Australian Government

Consumer Data Right

CDR participant on-boarding guide

Version 3
January 2026

Version Control		
December 2020	Version 1.0	First version of Guide.
March 2021	Version 1.2	Updated references to white label products
June 2021	Version 1.3	Updated references to participant contacts
April 2023	Version 1.4	Updated link to the certificate management information, certificate agreements and policy documents. Removed screenshots of the CTS certificate section of the Participant Portal.
February 2025	Version 2	Updated the on-boarding process and included relevant screenshots throughout the guide. Updated references to white label products. Updated to improve readability of guide.
January 2026	Version 3	Updated the process for using the Conformance Test Suite Updated the process to request activation on the Register of Accredited Person and associated database Updated wording throughout the document to improve readability

Table of Contents

! Important notice

The information in this publication is for general guidance only. It does not constitute legal or other professional advice and should not be relied on as a statement of the law in any jurisdiction. Because it is intended only as a general guide, it may contain generalisations. You should obtain professional advice if you have a specific concern.

The ACCC has made every reasonable effort to provide current and accurate information, but it does not make any guarantees regarding the accuracy, currency or completeness of that information.

Parties who wish to re-publish or otherwise use the information in this publication must check this information for currency and accuracy with the ACCC prior to publication. This should be done prior to each publication edition, as ACCC guidance and relevant transitional legislation frequently change. Such queries should be addressed to accc-cdr@accc.gov.au

1. What is on-boarding?

1.1. Overview

We use the term 'participants' to refer to Consumer Data Right (**CDR**) data holders and accredited data recipients. 'On-boarding' is the process participants must complete to commence active participation in the CDR ecosystem.

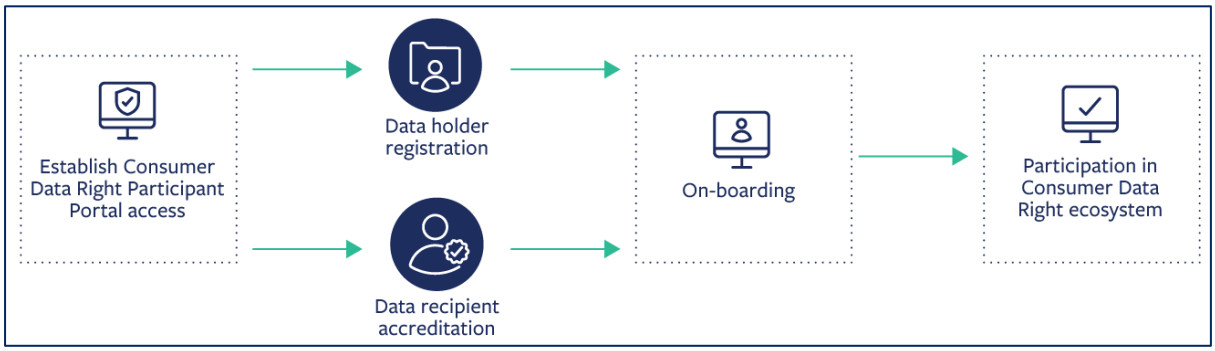
The on-boarding process enables the Accreditation Registrar (the **Registrar**) to confidently introduce new participants into the CDR ecosystem and ensure the ongoing security, integrity and stability of the Register of Accredited Persons (the **Register**) and the associated database.

This guide will help you understand what you must do to become an active CDR participant.

1.2. Context

The on-boarding process starts after a data holder completes registration, or accreditation is granted to a data recipient (figure 1).

Figure 1 On-boarding context



1.3. Role of the Accreditation Registrar

The Australian Competition and Consumer Commission (**ACCC**), acting as the Registrar, manages the on-boarding process and, maintains the ongoing security, stability and integrity of the Register and the associated database.

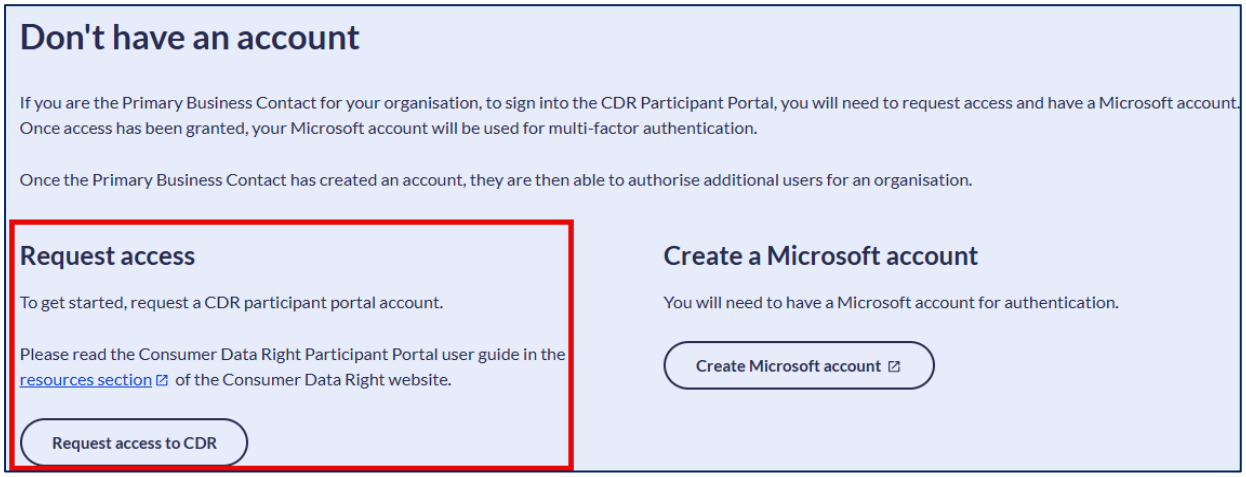
Other roles and functions of the Registrar include:

- issuing requests to participants to provide information or for participants to do specified things to fulfil its functions,
- publishing certain information about participants, and
- including other information about participants in the associated database if the Registrar considers that participants require that information to process data requests in accordance with the *Competition and Consumer (Consumer Data Right) Rules 2020* (**CDR Rules**) and, the Consumer Data Standards (the **Standards**).

1.4. Registering as a data holder

If you are a data holder with CDR obligations, your first step is requesting access to the CDR Participant Portal (the **Participant Portal**) by navigating to https://portal.cdr.gov.au and submitting an access request (figure 2).

Figure 2 Requesting access to the Participant Portal



Once you have access to the Participant Portal, you can login to complete your registration. The CDR Participant Portal user guide will assist you with this process and, interacting with the Participant Portal in the future.

1.5. Become an accredited data recipient

You can find information about becoming an accredited data recipient on the Become an accredited data recipient page on the CDR website and in the Accreditation Guidelines.

2. Getting started checklist

Before you can start on-boarding, you must meet the requirements in table 1. Please read this section carefully.

Table 1 Getting started checklist

Pre-requisites	Completed
Access to the Participant Portal The legal entity must be granted access to the CDR Participant Portal and, the following roles must be delegated to all appropriate users from your organisation; • the primary IT contact, and • authorised IT contacts who can provide technical information about your technology solution. Please see the CDR Participant Portal User Guide for more information.	☐
Accreditation or registration • **Data holders: your** legal entity must be registered to begin on-boarding. • **Data recipients:** your legal entity **must be accredited to** begin on-boarding.	☐
Identifying a legal authority contact You must identify a legal authority contact, who is authorised to accept the required legal agreements on behalf of your legal entity. Please ensure that you enter the details of your legal authority contact into the Participant Portal. See the CDR Participant Portal User Guide for more information.	☐
White label products **Please consult Appendix C: White label products** and, consider if any of the white labelling scenarios apply to you.	☐

3. Participant responsibilities

You are responsible for the development, release and, support of your solution. This includes but, is not limited to:

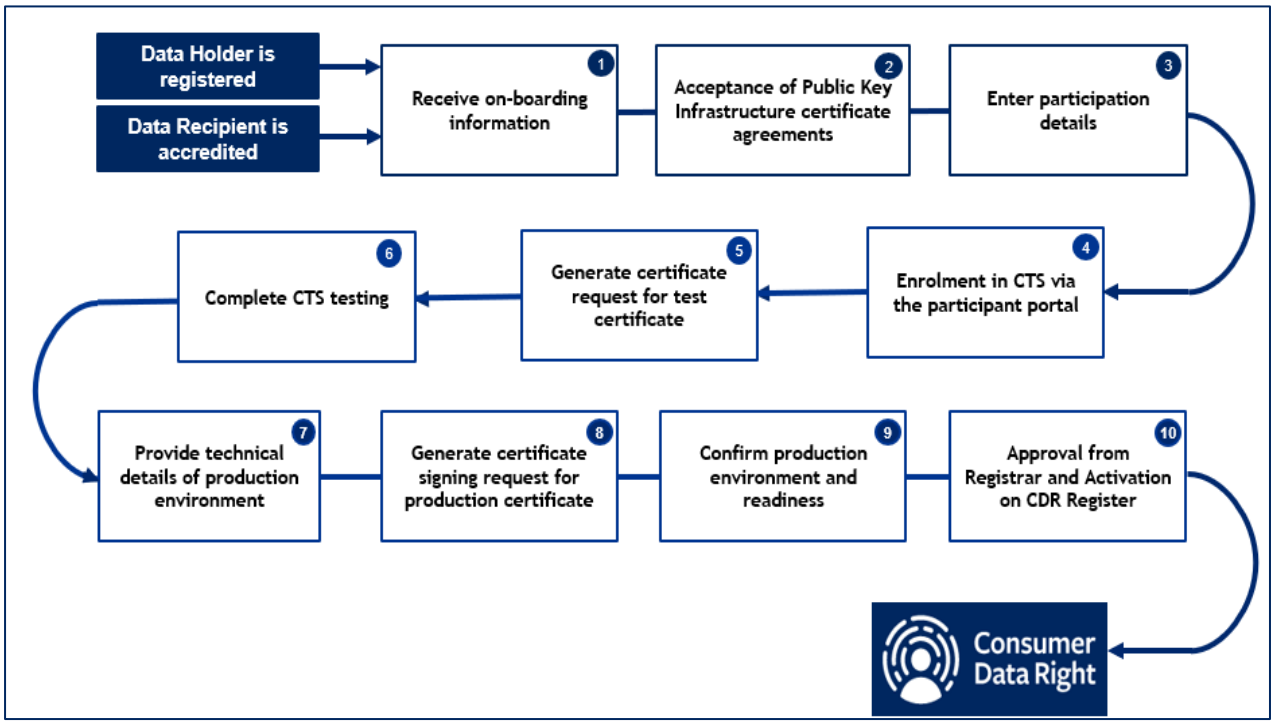
- establishing your infrastructure operations and, IT services/support procedures,
- building and deploying your production and test environments,
- training your technical users so they can provide support to your solution,
- keeping all documentation related to your solution up to date,
- completing all configuration activities within your control such as the installation of your production and test certificates,
- managing all change releases to your solution,
- monitoring the ongoing performance, scalability and, security of your solution,
- providing clear and accurate information to the market and consumers about your CDR offering,
- completing regular internal quality assurance and security testing of your CDR solution (see Appendix A: Testing guidance for further information), and
- ensuring on-going compliance with the CCA, CDR Rules, Data Standards and, Privacy Safeguards.

4. The on-boarding process

4.1. High level overview

The on-boarding process is a series of steps that participants must complete before they can participate in the CDR ecosystem (figure 3). You can find a detailed description of each step and, its associated activities in the 'On-boarding process – Step-by-step instructions' section of this guide.

Figure 3 Overview of the on-boarding process



4.2. Indicative timeframe

Each participant will take a different amount of time to complete the on-boarding process. Your unique circumstances and the maturity of your processes and systems influence how quickly you can complete on-boarding. Some general estimates of the timeframes for each step are listed in table 2.

Table 2 Indicative timeframes

#	Step	Participant	ACCC
1	**Receive on-boarding information**	N/A	1–3 business days
2	**Acceptance of Public Key Infrastructure certificate agreements**	1–5 business days Dependent on your legal review and acceptance processes.	N/A
3	**Enter participation details**	1–5 business days	N/A

4	**Enrolment in CTS via the participant portal**	1–14 business days You should have your test environment ready for deployment and be able to provide certain technical information.	N/A
5	**Generate certificate signing request for test certificate**	1 business day	1 business day
6	**Complete CTS testing**	1-30 business days This can be influenced by the maturity, readiness and conformance of your solution, as well as your ability to troubleshoot issues if they occur.	1–30 business days We will support you through this process.
7	**Provide technical details of production environment**	1–5 business days	N/A
8	**Generate certificate signing request for production certificate**	1–5 business days	3–5 business days We will review and check the request and provide the production certificate upon approval.
9	**Confirm production environment and readiness**	1–14 business days This depends on your change/release management practices and how long it takes to install your production certificate and configure your solution to connect to the Register and the associated database.	N/A
10	**Approval from the Registrar and activation on Register and associated database**	N/A	5–14 business days This depends on if the information you provide is sufficient for the Registrar to decide to activate you and that you pass the technical assessments.
	Indicative Total Timeframe	**3 weeks – 5 months**	

5. On-boarding process – Step-by-step instructions

This section will guide you through completing each step of the on-boarding process.

Note

We have presented the on-boarding process as a series of sequential steps. You will follow some steps in the order presented but, there are some steps that may be done in a different order or, in parallel with other steps.

For example, if your production environment is ready, you can provide us your production details or, request a production certificate from us at the same time as completing the Conformance Test Suite (CTS).

Ultimately, you must meet all of the on-boarding requirements and complete the entire on-boarding process before you can be activated in the ecosystem.

5.1. Step 1: Receive on-boarding information

We will send detailed information about the on-boarding process to your primary business contact after you are granted accreditation (data recipient), or you complete registration (data holder).

If you do not receive this email, please contact CDROnboarding@accc.gov.au

5.2. Step 2: Acceptance of Public Key Infrastructure certificate agreements

The Registrar issues Public Key Infrastructure (**PKI**) certificates to participants for use in the CDR ecosystem. PKI certificates enable secure and private communications between participants in the CDR ecosystem. Before the Registrar can issue your PKI certificates, you must agree to the Subscriber Agreement and, the Relying Party Agreement.

Subscriber Agreement

The Subscriber Agreement establishes the basis on which digital PKI certificates are issued to participants. It also sets an obligation on participants to safeguard and appropriately manage all PKI certificates issued to them. This is vital in ensuring the overall security, integrity and stability of the Register and associated database and the CDR ecosystem as a whole.

ACCC certification services and the use of PKI certificates are governed by the ACCC Certificate Policy, which is incorporated in its entirety in the Subscriber Agreement. Full details of the role and obligations of all entities associated with operation of the ACCC PKI are included in the Certificate Policy.

The Subscriber Agreement contains the contractual rights and obligations governing the use of a digital PKI certificate. This agreement contains some very important provisions governing the subscriber's responsibility and legal liability for using a PKI certificate. Participants should read this Subscriber Agreement and the documents referenced in it, carefully.

Relying Party Agreement

The Relying Party Agreement establishes the basis on which participants rely on the information protected by ACCC digital PKI certificates. It incorporates the ACCC Certificate Policy which includes a full description of the terms and conditions associated with reliance on ACCC digital PKI certificates.

The Relying Party Agreement sets out the contractual rights and obligations governing reliance on a digital PKI certificate. It contains very important provisions governing the

relying party's responsibility and legal liability in relying on a certificate. Please carefully read the agreement, and the documents referenced in it.

Policy and procedural documents

The use of PKI certificates in the ecosystem is underpinned by:

- the Certificate Policy document which defines the framework for the management and administration of PKI certificates, and
- the Certification Practice Statement which provides a detailed description of the processes and procedures related to our implementation of our Certificate Policy.

It is very important that you read and understand these documents. They form part of the Subscriber and Relying Party Agreements and place certain obligations and responsibilities upon subscribers and relying parties. The latest versions of the agreements, the policy and the procedural documents are available on the CDR website.

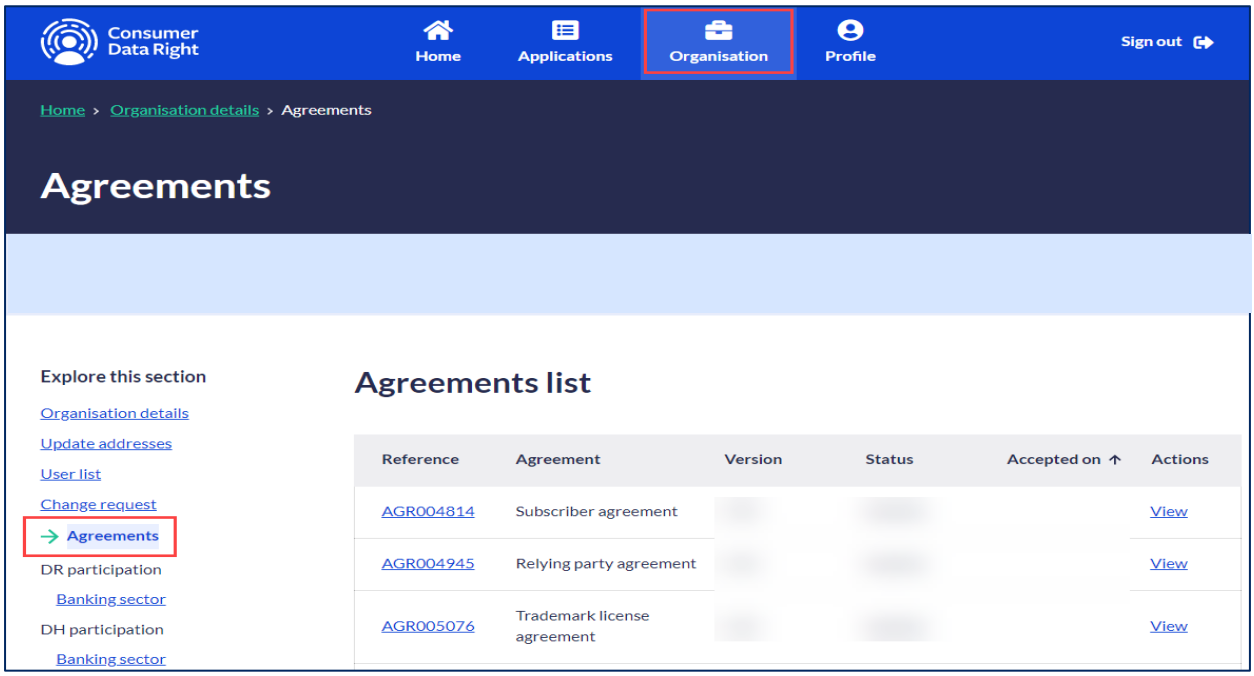
> **Note**
>
> These agreements can only be accepted by your legal authority contact in the Participant Portal.

Accepting the agreements

To accept the agreements:

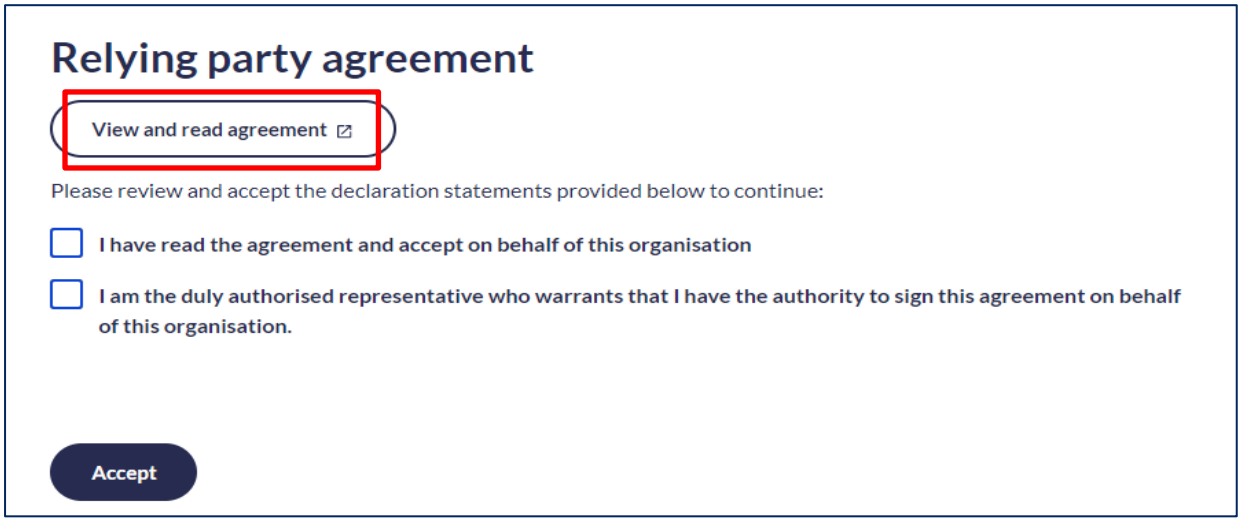
1. Login to the CDR Participant Portal and navigate to your organisation record.
2. Select the agreements option to view the list of agreements (figure 4).

Figure 4 Agreements list



3. Select an agreement (Subscriber Agreement or Relying Party Agreement) to view the contents.
4. On the agreement page, click on the view and read agreement button to review the agreement (figure 5).

Figure 5 View and read agreement



5. If you have the appropriate authority and wish to accept the agreement on behalf of your organisation, tick the checkboxes and press the accept button.
6. When you return to the agreements list, the agreement should now be shown as agreed.

5.3. Step 3: Enter participation details

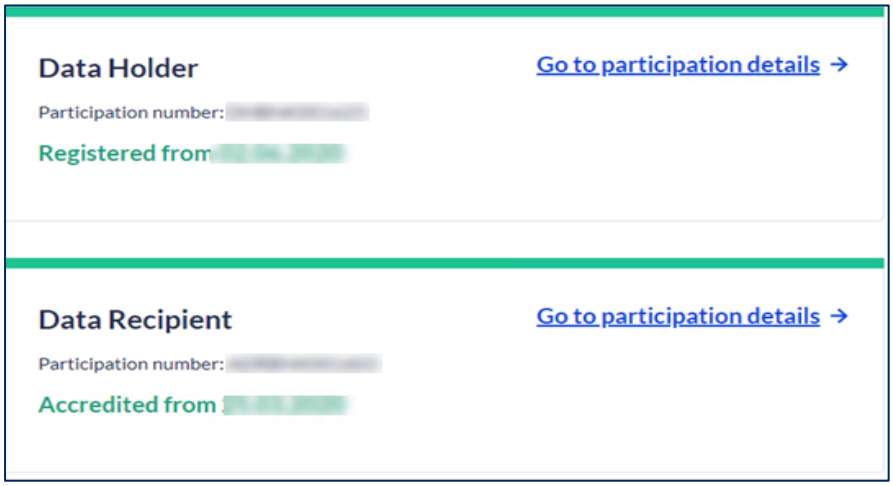
To enter your participation details:

1. Login to the CDR Participant Portal and navigate to your organisation record (figure 6).

Figure 6 Navigating to the organisation record

2. This should display your organisation's participation status (data holder and/or data recipient) as demonstrated in figure 7.

Figure 7 Display of participation status



For data holders with product reference data:

If you are a data holder in the non-bank lenders sector who has product reference data (**PRD**) obligations, you must provide the following information:

- Logo URI
- Website URL
- PRDpublicbase URI and ProoductbaseURI

> **Note**
>
> If you do not have consumer data sharing obligations, you do not need to complete the rest of the onboarding process.

For data holders with consumer data:

If you are a data holder in the non-bank lenders sector who has consumer data sharing obligations, you must provide the details listed in table 3. You can find additional guidance in the CDR Participant Portal User Guide.

Table 3 Entering data holder participation details

Section	Field name
Legal entity details	Legal entity website URL Legal entity logo URI Legal entity CDR policy URL
Brand details	Brand name Brand description Brand type Brand group (This is an optional field for white label products. Please see Appendix C for more information)
Brand details	Participation type Logo URL Website URL CDR policy URL

For accredited data recipients:

The data you provide in your accreditation application will be used to prefill your participation details. Please review the information to ensure it is complete and accurate. Based on your data recipient participation status, enter further details as necessary (table 4).

Further information is available in the CDR Participant Portal User Guide.

Table 4 Data recipient participation details

Section	Field name
Brand participation details	Participation type Logo URI Website URL CDR policy URL
Brand details	Brand name Brand description Brand type
Software product details	Name Description

Note – CDR representative arrangements naming convention

All data recipient software products for use by a CDR representative must include the full name of that CDR representative. This establishes a clear link between the representative arrangement and the software product for all users of the Register and the associated database.

This naming convention is an important component of the integrity of the Register and the associated database.

For example: ABC Credit Reporting Pty Ltd enters into a CDR representative agreement with a CDR principal who has unrestricted accreditation. It offers services to consumers under its brand name Quick Credit Checks. The software product for this arrangement could take the following forms:

- ABC Credit Reporting Pty Ltd, or
- Quick Credit Checks (ABC Credit Reporting Pty Ltd).

5.4. Step 4: Provide technical details of your test environment

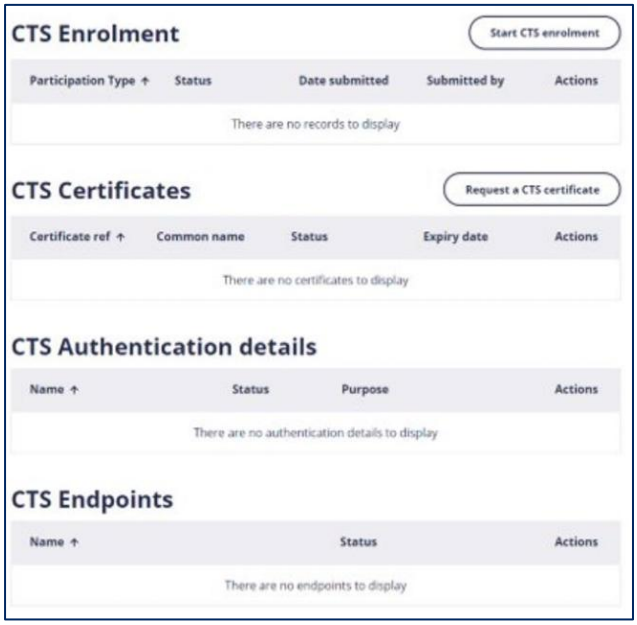
You must provide the technical details of your target test environment before you can conduct conformance testing through the Conformance Test Suite (**CTS**). Your test environment should have a similar configuration to your future production environment so that it provides an accurate representation of how your production environment will interact with the CDR ecosystem.

Providing the details

- After you have accepted the PKI certificates (section 5.2), your primary business contact, primary IT contact and authorised IT contact can complete the CTS enrolment form in the Participant Portal.
- For a data holder, the CTS enrolment form location is: “Participation” > “Data Holder” > “Brand” > “View Brand” > “View Brand Participation” > “CTS Details” > then “CTS Enrolment”.
- For a data recipient, the CTS enrolment form location is: “Participation” > “Data Recipient” > “Brand” > “View Brand” > “View Brand Participation” > “Software Product” > “CTS Details” > then” CTS Enrolment”.
- You will also need to nominate an authorised CTS tester who must have a valid Participant Portal user account.

- The CTS enrolment form can be amended in the Participant Portal by the primary business contact, primary IT contact or authorised IT contact before it is submitted.
- If you need to make an adjustment to the form after it has been submitted, please send an email to the Technical Operations team (CDRTechnicalOperations@accc.gov.au) and outline the relevant adjustment.
- After completing the CTS enrolment form, you will be able to generate your CTS PKI certificates, add your CTS authentication details and, your CTS endpoint URIs for testing (see figure 8).

Figure 8 CTS technical details



- When you complete your CTS enrolment, your conformance ID will be displayed on screen and sent to the primary business contact by email. Your next step is to configure this in your software solution to access the CTS APIs.
- You can find further technical information about conducting this activity on the Conformance Test Suite: version history and scenarios page of our website.

Note
Your primary business contact, primary IT contact and authorised IT contact can change your technical details for CTS if required in the Participant Portal after enrolment.

If we have already provided you with a CTS test plan, you will not be able to make these changes so please email the Participant Engagement team (CDROnboarding@accc.gov.au) to request the change and for a new test plan to be assigned to you.

5.5. Step 5: Generate certificate signing request for test PKI certificate

The primary business contact, primary IT contact and authorised IT contact of a participant can maintain your CTS certificates on the Participant Portal.

Generating a Certificate Signing Request

The Standards specify certain things you must do to generate a certificate signing request (CSR). Please ensure you meet the requirements of the Standards and then follow your internal processes and procedures for generating a CSR. Please refer to the Certificate Management – Consumer Data Standards for further information.

We will send you an email informing you of the outcome of your CTS certificate request. It will also provide information about the next steps for the participant to complete.

After we approve your request for a CTS certificate, you will be able to download your certificate from the Participant Portal using the download hyper link (figure 9). A copy of the certificate will be sent to the email address provided on your CTS certificate request.

The root and intermediate certificate chain for the generated CTS Certificate can be found in the CTS connection data sheets.

You can view the status of your CTS certificate on the CTS details section of the Participant Portal, along with actions that are available to you (Figure 9). We will notify you to renew your certificate 30 days before its expiry date.

Figure 9 CTS certificate status and actions

You can view current and previous CTS certificates in the Participant Portal by selecting view in the actions column (figure 9). This will display the CTS certificate details and, installation instructions.

5.6. Step 6: Confirm environment is configured and available for testing

You will need to configure your test environment to allow it to communicate with the CTS. The CTS connection data sheet provides further information to assist you with connecting to CTS. You may need to change some of your infrastructure settings, such as firewall rules or IP whitelisting to complete this action.

Once you have configured your test environment to connect to the CTS, you need to install your CTS certificate into your test environment to enable secure communication with CTS.

After configuring your test environment and installing your test certificate, you are ready to begin conformance testing. Please send an email to CDROnboarding@accc.gov.au using the following subject line: Commence CTS testing – [legal entity name] to confirm your readiness for CTS conformance testing and, we will then assign you a test plan for completion.

Further resources and information

There is a range of information and resources available to help you through CTS on the CDR website such as;

- the Participant conformance approach

- the CTS technical guides
- the CTS connection data sheets, and
- information about CTS for accredited data recipients and data holders

5.7. Step 7: Complete CTS conformance testing

We maintain the CTS which is a suite of automated test cases that are executed against your solution. It tests how your solution interacts with a simulation of the Register and the associated database and, other CDR participants.

Participants are expected to have developed their solution and completed quality assurance testing before requesting access to CTS. You can find more information about this and, other aspects of CTS in our guidance on the Participant conformance approach.

Additional brands and software products

Data holders must complete CTS on the latest applicable test plan for at least one brand. Further brands can skip CTS if they use the same CDR solution and data platform as the first brand.

If your additional brand has a different CDR solution or data platform to the first brand, or if the test plan has significantly changed since you last passed CTS, the additional brand will need to complete CTS.

Accredited data recipients must complete CTS on the latest applicable test plan for at least their first 2 software products. Further software products can skip the CTS step if they use the same code base as 2 of your active software products that have completed CTS on the latest applicable test plan.

If your additional software product has a different code base to your active software products, or if the test plan has significantly changed since you last passed CTS, the additional software product will need to complete CTS.

> **Note**
>
> CTS is regularly updated throughout its development lifecycle. If we make significant changes to CTS, the Registrar may request participants to complete CTS again against the updated CTS test plan.

Progress and results

You can track your progress and associated results in the CTS Portal. When you have completed and submitted the CTS test plan, please contact the Participant Engagement team on CDROnboarding@accc.gov.au and we will send you your completed CTS report.

Technical support through the CDR Service Management Portal

If you encounter any technical issues while performing conformance testing, you can request support by raising a ticket in the CDR Service Management Portal (**SMP**). You will also use SMP after you become active in the ecosystem to raise tickets for issues you encounter and receive tickets raised by other participants and the ACCC.

Each participant has a maximum of 5 customer and 2 agent licences on the SMP (see figure 10 for the SMP role types). Please inform the Participant Engagement team who you would like to add as agents and customers (with their names and emails) and the team will organise your access.

Figure 10 SMP role types

Role Type	Description
Customer	Has restricted access that allows this role to raise new incidents and service requests, view and comment on incidents that are shared with them.
Agent	Can access queues, raise and process incidents and service requests (i.e. move incidents through workflows, reassign incidents to other teams and make customer-facing comments).

There is further information in the CDR Service Management Portal user guide and in the knowledge article on How to get access to the CDR Service Management Portal.

5.8. Step 8: Provide technical details of production environment

After you complete the build, internal testing and quality assurance activities of your production environment, you will need to add the technical details into the Participant Portal. These details are like those provided for your testing environment in section 5.3.

You may find some information has been pre-populated in the Participant Portal. If so, please review the information to ensure that it is complete and accurate.

Note

Only your primary business contact, primary IT contact or authorised IT contact can request your production PKI certificate, maintain authentication details and, maintain endpoints.

Further information about adding your production details in the Participant Portal is available in the CDR Participant Portal user guide.

Required production details for accredited data recipients

Accredited data recipients must provide the ACCC with:

- Participation details
- Brand details
- Certificate request
- Authentication details
- Software product details
- Software product authentication details
- Software product endpoints

Required production details for data holders

Data holders must provide the ACCC with:

- Participation details
- Brand details
- Certificate request
- Authentication details
- Endpoints

5.9. Step 9: Generate certificate signing request for a production certificate

Generating a Certificate Signing Request

- Participants should follow their internal processes for generating a certificate signing request (**CSR**) and managing certificates.
- Please consult the Certificate Management guidance so you understand the type of certificates (server and/or client) you need.
- For guidance on generating the certificate signing request for your production certificate – please refer to the Participant Portal user guide Please note, it will take us 3 – 4 days to issue your production certificate.
- Please reach out to the CDR Technical Operations team via CDRTechnicalOperations@accc.gov.au if you require any assistance with your production certificate.

Note for data holders

Data holders must provide their production end points before requesting their production PKI certificate.

5.10. Step 10: Confirm production environment and readiness

After you receive your production PKI certificate, you need to configure it within your production environment before you are made active on the CDR Register. This includes confirming your solution infrastructure is in place, configured, and is ready to process data requests within the ecosystem.

Providing confirmation of readiness

The production readiness confirmation (**attestation**) provides assurance to the Registrar that you have completed the required tasks to begin active participation in the CDR ecosystem. Your primary business contact must complete the attestation and confirm:

- the brand(s) or software product(s) to be activated,
- that additional brands share the same core data platform, CDR solution, and level of conformance,
- the additional software product to be activated has the same code base as 2 of your existing active software products,
- your solution complies with relevant legal requirements (e.g. the CDR rules),
- CTS has been completed where relevant, and
- completion of all other activities required for your successful on-boarding.

You can also advise us if you have any implementation gaps in your solution. If this is the case, you need to provide the following information:

- details of the gap,
- how it impacts consumers and the total number of consumers affected, and
- your proposed resolution and when you anticipate implementing it.

Please allow at least 5 business days before your proposed activation date for us to process your activation request.

Note on activations

Data holders

You must be ready to process requests for CDR data as soon as you become active in the ecosystem. This is because you are immediately discoverable in the ecosystem when you are made active on the Register and the associated database. Therefore, you must ensure your production environment is available with the production PKI certificate installed before requesting activation. This ensures that you can control the release of your solution into the ecosystem.

Accredited data recipients

Accredited data recipients are responsible for performing Dynamic Client Registration (DCR) requests when they are ready to commence participation.

5.11. Step 11: Activation on the Register and associated database

When we receive your production readiness confirmation, we will:

- review the information and provide it to the Registrar who will assess the information and decide whether to approve activation,
- seek further information from the primary business contact if required,
- inform you of the Registrar's decision and, if approved, will confirm the timing of your activation on the CDR ecosystem, and
- activate you on the Register or associated database and inform you by email when this is complete.

Note

Please note, if issues are found with your production details after the Registrar has provided approval, we may need to delay your activation until these issues are resolved.

6. Participation

You can operate within the ecosystem once you have completed the on-boarding process and the ACCC has made you active on the Register or associated database. Congratulations!

As your solution continues to evolve and change over its life cycle, you may need to revisit certain aspects of the on-boarding process, such as CTS, to ensure new features meet conformance requirements, and the Registrar may issue requests for further information or further testing.

Appendix A: Testing guidance

Overview

The successful operation of the CDR ecosystem depends on the successful operation of the technology solution deployed by each participant. This section provides a general overview of our testing requirements to help you prepare for the production release of your solution.

We strongly encourage you to refer to the CTS guidance material for more detailed guidance about completing CTS testing including how to prepare for and execute the CTS tests. The CTS tests focus on the critical risk points for participation in the ecosystem. It does not test against all possible scenarios that may arise during your participation in the ecosystem.

You are responsible for ensuring that your technology solution meets all of the requirements for active participation including ongoing testing, quality assurance and conformance to the Standards, the CDR rules and the CCA.

Note:

The scope of CTS will evolve over time as the CDR ecosystem matures. This may include additional test scenarios and other changes. You can see the Conformance Test Suite: version history and scenarios for changes to CTS over time.

If there are significant changes to CTS, the Registrar may request you to complete CTS again in fulfilling its function of maintaining the security, stability and integrity of the Register and the associated database.

Testing principles

The principles listed below underpin our testing requirements:

- Each participant can enter the ecosystem without disrupting the continued operation of the ecosystem, ensuring scalability.
- Participants will complete regular and extensive internal testing of their solution.
- Participants will complete all internal testing activities before starting CTS testing.
- Participants will complete all relevant testing to ensure their solution meets the non-functional requirements of the data standards. You can find more information about the non-functional requirements in the data standards.

Participant testing scope

Each participant must ensure that their solution meets all the requirements for participation in the ecosystem. These requirements are defined by the Rules, the Standards, the Register Documentation and Consumer Experience Guidelines. You must develop your testing scope so that it can be traced back to these requirements.

Testing tools

You can use a variety of tools to support and execute your testing activities such as an internally built tool, market-based tools, or testing tools offered through industry bodies such as FAPI. The ACCC does not recommend or certify any specific testing tools.

Completion of testing

We will generally not seek evidence that you have completed testing during the on-boarding process. If we need to clarify any aspect of the testing you have completed, the Registrar may issue a request under the CDR Rules to you seeking further information. This may inform other roles and functions performed by the ACCC including incident management, compliance or enforcement.

Appendix B: Getting help

There are several resources available to support participants complete the on-boarding process.

CDR Support Portal

The ACCC and the Data Standards Body (**DSB**) maintain the CDR Support Portal (the **Support Portal**). You can post questions on the Support Portal.

CDR website

The CDR website provides participants with general information on the process of getting on-boarded to the CDR ecosystem. It also includes a CDR information map which provides a topic-based listing of CDR information published by the CDR agencies.

CDR implementation call

The ACCC and DSB facilitate the fortnightly CDR implementation call. It provides a forum for participants and other stakeholders to ask questions about their obligations and, receive important updates on the CDR.

Seeking assistance from the CDR Participant Engagement team

The Participant Engagement team is available to help you if you have questions or need support as you work through the on-boarding process.

You can contact the Participant Engagement team by email at CDROnboarding@accc.gov.au.

Appendix C: White label products

White label products are supplied by one legal entity (a white labeller) then branded and retailed to consumers by another legal entity (a brand owner) (figure 11).

Figure 11 White labelling data flow

One example of white labelling is when a data holder enters a white labelling partnership with a non-data holder. In this scenario the data holder may have CDR obligations connected to this white labelled product.

Where 2 separate data holders enter a white labelling partnership (for example, where a brand owner bank distributes a credit card on behalf of a supplying bank) the data holder that has the contractual relationship with the consumer is required to respond to data requests for the white label product. However, the data holder that has the contractual relationship with the consumer may agree with the other data holder, that the other data holder will be subject to those obligations instead.

There are two options for brand owners to be recorded on the Register or associated database (table 5).

Table 5 Options for brand owners

Option	Description
1	The brand owner is a data holder: • The brand owner will be responsible for adding and managing their data holder brand/s on the associated database. They will work with the white labeller to determine the configuration of the brand identity. • Both parties must work together and with the Participant Engagement team to ensure the brand identity is optimised for consumer experience.
2	The white labeller is a data holder, the brand owner is **not** a data holder: • The white labeller will be responsible for adding and managing brands on the associated database. • Both parties must work together and with the Participant Engagement team to ensure the brand identity is optimised for consumer experience

Multiple white label brands

White labelling arrangements present the possibility of multiple brand owners having a brand with the same name. This could cause confusion for consumers and accredited data recipients. To minimise confusion, the standards have introduced a 'brand group' field and the ACCC and other regulators are drafting guidance on how this new field can be used. Participants will be notified when this new guidance is available.

The ACCC understands there is a wide variety of white label arrangements, and the above options may not cover all potential scenarios. The scenarios above are general examples of how white labelled products are managed in the CDR. You have flexibility regarding the nature of your commercial operations. However, it is your responsibility to ensure you comply with your CDR obligations in relation to the products you offer.

If you have any compliance concerns or queries regarding white label arrangements, please contact accc-cdr@accc.gov.au.

You can find more information about CDR obligations in white labelling arrangements in sections 5.7 and 6.5 of the Compliance guide for data holders in the banking and non-bank lenders sectors. You may also find the knowledge article on White Labelled brands in the CDR helpful as it provides some in depth examples.

For technical guidance on how to list your white label brand or product on the Register or associated database, contact CDR Technical Operations by email at CDRTechnicalOperations@accc.gov.au.

Appendix D: Use of the CDR logo

The CDR logo (the **logo**) is symbol of trust in the ecosystem. Before you can use the logo in your CDR solution, you must accept the CDR Trade Mark Licence Agreement (**TMLA**). The TMLA sets out the terms and conditions regarding the use of the logo. The latest version of the TMLA is available on the CDR website.

Apart from other Commonwealth agencies, only entities that have accepted a TMLA (**Licensees**) can use the CDR logo. Licensees may only use the logo for the purpose as specified in the TMLA.

After accepting the TMLA, the logo can be used:

- by an accredited person when asking a consumer for consent to collect and use CDR data, or
- by a data holder when asking a consumer to authorise the disclosure of CDR data.

After you accept the TMLA, you will be provided access to the logo for inclusion in your solution. The logo is available in various styles and file formats (see *Appendix D:*).

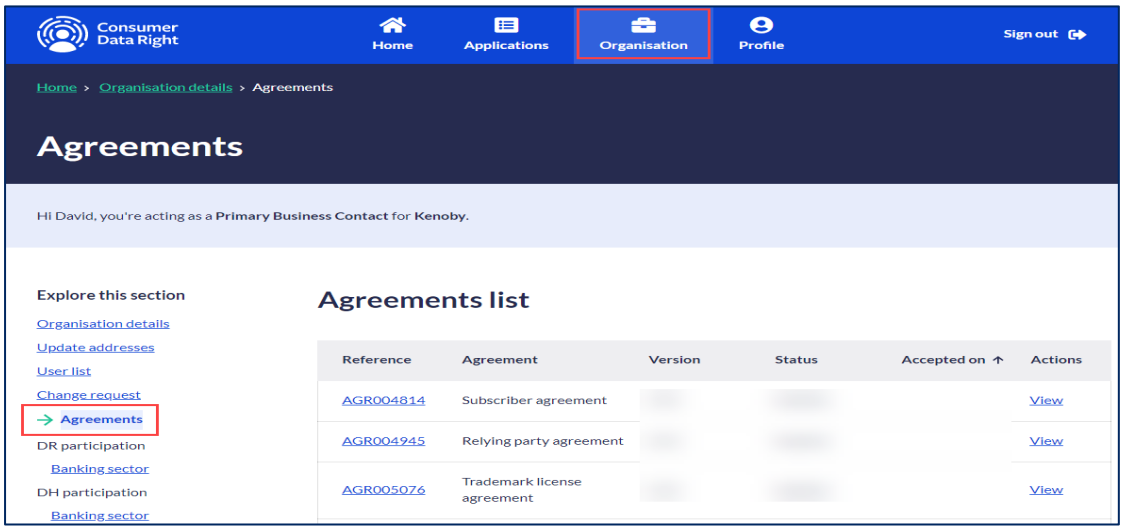
Further information about the use of the logo is available in the CDR logo fact sheet.

Confirming your intention to use the CDR Logo

To confirm your intention to use the logo:

1. Login to the CDR Participant Portal and, navigate to your organisation record.
2. Select the agreements option to view the list of agreements (figure 12).

Figure 12 List of agreements

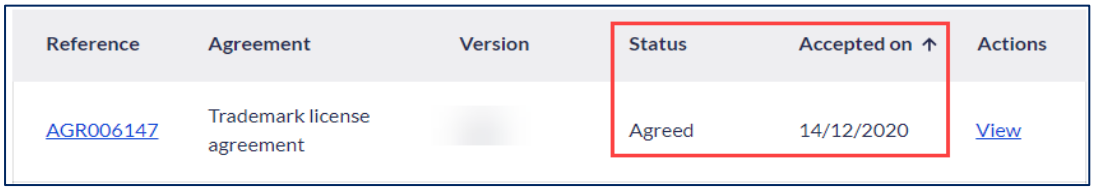


3. Select the trademark licence agreement to view the contents.
4. On the agreement page, click on the view and read agreement button to review the agreement (figure 13).

Figure 13 View and read agreement

5. If you wish to accept the agreement and, have the authority to accept it on behalf of your organisation, tick both checkboxes and press the accept button.
6. When you return to the agreements list the agreement should now be shown as agreed (figure 14).

Figure 14 Agreed trade mark licence agreement



7. The CDR Participant Portal user guide provides more information on viewing and accepting the agreements within the Participant Portal.
8. After you accept the TMLA, we will send the CDR logo by email in various styles (table 6) and formats (table 7). The primary lockup consists of the exact arrangement and design of the logo mark and the wordmark. This is the favoured orientation and should be used whenever possible.

You can find further information regarding the appropriate use of the logo in the Brand guidelines for participants and CDR logo - fact sheet.

Table 6 CDR logo styles

Coloured version (Primary logo)	
Mono version: White version Only used when colours are not allowed or if used over a busy background	
Mono version: Black version Only used when colours are not allowed or if used over a busy background	

Table 7 CDR logo formats

File Format	Style	Colour Scheme	Width	Height
PNG	Monogram	Black	1413	1412
PNG	Monogram	Colour	1413	1412
PNG	Monogram	White	1412	1412
PNG	Primary	Black	3845	1396
PNG	Primary	Colour	3844	1396
PNG	Primary	White	3845	1396
PNG	Short	Black	1413	2076
PNG	Short	Colour	1439	2137
PNG	Short	White	1412	2076
SVG	Monogram	Black		
SVG	Monogram	Colour		
SVG	Monogram	White		
SVG	Primary	Black		
SVG	Primary	Colour		Scalable
SVG	Primary	White		
SVG	Short	Black		
SVG	Short	Colour		
SVG	Short	White		

Appendix E: Participant Contacts

The ACCC will need to communicate with your organisation before and after you are active on the Register or associated database. It is important that you keep your list of contact people updated in the participant portal as set out in table 8.

Table 8 List of participant contacts

Communication type	Contact	System nominated/ maintained in	Communication method	Communication purpose
CDR ecosystem incidents	Agent licence	Service Management Portal (SMP)	System notification (SMP) / Email / Phone	Responding to tickets raised by a participant alerting the ACCC to issues emerging in the ecosystem.
CDR Logo - CDR Trademark Licence Agreement	Legal Authority Contact	CDR Participant Portal | User Guide	System notification (SMP) / Email / Phone	The ACCC will make contact if the terms in the Licence Agreement or the logo changes.
Certificates (Agreements)	Legal Authority Contact	CDR Participant Portal | User Guide	Email / Phone	The ACCC will contact you if terms in the agreements change or if any other changes affect use of the certificates. This communication purpose excludes the technical configuration of the certificates.
Certificates (Technical)	Primary IT Contact (PITC)	CDR Participant Portal | User Guide	Email / Phone	We will contact your PITC to: • provide technical support, • request the PITC to perform an action as part of steps 7.5 and 7.9 of the on-boarding process and, • for PKI certificate renewals. The ACCC **will not** use this method to transfer sensitive information or data related to your certificates. Your PITCs must use the CDR Participant Portal to action certificate related requests.

Communication type	Contact	System nominated/ maintained in	Communication method	Communication purpose
Compliance and Enforcement	Primary Business Contact	CDR Participant Portal | User Guide	System notification (SMP) / Email / Phone Letter	When the ACCC CDR Compliance and Enforcement teams need to contact you about CDR compliance related matters.
Conformance Test Suite	Primary IT Contact	CDR Participant Portal | User Guide	System notification (SMP) / Email / Phone	To assist you with working through CTS during the on-boarding process and throughout your active participation.
Get Metrics	Primary IT Contact	CDR Participant Portal | User Guide	System notification (SMP) / Email / Phone	To inform you about problems when attempting to obtain operational statistics from active data holders, such as, issues connecting to the endpoints or data quality issues.
On-boarding	Authorised Business Contacts / Authorised IT Contacts	CDR Participant Portal | User Guide	Email / Phone	Coordination of on-boarding and CTS activities prior to activation on the Register and associated database.
Update information on the Register or associated database	Primary Business Contact	CDR Participant Portal | User Guide	Email / Phone	Completion of production readiness confirmation for activation on the Register or associated database. Request for removal or name change on the Register or associated database.
Reporting	Primary Business Contact	CDR Participant Portal | User Guide	Letter / Email / Phone	Explore issues with reporting for purposes of rule 9.4, including data inaccuracy or anomalies emerging in analysis on data collected in the CDR ecosystem.

Communication type	Contact	System nominated/ maintained in	Communication method	Communication purpose
Temporary direction to refrain from Processing consumer data requests	Primary and Authorised Business Contacts; Primary and Authorised IT Contacts	CDR Participant Portal | User Guide	Trusted communications	This could stem from ecosystem wide issues such as a cyber-attack, major issues with participants platforms, unplanned and extended outages, data breaches etc.
Temporary restriction on use of Register and associated database (data holder)	Primary and Authorised Business Contacts; Primary and Authorised IT Contacts	CDR Participant Portal | User Guide	Trusted communications	This could stem from ecosystem wide issues such as a cyber-attack, major issues with the platform, unplanned and extended outages etc.