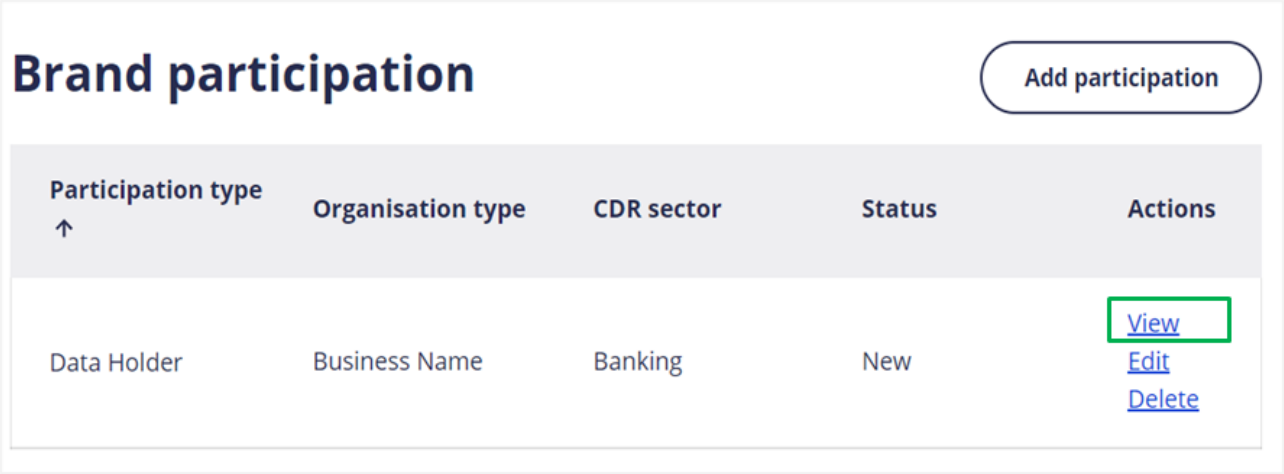
To be able to conduct conformance testing via the CTS, the technical details of your target testing environment must be provided to the ACCC. Authorised users are able to enrol in CTS, submit CTS certificate request, CTS authentication details and CTS endpoints from the Conformance Test Suite (CTS) details page in the Participant Portal.

11.1 View CTS details

To view Conformance Test Suite (CTS) details page:

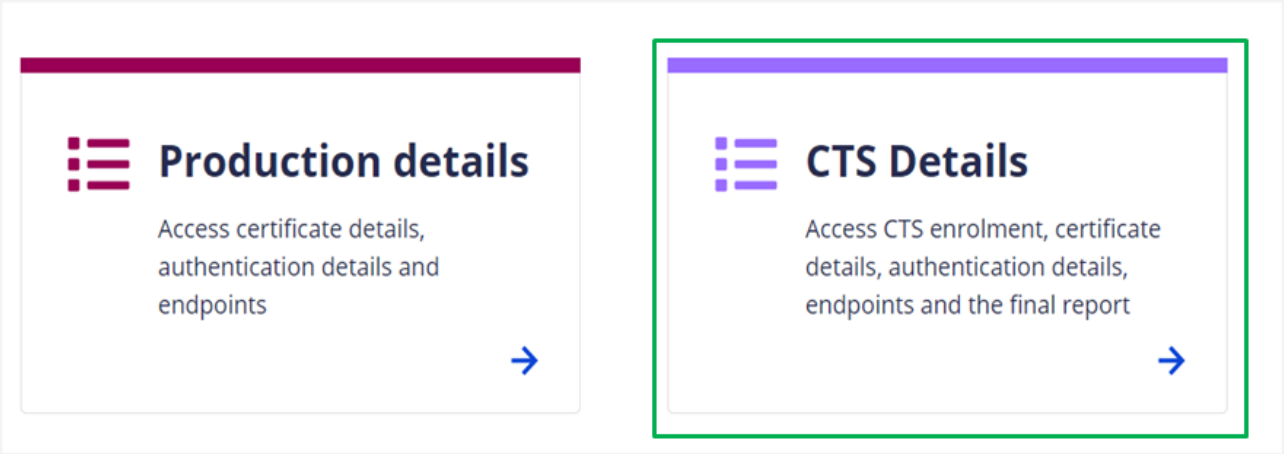
- As a primary business contact, primary IT or an authorised IT contact, log in to the Participant Portal at https://portal.cdr.gov.au and select **Participation** from the top navigation menu.
- Select to **View** an applicable **Brand**. and then select to **View** the relevant **Brand participation**.





Note: For data recipients, you will need to further select a software product.

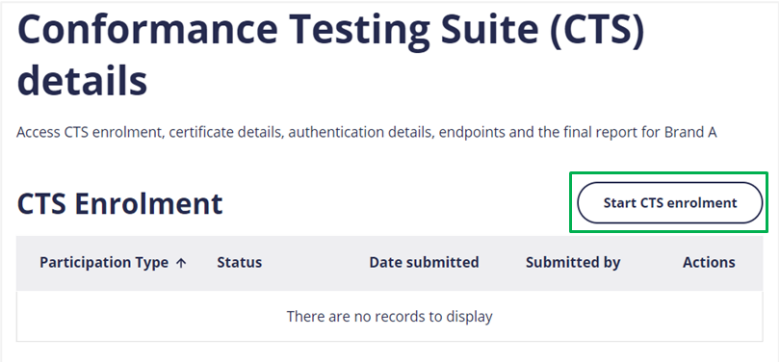
- Select the **CTS Details** tile to access CTS information



11.2 Submit CTS Enrolment

The CTS enrolment form is available to the primary business contact, primary and authorised IT contact and the authorised CTS tester to complete.

- From the **CTS** Details page, select **Start CTS Enrolment**.



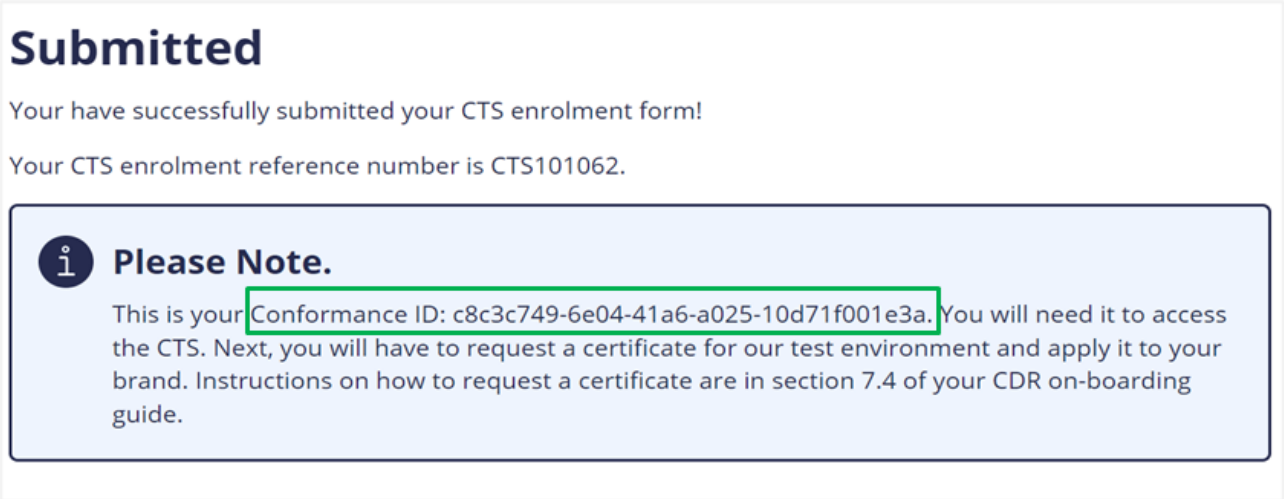
- The **Before you start** page displays information on what to expect and what information is required to complete CTS testing. Please read carefully.
- Select **Start** to commence enrolment.
- In the **Contact details** section, you can create new CTS testers or edit and remove existing CTS tester as required.
- To create a new CTS tester, select **Add new CTS contact** and provide the necessary information.

- Select **Save and continue** to proceed to the next section.
- In the **Test scenarios** section, provide details in relation to your brand or software product, these details determine the relevant test scenarios that will be allocated.

> **Note:** More information can be found by clicking on the hyperlinks provided.

- Complete the details and select **Save and continue**.
  - Data Holders proceed to Step 9 (Ciphers section)
  - Data Recipients proceed to Step 12 (Review section)
- In the **Ciphers** section, indicate which Cipher(s) your brand support and select **Save and continue** to proceed.

- Complete the relevant details relating to your test data preparation and select **Save and continue** to proceed.
- Complete the **Network configuration** details relevant to your brand and select **Save and continue** to proceed.
- The Review tab provides a view of all the details you have populated. You can view the details by clicking on the dropdown. Once you have completed reviewing the details, select **Continue**.
- To submit your CTS enrolment form, you must review and accept the details in the acknowledgment page, and then select **Submit CTS enrolment form**.
- Upon submission, your CTS conformance ID will be displayed on the submission confirmation page. Additionally, you will also receive this confirmation by email.



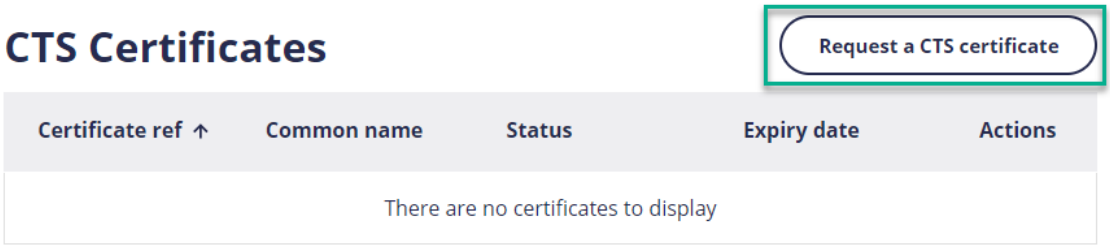
Note: The auto-generated email will contain the details to help you complete CTS next steps, along with your Conformance ID, CTS Guidance Documentation and CTS Connection Datasheet.

11.3 Maintain CTS certificates

Primary business contact, primary IT contact and authorised IT contact of a data holder and data recipient can maintain their CTS certificates on the Participant Portal.

11.3.1 Request a CTS certificate

- Select Request a CTS certificate.



- Proceed to fill in the mandatory fields.

11.3.1.1 Data Holder Server CTS Certificate type default screen

Request a CTS certificate

Required fields are marked with a red asterisk (*) and must be filled in to save.

CTS Certificate type *

Server

CTS DNS name *

CTS Additional DNS names

CTS Certificate signing request *

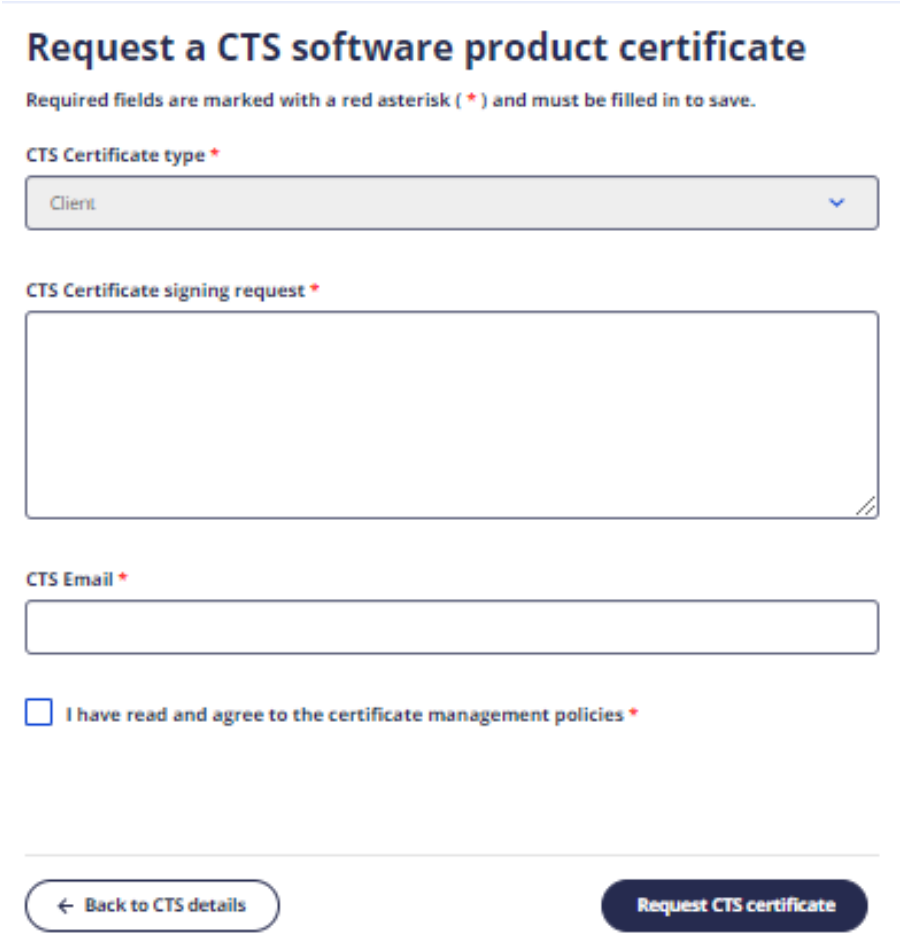
CTS Email *

I have read and agree to the certificate management policies *

Back to CTS details

Request CTS certificate

11.3.1.2 Data Recipient Client CTS Certificate type default screen



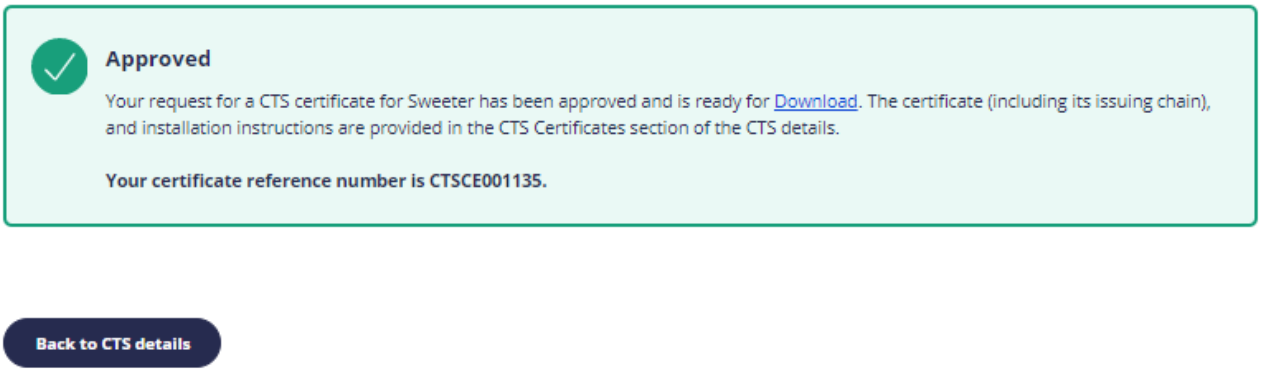
- When the mandatory fields have been completed including the agreement to the certificate management policies checkbox, then the User can request a CTS certificate by clicking the Request CTS certificate button.

11.3.2 Receive CTS certificate

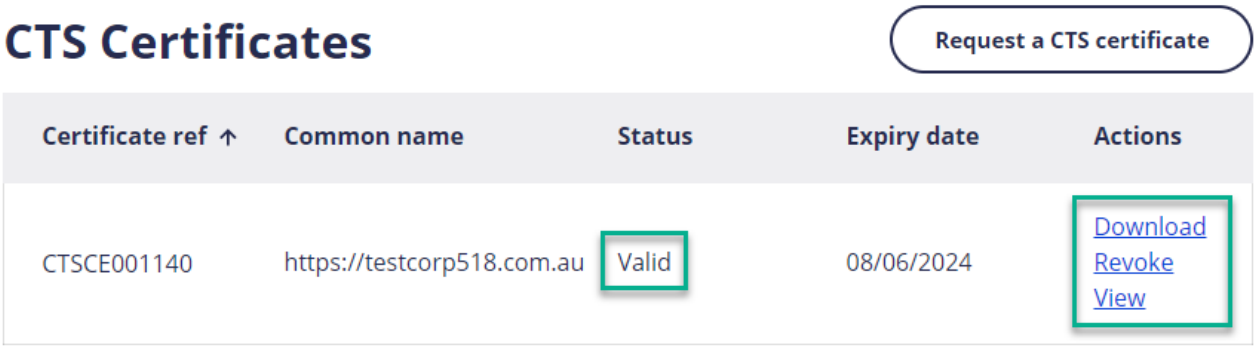
- Data recipients and data holders will receive notifications on the outcome for the CTS certificate request. An email of the outcome will be sent to the participant with either an approval or rejection with next steps for action. The outcome will also be visible in the **'status'** field on the Participant Portal.

11.3.2.1 Successful submission

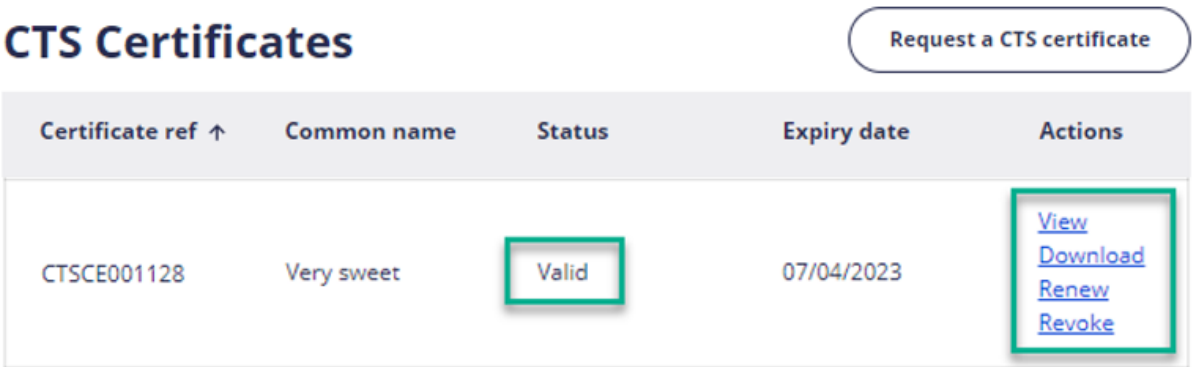
- Upon successful request submission, an approval success page will be displayed with a CTS certificate Download hyperlink and a button to return to an updated CTS Details page.



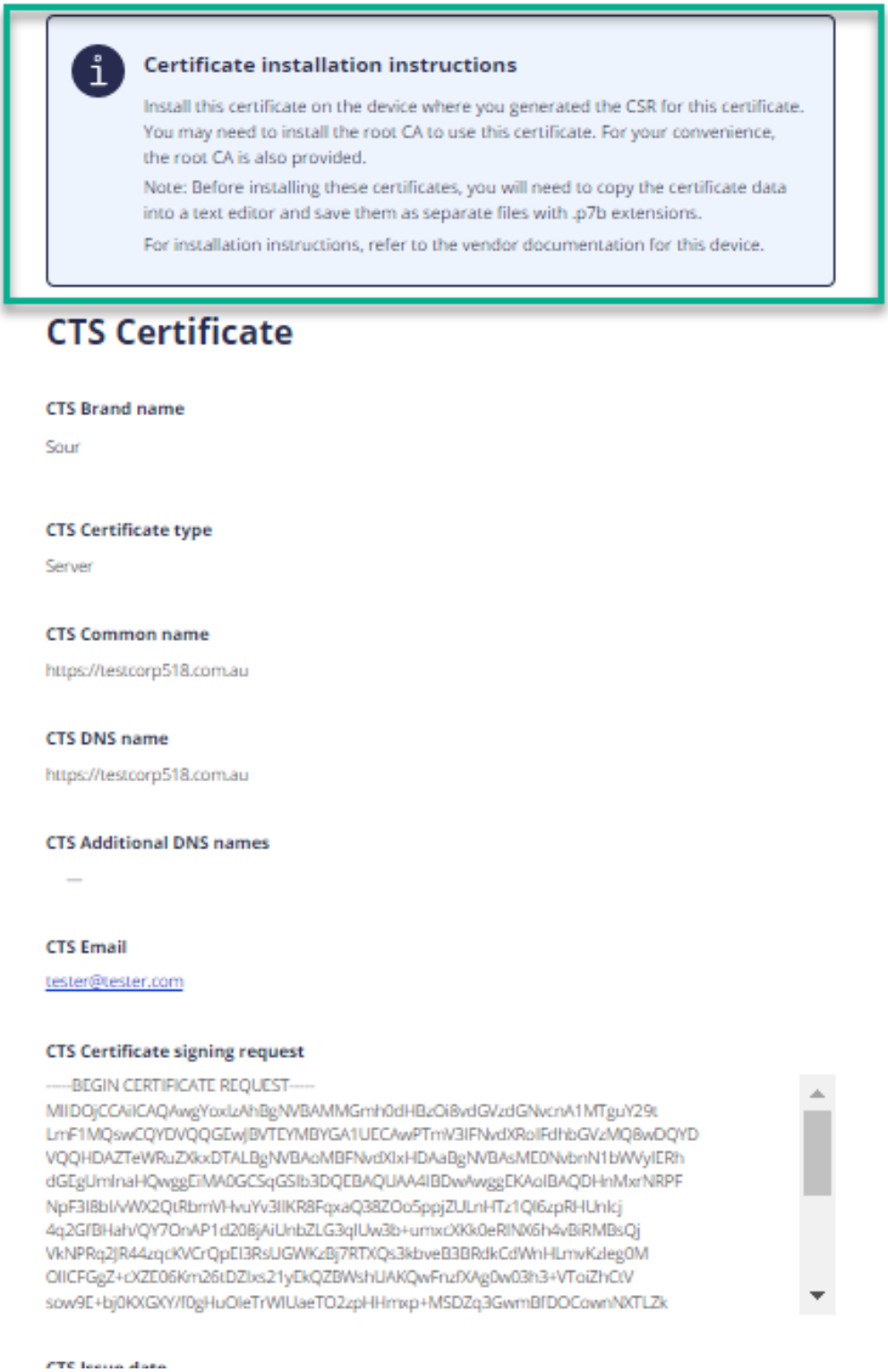
- The CTS Details page is updated to show the certificate status as Vaild and provide actions to view, download, revoke and renew the CTS certificate. The Renew action will only appear when the Valid CTS certificate is approaching its expiry date.

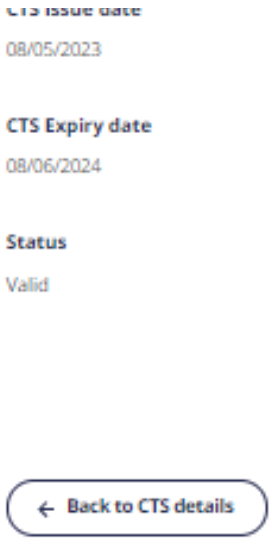


- The Renew action will only appear when the Valid CTS certificate is approaching its expiry date.



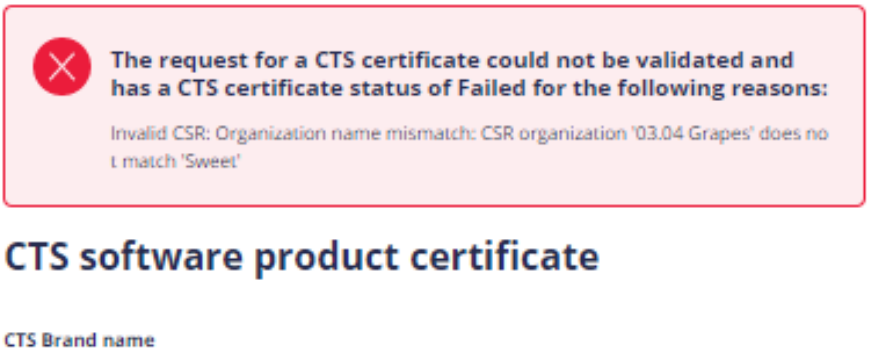
- Data holders and data recipients can View current and historical CTS certificates from the Participant Portal by selecting **View** from the Actions column.
- Viewing the CTS Certificate will provide details of the CTS Certificate and provide certificate installation instructions.



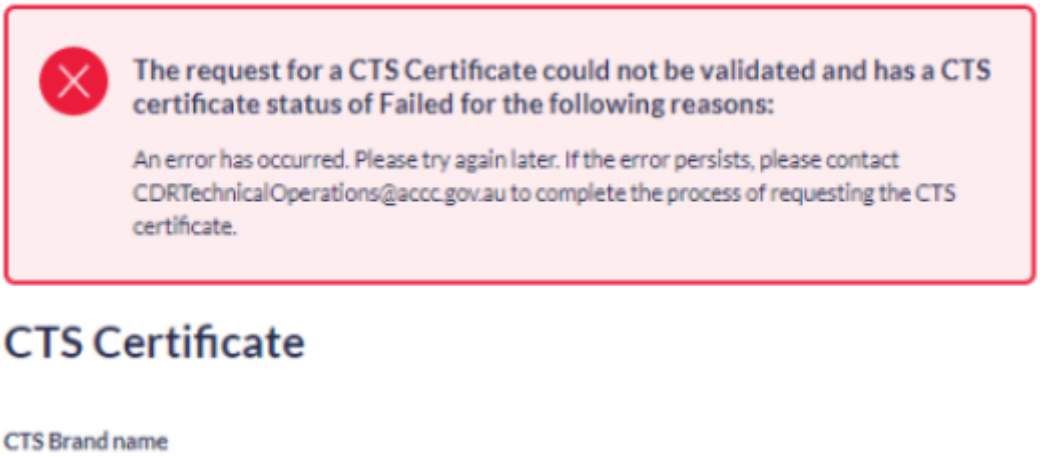


11.3.2.2 Unsuccessful submission

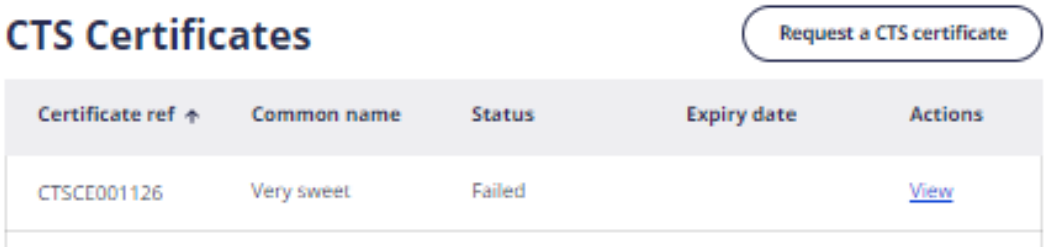
- Upon an unsuccessful request submission, a failed message will be displayed.
- Submissions with incorrect details will include the reason for the failure in the message and will display the CTS certificate request details.



- A communication link failure message will request the user to try again and/or to contact CDR Technical Operations if the error persists.

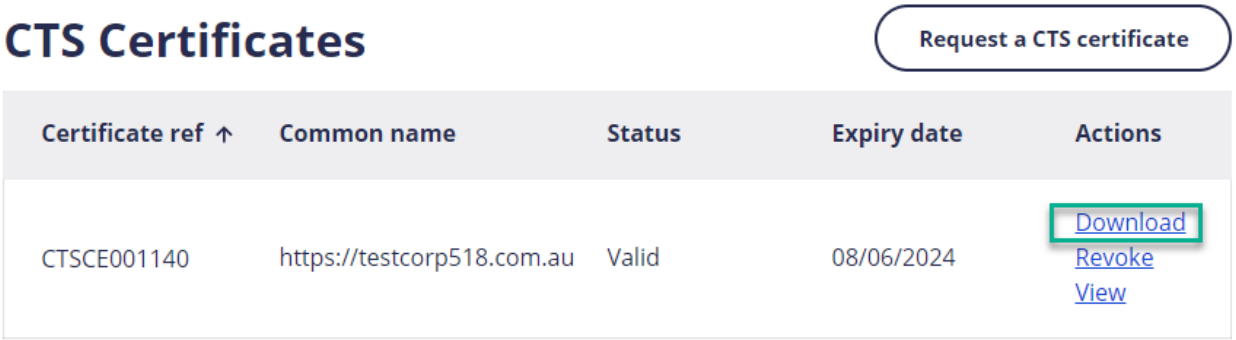


- The status of an unsuccessful request will be Failed and this status will be displayed on the CTS Certificate and on the CTS Certificate details page.



11.3.3 Download CTS certificate

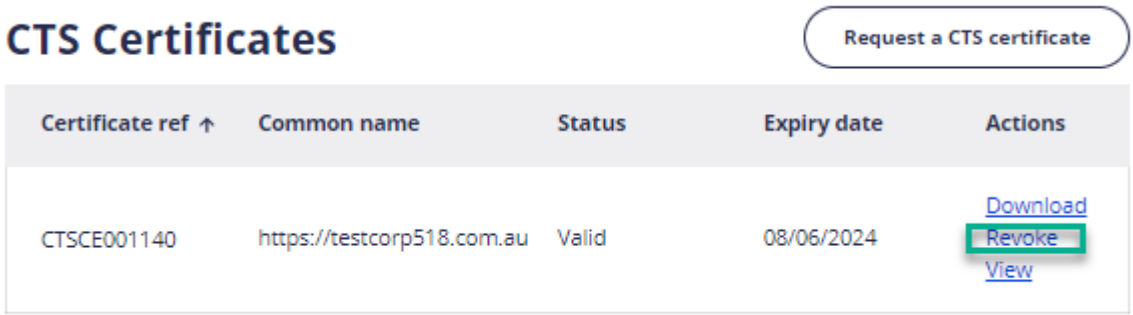
Data holders and data recipients can download current CTS certificates from the Participant Portal by selecting **Download** in the CTS Certificate Actions column.



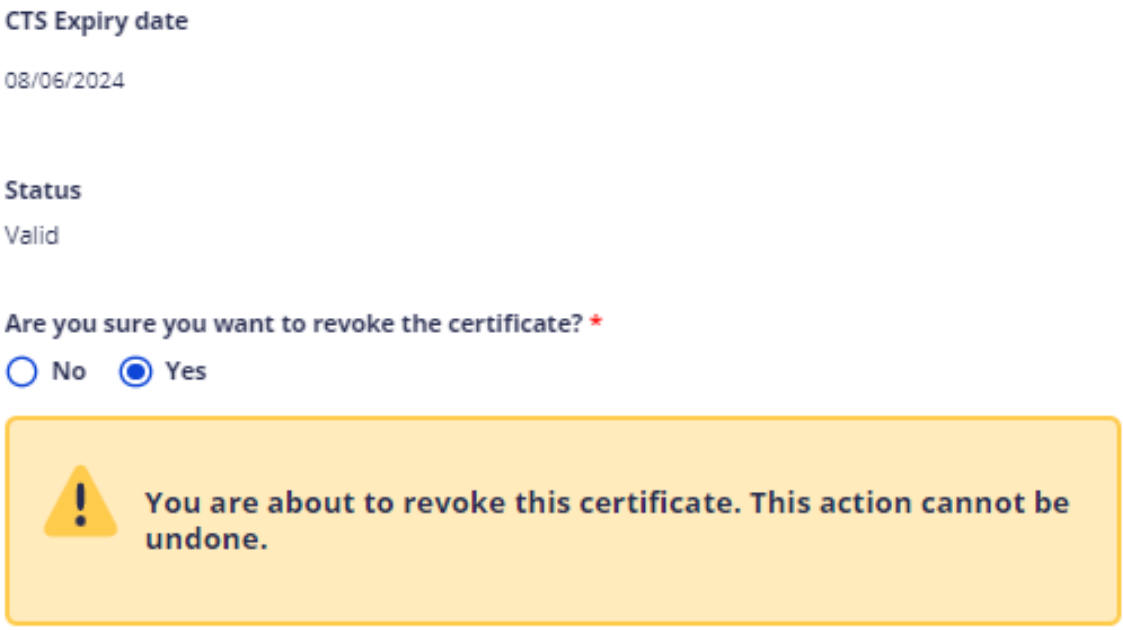
11.3.4 Revoke a CTS certificate

Primary business contact, primary IT contact, and authorised IT contact of a data holder and data recipient can revoke an existing valid CTS certificate by following the below steps:

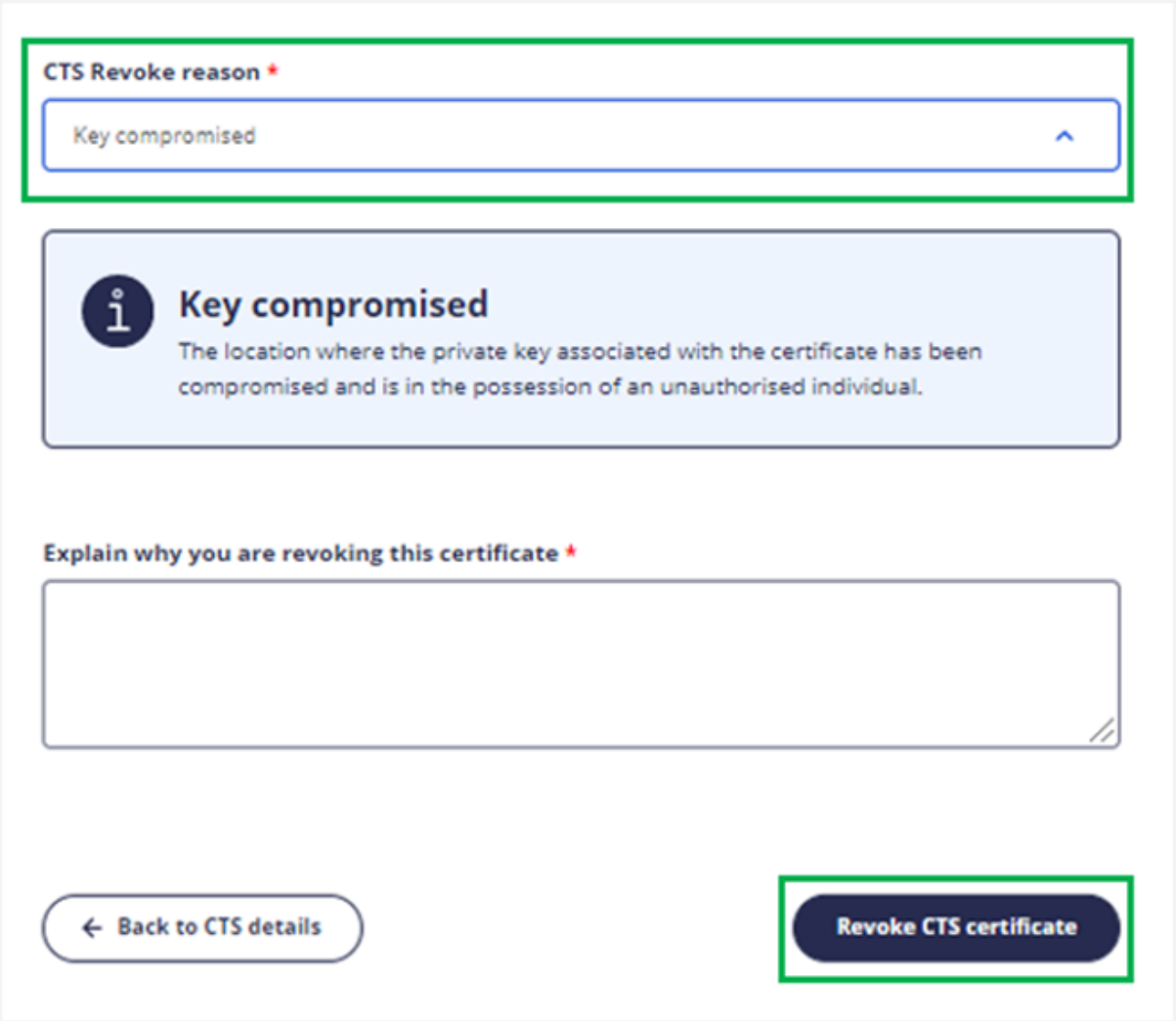
- Select the **Revoke** action against a valid CTS certificate.



- In the 'Are you sure you want to revoke the certificate' field, select the **Yes** radio button.
- When the Yes radio button is selected an information warning will be displayed.



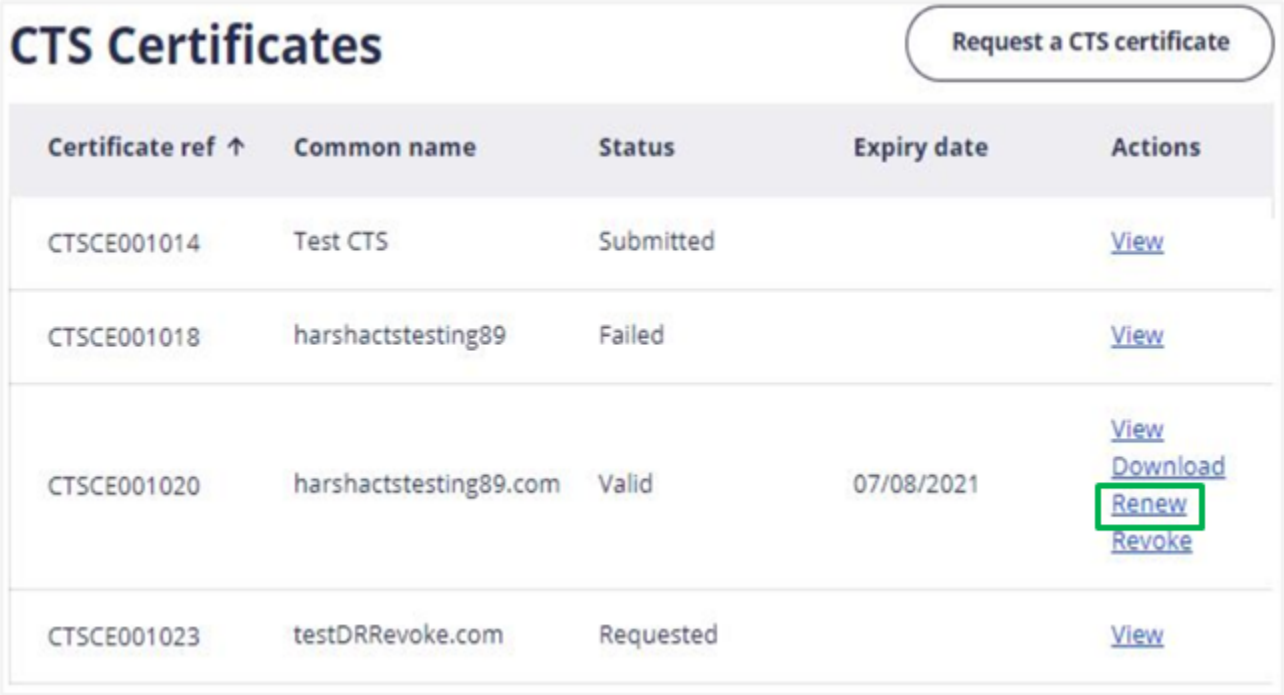
- Select an appropriate revoke reason from the **CTS Revoke Reason** drop-down list and click the **Revoke CTS certificate** button to submit the form.



11.3.5 Renew a CTS certificate

Primary business contact, primary IT contact, and authorised IT contact of a data holder and data recipient can renew an existing CTS certificate within 30 days of its expiry by:

- Select the **Renew** action against a valid CTS certificate.



CTS Certificates

Request a CTS certificate

Certificate ref ↑	Common name	Status	Expiry date	Actions
CTSCE001014	Test CTS	Submitted		View
CTSCE001018	harshactstesting89	Failed		View
CTSCE001020	harshactstesting89.com	Valid	07/08/2021	View Download Renew Revoke
CTSCE001023	testDRRevoke.com	Requested		View

- Complete the certificate renewal form and select **Renew CTS certificate** to submit the form.

Renew CTS software product certificate

CTS Certificate type

Client

CTS Common name

Very sweet

CTS Email *

tester@tester.com

CTS Certificate signing request

-----BEGIN CERTIFICATE REQUEST-----
MIIDAzCCAesCAQAwezETMBEGA1UEAwwKVmVyeSBzd2VldDELMAkGA1UEBhMCQVUx
GDAWBgNVBAgMD05ldyBTb3V0aCBXYWxlczEPMA0GA1UEBwwGU3lkbmV5MQ4wDAYD
VQQKDAVTd2VldDEcMBoGA1UECwwTQ29uc3VtZXlgRGF0YSBSaWdodDCCASIwDQYJ

CTS Issue date

04/04/2023

CTS Expiry date

07/04/2023

Status

Valid

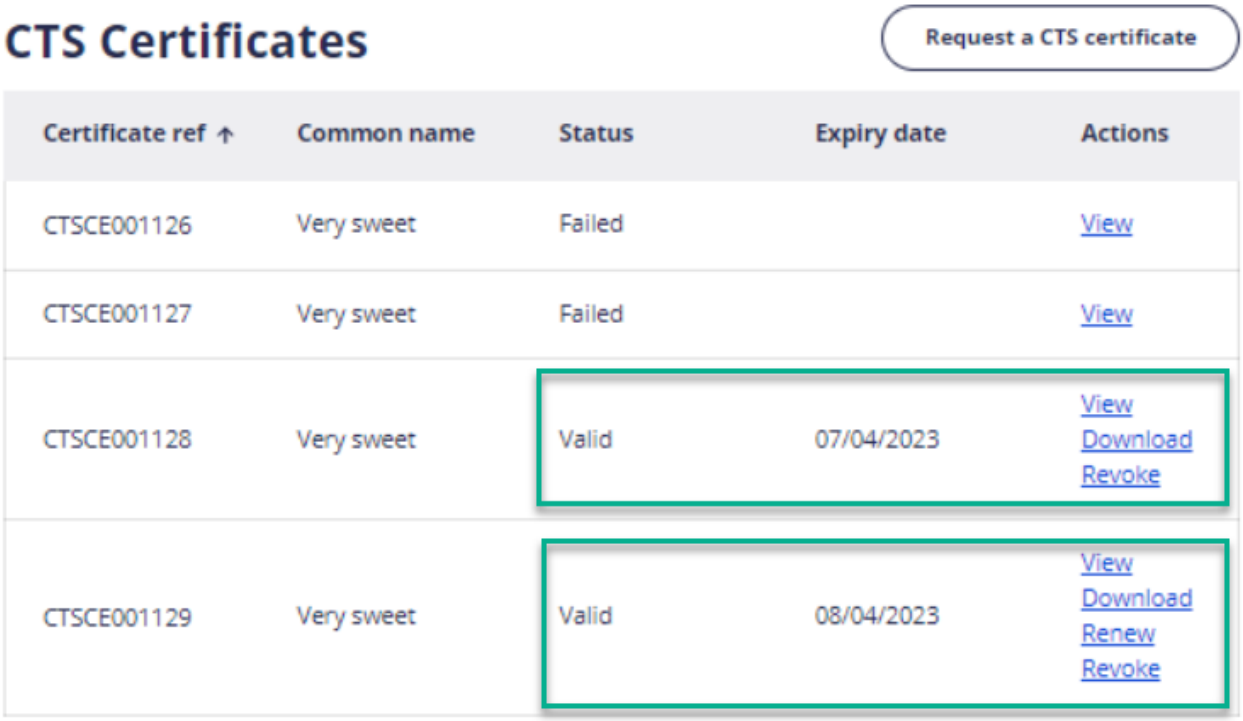
☐ **I have read and agree to the certificate management policies** *

← **Back to CTS details** **Renew CTS certificate**

> **Note:** When the certificate expiry date has lapsed, the renewal button will no longer be available. You will need to request a new certificate using the “Request a certificate” process.

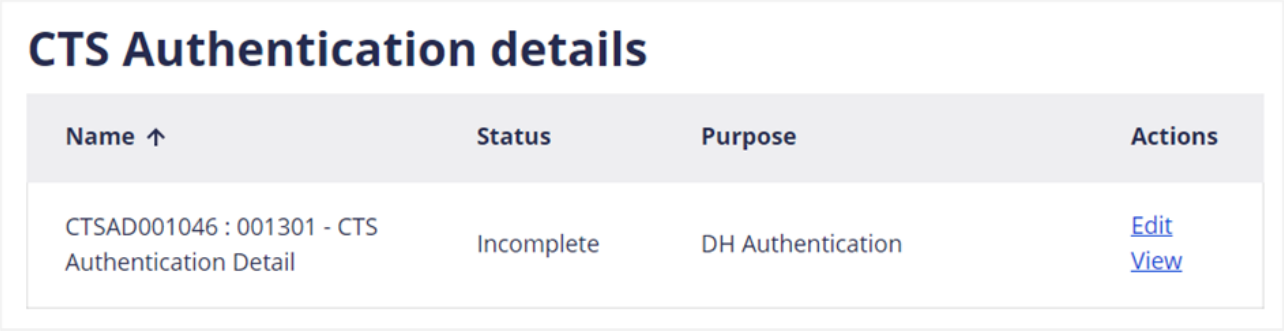
- When the agreement checkbox is selected an information warning will be displayed.

- You will be notified via email of the outcome of the renewal request and the CTS certificate details page will display both the current Valid certificate and the newly renewed certificate.



11.4 Maintain CTS authentication details

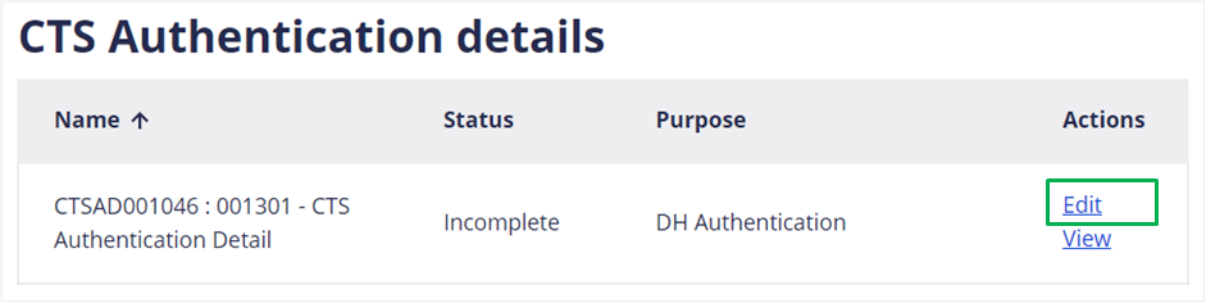
When the CTS enrolment form has been submitted, the Participant Portal automatically creates a blank CTS Authentication details entry, as shown below:



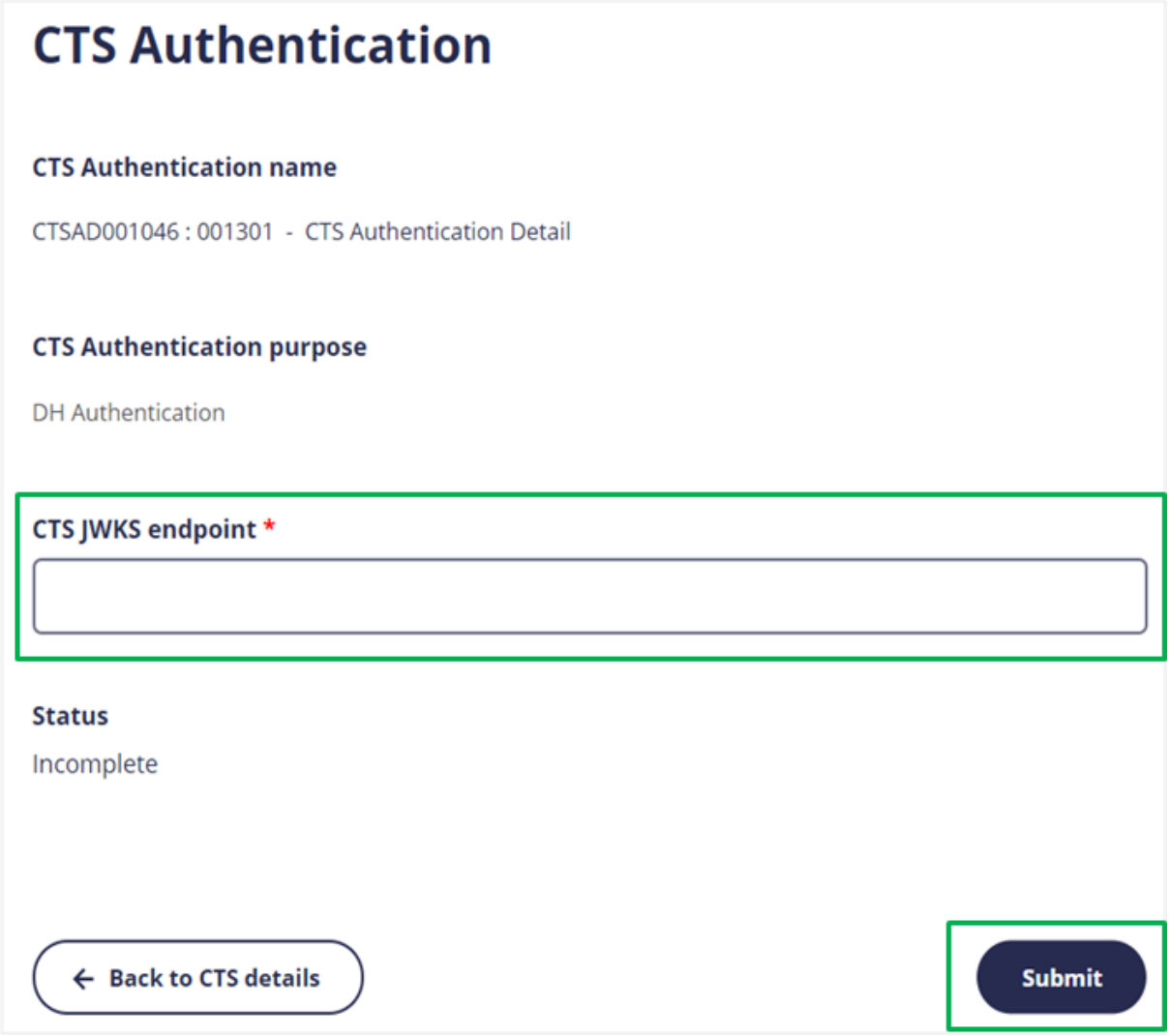
Primary business contact, primary or authorised IT contact and authorised CTS tester can edit or view CTS authentication details in the **CTS details** page.

11.4.1 Submit CTS authentication details

1. Select the **Edit** action.



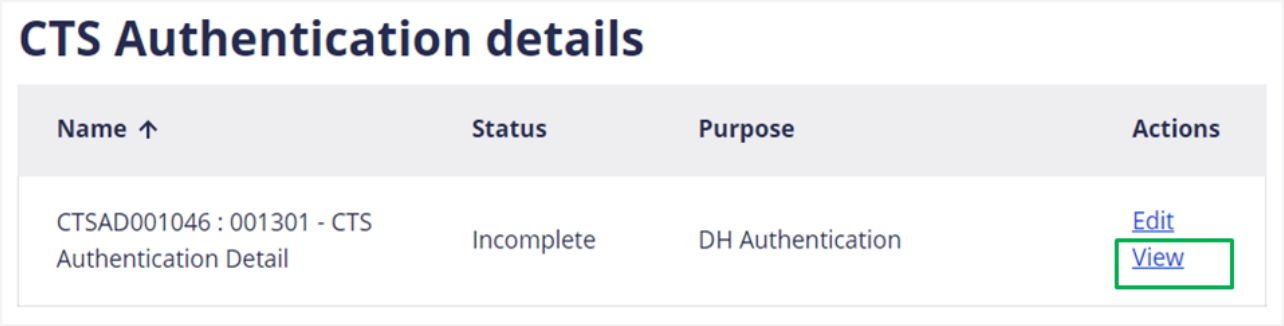
2. Enter **CTS JWKS endpoint** and select **Submit** to finish the process.



Note: Upon submission, the record is made active and you will not be able to edit this entry. If you need to edit CTS authentication details, please contact the ACCC via the CDR Service Management portal or the CDR Technical Operations mailbox CDRtechnicaloperations@accc.gov.au.

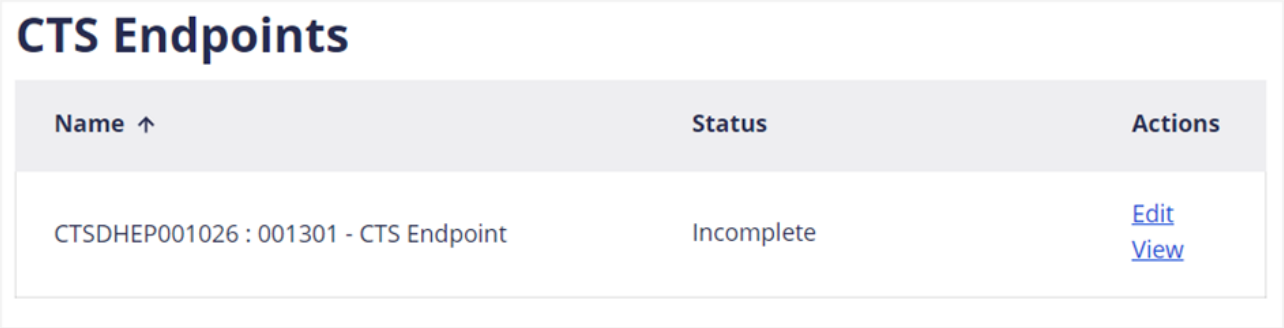
11.4.2 View CTS authentication details

To view CTS authentication details, select the **View** action as shown below.



11.5 Maintain CTS endpoints

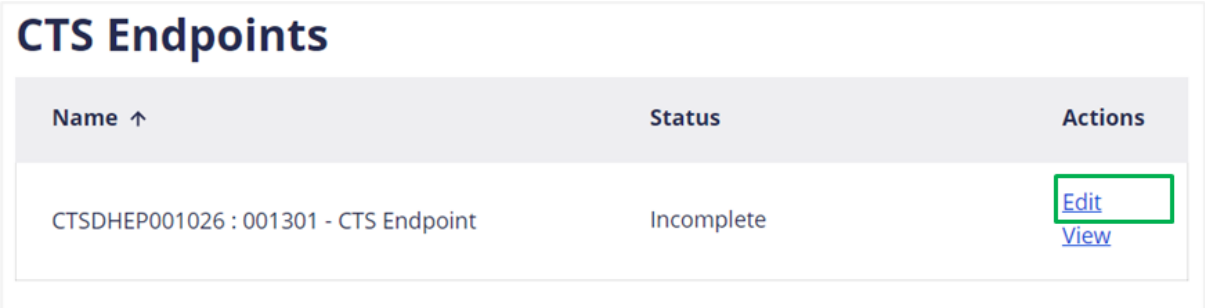
When the CTS enrolment form has been submitted, the Participant Portal automatically creates a blank CTS Authentication details entry.



Primary business contact, primary or authorised IT contact and authorised CTS tester can edit or view CTS endpoints details in the **CTS details** page.

11.5.1 Submit CTS endpoints

1. To submit CTS endpoint, select the **Edit** action.



2. Fill in mandatory details as required and select **Submit**.

Note: Upon submission, the record is made active and you will not be able to edit this entry. If you need to edit CTS endpoint details, please contact the ACCC via the CDR Service Management portal or the CDR Technical Operations mailbox CDRtechnicaloperations@accc.gov.au.

12 Rule 9.4 reporting

Rule 9.4 reports can be completed and lodged on the Participant Portal so that accredited data recipients and data holders can meet their reporting obligations under rule 9.4 of the *Competition and Consumer (Consumer Data Right) Rules 2020 (Cth)*.

The reporting process on the Participant Portal allows participants to:

- Edit, save and submit a report at any time before the due date.
- View and download a submitted report.
- Receive email reminder about upcoming due date.

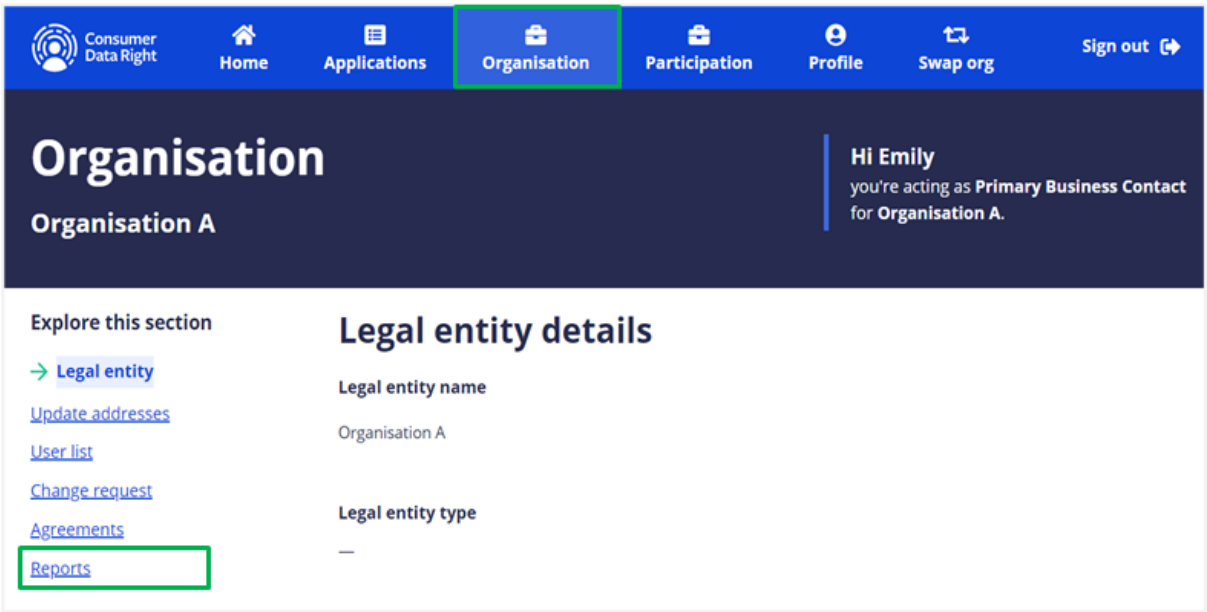
> **Note:** By lodging the report via the Participant Portal, CDR participants will satisfy the requirement of submitting their reports to both the ACCC and the Office of Australian Information Commissioner.

12.1 Lodging a rule 9.4 report on the Participant Portal

As a data holder and/or an accredited data recipient, you can start, edit and submit a rule 9.4 report on the Participant Portal by following the below steps:

12.1.1 Start and submit a rule 9.4 report

1. As a primary business contact, authorised business contact, primary IT contact or an authorised IT contact, log in to the Participant Portal at https://portal.cdr.gov.au and select **Organisation** from the top navigation menu, then **Reports** from the left side navigation pane.



2. Based on your participation (data holder, accredited data recipient, CDR principal), you will be presented with a summary view of your rule 9.4 reporting obligation for the current reporting period.

Reporting overview

Accredited data recipient reports

View all accredited data recipient reports

Reporting year	Reporting period ↑	Status	Due date	Date submitted	Submitted by	Actions
2022	1 July - 31 December	Not Started	30/01/2023			Start Download

1 - *Example view for accredited data recipient*

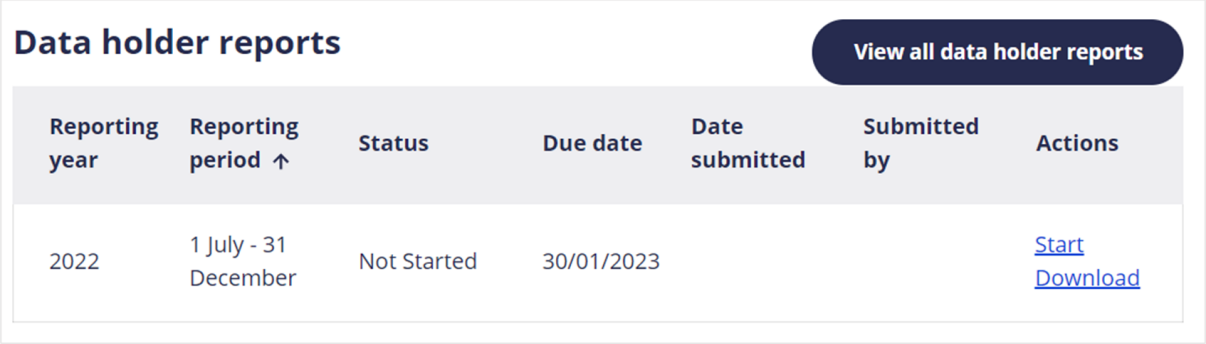
CDR principal reports

View all CDR principal reports

Enter text to search...

CDR Representative ↑	Reporting year	Reporting period	Status	Due date ↑	Date submitted	Submitted by	Actions
Company A	2022	1 July - 31 December	Not Started	30/01/2023			Start Download
Company B	2022	1 July - 31 December	Not Started	30/01/2023			Start Download
Company D	2022	1 July - 31 December	Not Started	30/01/2023			Start Download

2 - *Example view for accredited data recipient that is also a CDR principal*



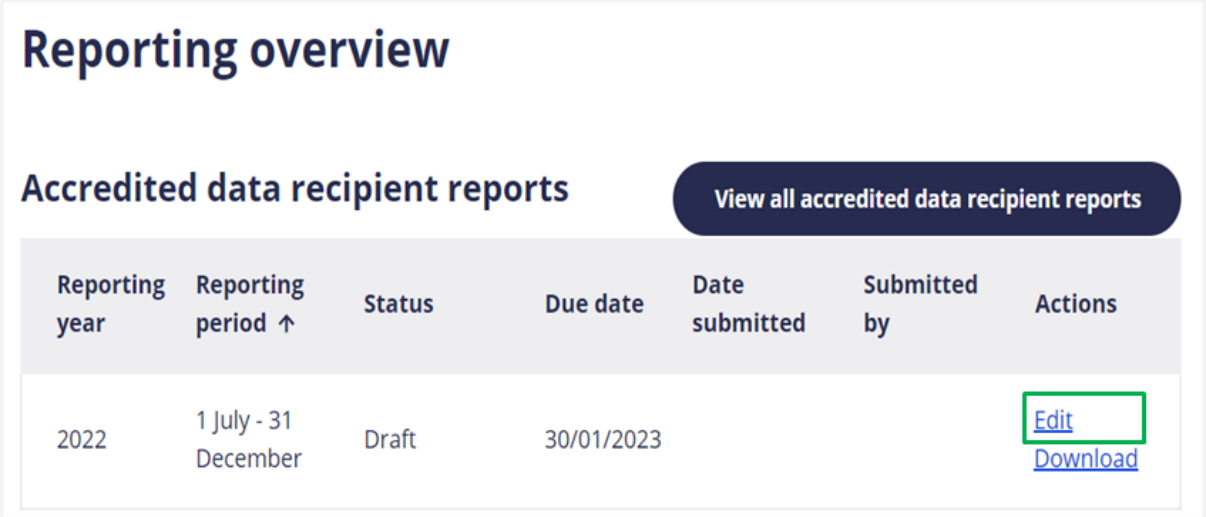
3 - *Example view for data holder*

3. Select **Start** from the Actions column.
4. Complete all mandatory questions and select **Submit**.
5. Upon submission, a confirmation will be shown.

12.1.2 Edit a rule 9.4 report

A primary business contact, authorised business contact, primary IT contact or an authorised IT contact can edit a draft report any time before the reporting cut-off date.

1. Log in to the Participant Portal at https://portal.cdr.gov.au and select **Organisation** from the top navigation menu, then **Reports** from the left side navigation pane.
2. Select **Edit** from the Actions column.



3. Proceed to edit and submit the report.
4. Upon submission, a confirmation will be shown.

12.1.3 Download a rule 9.4 report

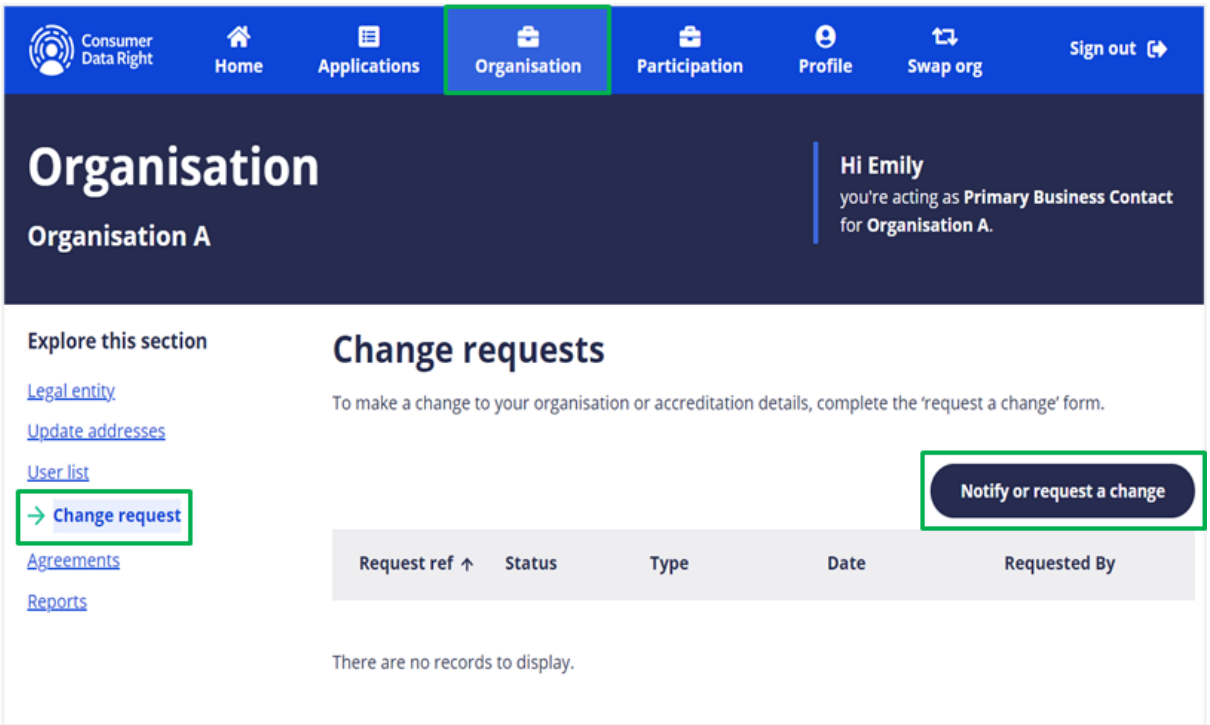
You can download a PDF copy of the report at any time by selecting **Download** from the Actions column and follow the prompts.

12.2 Amend a submitted report

A primary business contact can raise a change request to amend a submitted report before the due date.

To raise a change request:

1. Log in to the Participant Portal at https://portal.cdr.gov.au and select **Organisation** from the top navigation menu.
2. Select **Change request** from the left side navigation pane and select **Notify or request a change.**



3. Under the **Change type**, select **Amend a rule 9.4 report** option.
4. You can search for a submitted report by launching the lookup modal. Select a report that needs to be amended and then click **Select** to confirm.

5. Complete the rest of the form and select **Submit request** to complete the process.
6. When the change request is approved, you will be notified by email, and the relevant report will be set to the **Draft** status to allow editing.

13 Schedule 1 reporting

Schedule 1 reports can be completed and lodged on the Participant Portal so that accredited data recipients can report annually to the ACCC, as the Accreditor, on their ongoing compliance with the information security obligations in Schedule 2 to the CDR Rules. The requirements relating to this reporting are contained in Schedule 1 to the CDR Rules. Schedule 1 requires accredited persons to provide either an 'attestation statement' or an 'assurance report' each year starting with the provision of an attestation statement.

The reporting process on the Participant Portal allows participants to:

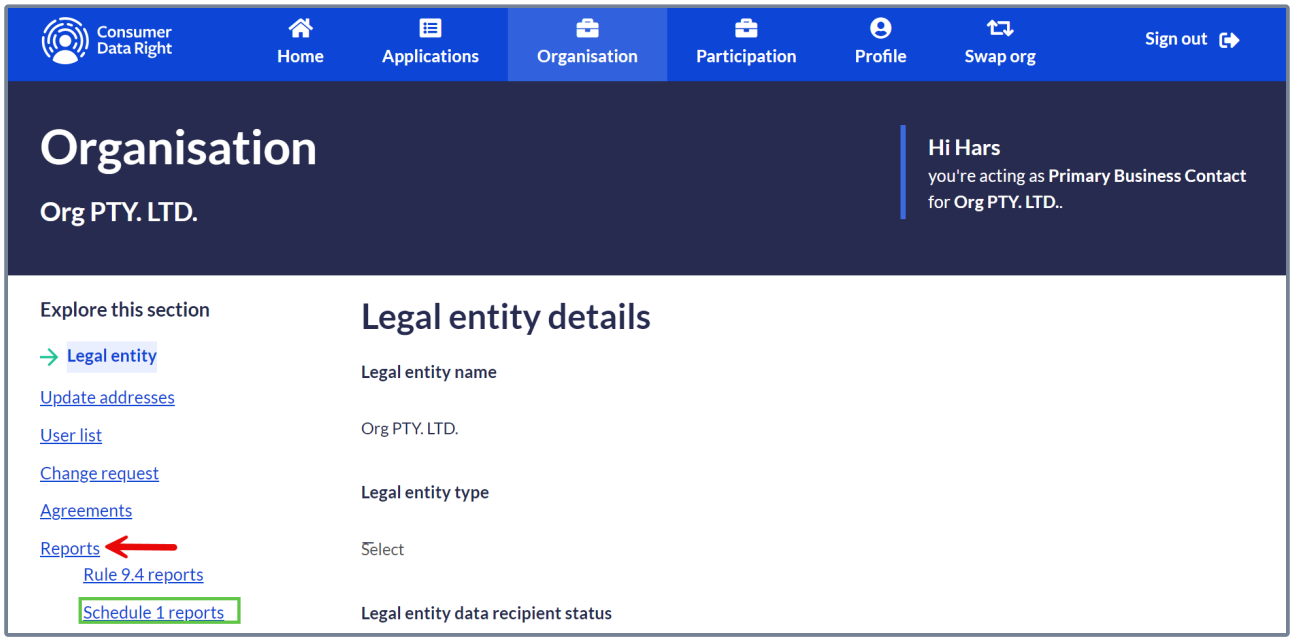
- Start, edit, and submit a report any time that are due;
- View and download a report in any status;
- Receive email reminder about upcoming due date and overdue reports.

13.1 Lodging a Schedule 1 report on the Participant Portal

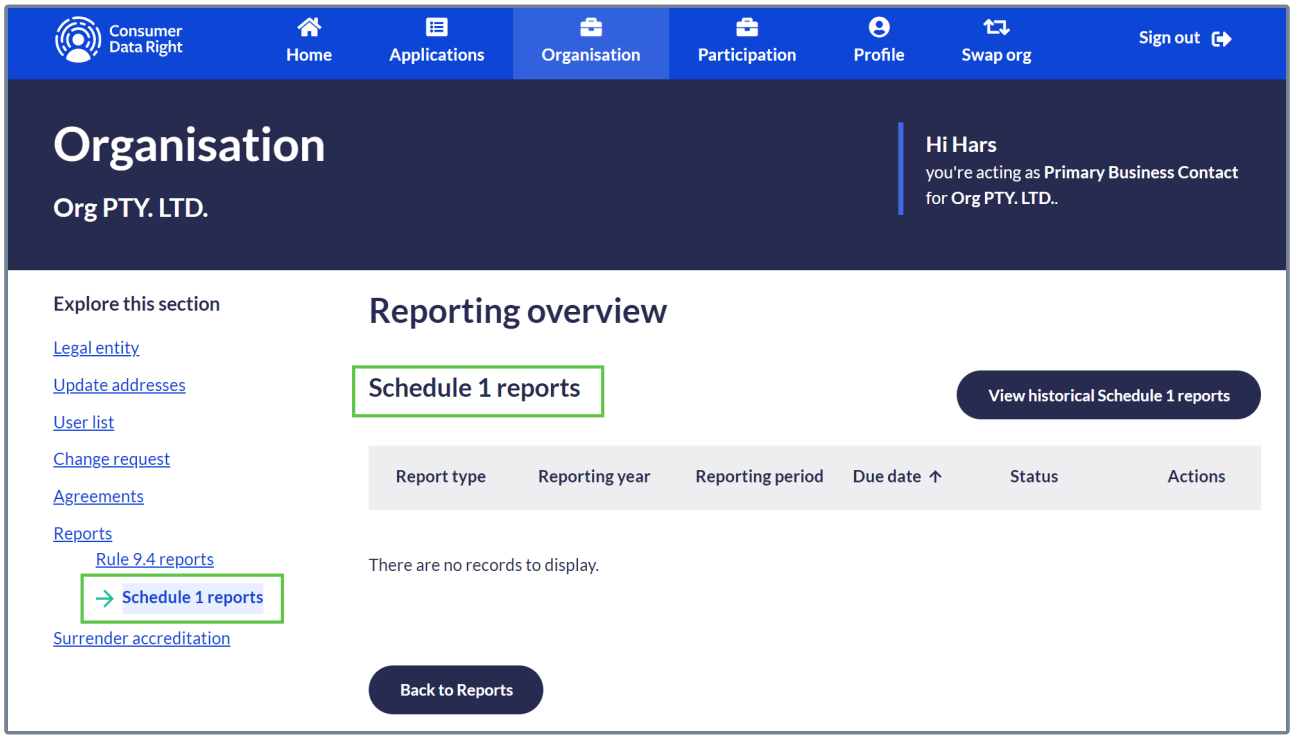
As an accredited data recipient, you can start, edit and submit a Schedule 1 Attestation statement and Assurance report based on your reporting year on the Participant Portal by following the below steps:

13.1.1 Start and submit a Schedule 1 report

1. As a primary business contact, authorised business contact, primary IT contact or an authorised IT contact, log in to the Participant Portal at https://portal.cdr.gov.au and select **Organisation** from the top navigation menu, then **Reports>Schedule 1 reports** from the left side navigation pane.



2. Based on your participation (accredited data recipient who has not gone through streamline application process), you will be presented with a summary view of your Schedule 1 reporting obligation for the current reporting period and next 2 years that are not submitted.



3. Select **Start** from the Actions column. Start action is available 3 months before the due date.
4. Complete all mandatory fields, upload one or more files and select **Submit**.
5. Upon submission, a confirmation message will be shown and record will move to historical page.

13.1.2 View a submitted Schedule 1 Historical report

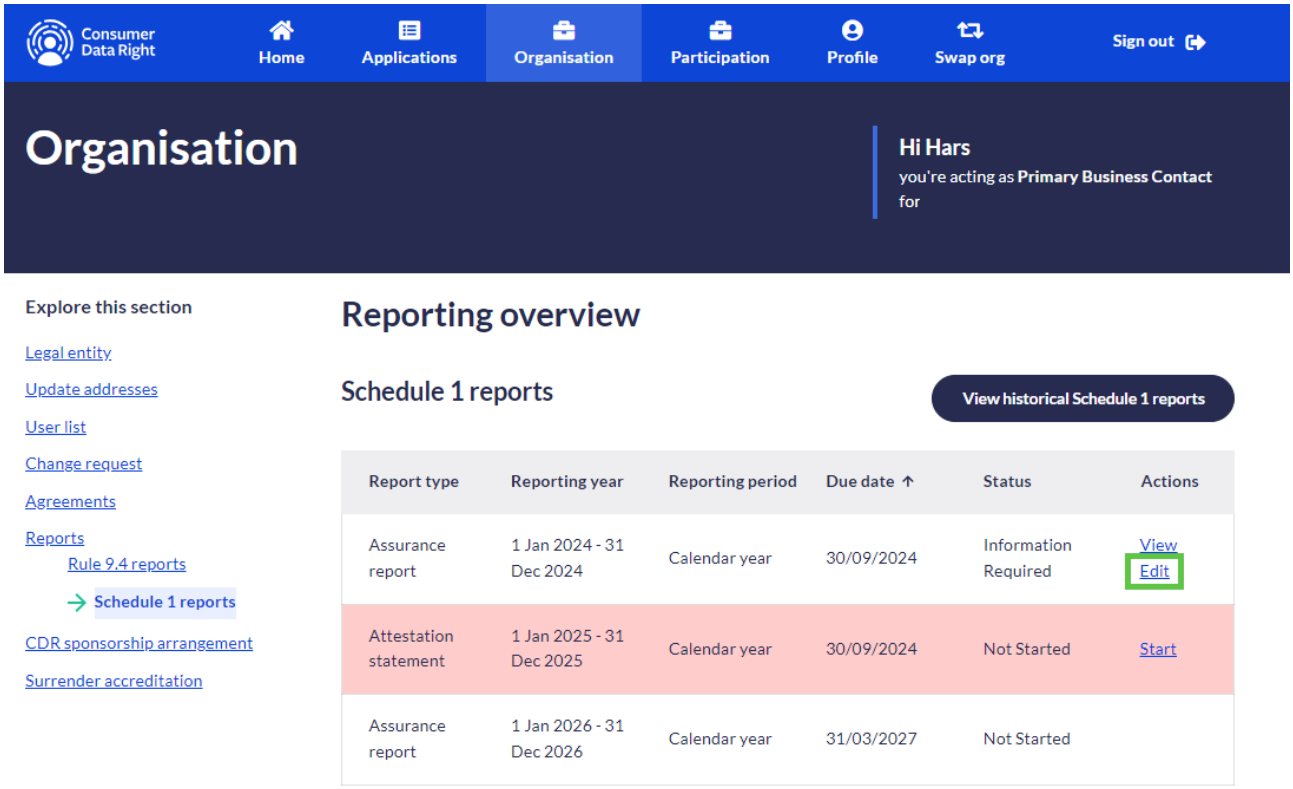
A primary business contact, authorised business contact, primary IT contact or an authorised IT contact can view the submitted reports by following the below steps:

1. Log in to the Participant Portal at https://portal.cdr.gov.au and select **Organisation** from the top navigation menu, then **Reports>Schedule 1 reports** from the left side navigation pane.
2. Select **View historical schedule 1 reports** to view reports that are submitted in the past.
3. Select **View** from the Actions column.
4. View all submitted details including files uploaded.
5. Click on the file name to download a copy of the report.

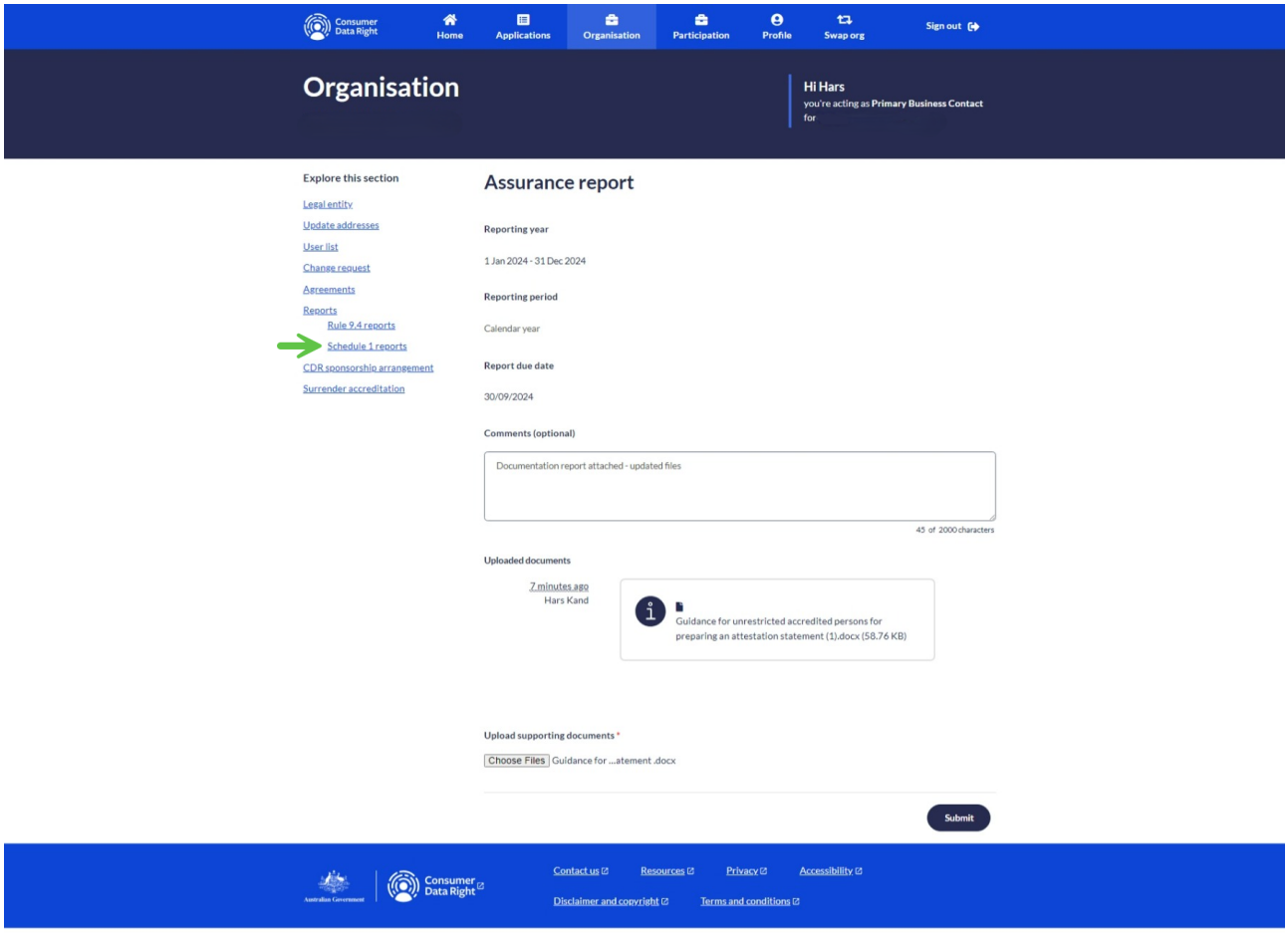
13.1.3 Edit a submitted Schedule 1 Historical report

A primary business contact, authorised business contact, primary IT contact or an authorised IT contact can edit a submitted reports by following the below steps:

1. Log in to the Participant Portal at https://portal.cdr.gov.au and select **Organisation** from the top navigation menu, then **Reports>Schedule 1 reports** from the left side navigation pane.
2. Select **Edit** from the Actions column for the record that is in 'Information required' status.



3. Upload additional documents and comments if required. User can view previous comments and files uploaded.
4. Click on the file name to download a copy of the report that was uploaded in the past.
5. Click on submit to provide the updated report.


Consumer Data Right
Home
Applications
Organisation
Participation
Profile
Swap org
Sign out
Organisation
Hi Hars
you're acting as Primary Business Contact
for
Explore this section
Legal entity
Update addresses
User list
Change request
Agreements
Reports
Rule 9.4 reports
Schedule 1 reports
CDR sponsorship arrangement
Surrender accreditation
Assurance report
Reporting year
1 Jan 2024 - 31 Dec 2024
Reporting period
Calendar year
Report due date
30/09/2024
Comments (optional)
Documentation report attached - updated files
45 of 2000 characters
Uploaded documents
7 minutes ago
Hars Kand
Guidance for unrestricted accredited persons for preparing an attestation statement (1).docx (58.76 KB)
Upload supporting documents *
Choose Files Guidance for ...atement .docx
Submit
Australian Government
Consumer Data Right
Contact us
Resources
Privacy
Accessibility
Disclaimer and copyright
Terms and conditions

14 Getting help

If you have any questions about accessing and using the CDR Participant Portal, please contact us via the CDR Service Management portal.

Alternatively, you can contact us via email at CDRtechnicaloperations@accc.gov.au.

15 Appendix: User roles and permissions

The Participant Portal supports multiple user roles with different permission profiles which allow participants to effectively manage their entity's information. Multiple users in an organisation can be assigned to each role except for the authorised CTS tester role.

Role	Overview	User actions	Legal entity	Accredited data recipient	Data holder

Primary business contact	Administration role for the participant's activities on the Participant Portal. At least one primary business contact is required and is the first role assigned during the account creation process. The initial primary business contact must be a person who is listed on the organisation's business record	• manage own profile • view user list • invite new users • assign and modify a user's role • modify details of existing users • remove a user	• view and update organisation details • view and accept agreements • manage on-boarding • Submit change request • start, update and submit rule 9.4 report	• start, view, update, submit, and withdraw "draft" accreditation application • create, update, view brand and brand participation • create, update and view software product • manage production certificate, authentication and endpoint details • submit CTS enrolment form • manage CTS certificate, authentication and endpoint details	• register as a data holder • create, update, view brand and brand participation • manage production certificate, authentication and endpoint details • submit CTS enrolment form • manage CTS certificate, authentication and endpoint details

				• Notify CDR representative arrangement (unrestricted ADR) • Notify CDR sponsorship arrangement (unrestricted ADR) • Surrender accreditation	

Authorised business contact	Performs a supporting administrator role for the legal entity's activities on the Participant Portal	• manage own profile • view user list	• view and update organisation details • view agreements • view change request • start, update and submit a rule 9.4 report	• view, update and withdraw "draft" accreditation application • create, update, view brand and brand participation • view software product production certificate, authentication and endpoint details	• register as a data holder • create, update, view brand and brand participation • view production certificate, authentication and endpoint details

Primary IT contact	A primary IT contact performs an IT administrator role for the legal entity's activities on the Participant Portal.	• manage own profile • view user list	• view organisation details • view agreements • manage on-boarding • view change request • start, update and submit a rule 9.4 report	• view, update and withdraw "draft" accreditation application • create, update, view brand and brand participation • create, update and view software product • manage production certificate, authentication and endpoint details • submit CTS enrolment form • manage CTS certificate, authentication and endpoint details	• view registration • create, update, view brand and brand participation • manage production certificate, authentication and endpoint details • submit CTS enrolment form • manage CTS certificate, authentication and endpoint details

Authorised IT contact	An authorised IT contact is a support role for the primary IT contact	• manage own profile • view user list	• view organisation details • view agreements • manage on-boarding • view change request • start, update and submit a rule 9.4 report	• view and update "draft" accreditation application • create, update, view brand and brand participation • create, update and view software product • manage production certificate, authentication and endpoint details • submit CTS enrolment form • manage CTS certificate, authentication and endpoint details	• view registration • create, update, view brand and brand participation • manage production certificate, authentication and endpoint details · submit CTS enrolment form · manage CTS certificate, authentication and endpoint details

Legal authority contact		• manage own profile • view users list	• view organisational details • view and accept agreements • view change request	• view accreditation application • view brand and brand participation • view software product • view production certificate, authentication and endpoint details • Notify CDR representative arrangement (unrestricted ADR) • Notify CDR sponsorship arrangement (unrestricted ADR)	• view registration • view brand and brand participation • view production certificate, authentication and endpoint details

Authorised CTS tester	The authorised CTS tester role provides access to the CTS to conduct technical testing on brand and software products.	• manage own profile • view users list	• view organisational details • view agreements	• view brand and brand participation • view software product • submit CTS enrolment form • view and update CTS authentication and endpoint details • view CTS certificates	• view brand and brand participation • submit CTS enrolment form • view and update CTS authentication and endpoint details • view CTS certificates