MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT
HĪKINA WHAKATUTUKI

CONSUMER DATA RIGHT

ACCREDITATION GUIDELINES

Version: 1.0

Date: December 2025

MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT
HĪKINA WHAKATUTUKI

PURPOSE

The purpose of this document is to provide guidelines for accreditation as a Data Requestor under the Customer Product Dat Act 2025

IMPORTANT NOTE:

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. Because it is intended only as a general guide, it may contain generalisations. MBIE 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. It is the responsibility of each CDR participant to be fully aware of its obligations under the CDR regulatory framework. We recommend that CDR participants obtain professional advice on how the CDR framework applies to their specific circumstances.

Version history

Version	Date	Amendments
1.0	Initial published version	Initial version

MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT
HĪKINA WHAKATUTUKI

ACCREDITATION

To participate fully in CDR, a service provider must be an accredited party under the CDR Rules. Data holders must provide an accredited party data and enable actions only at the request and with the consent of the consumer.

To receive CDR data or enable payment actions, a provider must be accredited by the CDR Accreditor (the Ministry of Business Innovation and Employment). Anyone seeking to be accredited must apply, and the Accreditor will grant accreditation if it is satisfied that the applicant meets the criteria specified.

There are 4 classes of accreditation:

- Non-intermediary - Data
- Non-intermediary - Payments
- Intermediary - Data
- Intermediary - Payment

To maintain their accreditation, an accredited person must:

- Only use data for the purpose agreed by the customer
- Keep customer data safe and secure
- Follow all rules under the Customer and Product Data Act 2025 and related regulations
- Maintain clear complaints processes and respond promptly to issues
- Throughout their active accredited period, report any changes to their position as it relates to accreditation criteria that may impact their accreditation status or class.

APPLICATION PROCESS

To apply for one or more accreditation classes, the applicant will apply via the online form. Access to the online form requires a RealMe login (refer here RealMe® | New Zealand Government for more information), and a subsequent Business Connect account which will enable the applicant to save a draft for completion over time before submitting.

We recommend that supporting documents are prepared ahead of time. The list of supporting documents can be referenced in Appendix 1.

Step 1: Assign an authorised representative to complete the application. This person will be the main business contact throughout the application process.

Step 2: Click on the link to the application form and login via RealMe (alternatively create a login if required).

Step 3: On your first access you will be prompted to create a Business Connect account.

Step 4: Select the "Consumer Data Right Accreditation" tile on the dashboard

Step 5: You can begin your application. You can save the application as a draft along the way.

Step 6: Ensure you have completed all relevant questions before submitting.

Step 7: Once you submit this will be placed in our processing queue.

Step 8: Pay the application fee invoice - you will receive an invoice for payment to the billing contact details provided in your application. The only current method is to pay via direct credit/internet banking (this will be amended in the future). Be sure to provide the applicant name and the application number on your payment details.

RELATED APPLICATIONS

An applicant may wish to have two or more related applications (for example, applications by related limited companies) considered by the Accreditor at the same time. This can be noted at the end of the accreditation application form. When an applicant wishes to have multiple applications assessed simultaneously, the Accreditor may be able to consider certain information in support of more than one application. We encourage applicants to discuss the types of information they can use to support related applications with us before submitting their application.

COMPLETENESS CHECK

Before assessing an application, we check whether it is complete. An application is incomplete when required fields on the form have not been answered or required documents are missing. We cannot assess incomplete applications. If the application is incomplete, we will notify the applicant, indicating where missing information is required. The applicant will be given the opportunity to complete the relevant section of the application and resubmit it.

AMENDING AN APPLICATION

Once an applicant has submitted their application, they cannot directly amend it. If the applicant is wishing to amend the application contact our processing team at consumerdataright@mbie.govt.nz.

MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT
HĪKINA WHAKATUTUKI

WITHDRAWING AN APPLICATION

An applicant can withdraw their application at any stage of the application process. To withdraw an application after it has been submitted contact the team at consumerdataright@mbie.govt.nz.

FURTHER INFORMATION AND CONSULTATION

If the application is complete but the Accreditor needs further information before deciding whether to grant accreditation, the Accreditor may:

- request additional information from the applicant
- consult with New Zealand Government authorities such as the Companies Office, Office of the Privacy Commissioner, Financial Markets Authority, or similar authorities overseas

ACCREDITATION DECISION

If the Accreditor decides to grant accreditation, they will notify the applicant of this in writing. If the Accreditor decides not to grant accreditation, they will advise the applicant in writing and provide information about the applicant's rights to have the decision reviewed.

COMMENCEMENT OF ACCREDITATION

Accreditation takes effect when the Accreditor's decision to accredit the applicant is recorded in the Register of Participants. The Accreditor will also inform designated data-holders of the newly accredited party.

The accredited party will then be guided to contact the data holders to begin the onboarding process before they can start actively participating in CDR.

ONBOARDING

Newly accredited persons must go through an on-boarding process with each data holder before they can actively participate in CDR with that data holder. As part of this process, they may need to successfully complete testing and meet other requirements of the data holders. The Accreditor will provide information on how to engage in the process at the point of accreditation.

DURATION OF ACCREDITATION AND RENEWAL

An accredited requestor's accreditation starts when the accreditation is registered and ends when the accreditation is removed from the register.

Accreditation is granted for a period of 12 months. An accredited requestor may apply to renew its accreditation. If a renewal application is made on or before the date of expiry of an accredited requestor's accreditation, the accreditation continues to have effect until the renewal application is decided by the Accreditor.

If the accredited requestor's accreditation expires before a renewal application is made, instead of a renewal application, the accredited requestor must make a fresh accreditation application.

If an accredited requestor no longer wishes to be accredited, they may apply to the Accreditor to surrender accreditation. Requests to surrender accreditation must be in writing. An accredited person can do this by submitting a request through to consumerdataright@mbie.govt.nz. The Accreditor will advise the person in writing that their application to surrender accreditation has been accepted.

FEES AND LEVIES

Fees

Fees for submission of an application are as follows:

	Application to become accredited	**Application to renew accreditation**
Intermediary	$2,000	$1,700
Non-intermediary	$1,500	$1,000

If you are applying for both non-intermediary and intermediary classes in one application, only one fee is payable (the higher fee applies).

Fees will be payable on receipt of the invoice which will be emailed to the billing contact provided. Once payment is received the Consumer Data Right team will begin processing your application.

Levies

Accredited requestors must also pay a levy. For accredited requestors, this levy will only be payable at the time of accreditation renewal and will be based on the total gross annual revenue of the accredited requestor and its interconnected bodies corporate. The levies are outlined below:

Accredited Requestor	**Levy**
Annual revenue exceeding $100 million	$85,000
Annual revenue between $10 million and $100 million	$32,000
Annual revenue between $1 million and $10 million	$10,000

Annual revenue not exceeding $1 million	$1,300

ACCREDITATION CRITERIA

Organisation and Product Information

An applicant will be asked to provide information on the applicants' ownership structure, and also details about the product/service offering that will be offered.

Fit and proper person

An applicant must be a fit and proper person to manage CDR data. When assessing an application against this criterion, the Accreditor will consider whether the applicant or an associated Senior Manager/Director been or currently is the subject of the following:

- criminal investigation
- investigation or disciplinary action by a professional body
- inquiry or investigation by a government agency
- court proceedings initiated by a government agency.

The Accreditor will undertake relevant checks to verify an applicant's answers relating to the fit and proper person criterion. This includes the request for criminal background checks.

In this context a "Senior Manager" means a person who is not a Director but occupies a position that allows that person to exercise significant influence over the management or administration of the applicant (for example, a chief executive or a chief financial officer).

Information security

To protect consumer data applicants must take steps to protect CDR data from misuse, interference, loss, unauthorised access, modification or disclosure. When applying for accreditation, an applicant must provide evidence to show that it is able to take these steps.

If the applicant has a relevant security certification e.g. ISO27001. This can be used as evidence to support the questions asked. Examples of supporting evidence that it required for those without a certification are summarised in Appendix 1.

Dispute Resolution

Internal dispute resolution: Applicants must have IDR processes and provide details of this process within the application, including where information can be found on this for publishing on the Register of Participants.

External dispute resolution: an applicant is required to be a member of an external dispute resolution scheme only if the applicant is required to be registered under the Financial Service Providers (Registration and Dispute Resolution) Act 2008, and the applicant is registered under that Act.

Insurance

As per the regulations, applicants for accreditation as a data requestor must have one of the following in order to cover liabilities in the case of a breach:

1. A contract of insurance; or
2. a contract of guarantee; or
3. an arrangement maintained by the applicant to set aside financial resources to cover a potential liability

Evidence of cover will be required to support the assessment and determination on whether it is adequate as required by the regulations. Also to support this will be a signed representative statement that summarises the cover and why it is deemed to be adequate.

Intermediaries

Additional requirements are imposed on those acting as an intermediary (i.e. those wanting to make requests under section 15 and/or section 19 of the Act). Primarily these requirements are for ensuring adequate due diligence measures are in place for engaging with 4th parties to whom data requests will be fulfilled. Evidence is required for the Accreditor to be satisfied that appropriate measures are in place.

MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT
HĪKINA WHAKATUTUKI

APPENDIX 1: REQUIRED DOCUMENTATION/EVIDENCE

To assist in your preparation, listed below are the documents you will be asked to provide in support of your application (some are conditional based on your answers to questions provided). For Security this evidence is suggested as examples to prove the relevant controls that are in place.

SECTION	DOCUMENT/EVIDENCE
Organisation and Product Information	- Financial statement from last financial year (or latest draft) - Worked example of how an individual customer/business would use the applicants product/service - Evidence of customer consenting process
Fit and Proper Person	- All Senior Managers and Directors will be required to complete an criminal history check and email through to the Consumer Data Right team (this is not an upload in the application form).
Security	- If you have a form of security certification (e.g. ISO270001), a copy of this certification and/or a latest audit report will be required. You will not need additional evidence if you can show how your certification covers each area. The following is **suggested examples** of evidence to be provided under each sub-section if this is not covered by a certification. Security awareness: - Approved policy and training plan (version/date) - LMS completion reports for last 12 months; onboarding checklist samples - Role-based training materials; sign-off records - Communications (emails, intranet posts) and acknowledgement receipts - Management dashboards/minutes summarising awareness metrics Risk Management: - Risk policy/methodology - Risk appetite statement - Enterprise risk register export with cyber entries - Risk owner assignments; review logs; treatment status reports - Threat intel advisories and resulting risk updates - Supplier risk assessments; contracts with security clauses

SECTION	DOCUMENT/EVIDENCE
	Asset and their Importance: - CMDB/inventory export with ownership - Classification & labelling standard; sample labels - Owner appointment letters; RACI charts - Lifecycle policy; EOS register; disposal certificates - Procurement workflow with security checkpoints Secure Configuration of Software - Baseline standards (CIS/NZISM references) - Build validation checklists; golive signoffs - Change tickets; CAB minutes; rollback plans - Config audit reports; drift detection outputs - SDLC artefacts: threat models, code reviews, security test reports Patching: - Patch policy and SLA table - Scanner reports; exploit advisories - Test plans; approvals; change tickets - Rollback procedures; failure logs - Compliance dashboards; EOS/upgrade plans Multi-factor Authentication: - MFA policy; control scope list - IdP/SSO config export; conditional access policies - SIEM log extracts for MFA events; review tickets - Authenticator inventory; issuance/revocation logs - SaaS admin screenshots/config reports Detect Unusual Behaviour - SIEM/Log platform configuration; retention settings - Baseline documents; utilisation trend reports - Usecase library; correlation rules; alert samples - Triage/runbooks; incident tickets; SLA metrics - Control configs (lockout policies) Least Privilege - RBAC matrices; entitlement catalogue - PAM/JIT logs; privilege elevation requests - Endpoint admin exceptions register; approvals - Account register; quarterly attestation reports

SECTION	DOCUMENT/EVIDENCE
	- Privileged access monitoring dashboards; review minutes Data Recovery - RPO/RTO register; BIA outputs - Backup policies; job configurations; encryption settings - Test logs/reports; remediation actions; signoffs - Training records; DRP playbooks; role assignments - Budget line items; contracts/licences Response Planning - IR plan; playbooks; approval dates - Role matrices; contact trees; comms templates - Exercise reports; improvement trackers - Categorisation/severity model; activation records - Logging coverage reports; chainofcustody procedures Restrict Service Accounts - Service account policy and standards - Account configurations/screenshots (noninteractive; denied login) - Vault rotation logs; inventory with owners - SIEM dashboards reviewing service account activity Password Policies - Password policy; IdP enforcement settings - Hashing/vault configurations; key management docs - Helpdesk/reset logs; MFA reset procedures - Build checklists removing defaults; audit reports Network Security Enforcement - Network zoning diagrams; ACLs/security groups - Firewall baseline and audit results - NDR/SIEM detections; lateral movement playbooks - VPN/MFA configs; device posture enforcement End User Device Management - MDM/EDR policies; baseline profiles; encryption status reports - Local admin exception register; approvals - Endpoint patch compliance reports - Device inventory exports; reconciliation logs Data Segregation

SECTION	DOCUMENT/EVIDENCE
	- Data classification scheme; architecture diagrams - SaaS segregation tests/attestations - Access control matrices; encryption configs Data Loss Prevention - DLP policy set; rule library; tuning records - Incident tickets; metrics; reports to management - Data classification mappings used by DLP Antimalware/Antivirus - EDR deployment reports; policy configs - Update compliance dashboards - IR playbooks; incident records; containment timelines Content Filtering - Web/DNS filtering configs; policy reports - Email security configs; DMARC reports; sandbox logs - Review minutes; change logs for lists Non-production data use: - Policy; standards for masking/tokenisation - Nonprod configs; segregation diagrams - Audit logs showing no raw prod data in nonprod Data Lifecycle Management: - Retention schedules; legal holds; records policy - Deletion/archival logs; disposal certificates - Backup/DR integration docs; testing reports Human Resource Security: - Human Resource Security Policies and Standards Data Encryption - Data Encryption Configurations and Algorithm Standards Privacy - Privacy policy - Privacy statement
Insurance	Evidence depends on the liability cover type selected: Contract of Insurance: - Certificate of insurance; - Insurance policy document; - Signed authorised representative statement

SECTION	DOCUMENT/EVIDENCE
	Contract of Guarantee - Evidence of guarantee (signed by Guarantor) - Signed authorised representative statement Financial resource arrangement - Evidence of financial resource arrangement - Signed authorised representative statement
Customer Dispute Resolution	- Documented internal dispute resolution process
Intermediaries (if this section is relevant for your application)	- Evidence of your due diligence process performed on 4th parties