Australian Government

Consumer Data Right

Compliance Guide for Data Holders

Banking sector

Version 2
June 2022

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.

Guidance Revision History

Version 2 of this Guide, published in June 2022, includes the following changes that have been made since the Guide was first published in April 2021:

- Updated references to CDR Rules and Standards where these have changed since the previous publication.
- Removal of references to commencement dates that have since passed.
- New text clarifying whether a service for nominating or withdrawing a secondary user instruction should be provided online or offline (section 4.6.2)
- New text detailing the obligations of reciprocal data holders (section 4.7)
- Revised text on joint account obligations to align with the joint account provisions from v3 of the CDR Rules (sections 4.9 and 4.10)
- Revised text on internal dispute resolution to reflect that ASIC Regulatory Guide 271 is now the applicable guide for internal dispute resolution under the CDR Rules (section 5.1).

1. Background

1.1. The Consumer Data Right

The Consumer Data Right (CDR) aims to give consumers more access to and control over their personal data. Being able to easily and efficiently share data improves a consumer's ability to compare and switch between products and services, and encourages competition between service providers, leading to more innovative products and services for consumers and the potential for lower prices. The CDR has already been rolled out to the banking sector, with energy following as the second sector.

Data holders four main roles under the CDR:

- providing the necessary CDR infrastructure to enable requests to be made for product and consumer data, including joint account data,
- disclosing general product data about products they offer, covering interest rates, fees and charges, discounts and other features,
- securely transferring, with a consumer's authorisation, a consumer's data in a machine-readable format when they receive a valid request, and
- managing a consumer's authorisation to disclose CDR data and any amendment or withdrawal of that authorisation.

In doing these things, data holders need to meet legal and technical requirements.

A glossary of common terms is published on the CDR Support Portal.

1.1.1. Regulatory framework

The CDR is regulated by a framework that consists of:

- legislation including the *Competition and Consumer Act 2010* (CCA), *Privacy Act 1988* and the *Australian Information Commissioner Act 2010*
    - the core legislative provisions are contained in Part IVD of the CCA, including provisions under which the CDR rules and standards are made, and the role of the Data Recipient Accreditor and the Accreditation Registrar is set out
- designation instruments made under the legislation, including the *Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019*, which designates the banking sector as subject to the CDR
- the *Competition and Consumer (Consumer Data Right) Rules 2020* made under the legislation (CDR Rules)
    - You can find the most recent version of the CDR Rules on the Federal Register of Legislation.
- Consumer Data Standards (Standards), which include technical and Consumer Experience Standards (CX Standards). The CX Standards contain technical requirements for what data holders need to do in their consumer facing interactions. More information about the Standards is set out below.

1.1.2. Using this guide

The CCA, CDR Rules and Standards impose a range of requirements that data holders, accredited data recipients and other participating entities (for example, outsourced service providers and CDR representatives) must comply with.

The focus of this guide is on the obligations for data holders arising under the CDR Rules and Standards in relation to the Banking sector only.

The Australian Information Commissioner (OAIC) has certain privacy-related regulatory responsibilities under the CDR regime, in particular the enforcement of the Privacy Safeguards under Part IVD of the Act. Some of these safeguards impose obligations upon data holders. Data holders should read this guide alongside guidance issued by the OAIC: Guide to privacy for data holders and the CDR Privacy Safeguard Guidelines.

This guide is limited to data holder obligations after registration and on-boarding have been completed. At section 4.3 of this guide there are links to information about registration and on-boarding.

Some data holders may be an accredited data recipient in addition to being a data holder. Accredited data recipient status imposes separate and additional obligations that are not covered in this guide.

This guide is current as at the date of publication. The CDR operates in a dynamic regulatory framework and users of this guide should ensure they refer to the current versions of the CCA, the CDR Rules, Standards and other compliance guidance material referred to throughout this guide.

This guide contains general information only. It is not legal advice and is not a comprehensive or exhaustive statement of all the obligations data holders need to comply with under the CDR, or of all the potential consequences of non-compliance. Please see the *Important Notice* at the start of this guide.

1.1.3. The CDR agencies

The CDR is a dual-regulator model, with the ACCC and the OAIC responsible for jointly monitoring compliance. In the CDR regime the ACCC seeks to promote competition and the OAIC aims to protect privacy and confidentiality. Consumer focused outcomes are paramount for both regulators. We work together to jointly monitor compliance with the CDR regulatory framework, respond to issues and pursue enforcement activity if necessary.

The Treasury leads CDR policy and is responsible for the development of CDR Rules and for advice to government on which sectors the CDR should apply to in the future. The relevant Minister is responsible for designation of sectors and making of CDR Rules.

Within Treasury, the Data Standards Body (DSB) develops the Standards that prescribe the technical requirements for how data is shared under the CDR.

1.1.4. Compliance and Enforcement Policy

The ACCC and OAIC have developed a Compliance and Enforcement Policy. This Policy aims to help data holders and accredited persons (CDR participants) and consumers to understand the approach the regulators will adopt to encourage compliance and prevent breaches of the CDR regulatory framework.

We use a risk-based approach to monitoring and assessing compliance matters and taking enforcement action. We cannot pursue all matters that come to our attention. Our role is to focus on those circumstances that will, or have the potential to, cause significant harm to the CDR regime or result in widespread consumer detriment.

1.1.5. Data holders

Under the CDR regime, in the banking sector, a data holder is an Authorised Deposit-taking Institution (ADI) or an accredited data recipient that holds CDR data about:

- a banking product[1];
- the consumer of a banking product; or
- a consumer's use of a banking product.

Authorised Deposit-taking Institutions (ADIs)

The four major banks (Australia and New Zealand Banking Group Limited, Commonwealth Bank of Australia, National Australia Bank Limited and Westpac Banking Corporation) are identified in the CDR Rules as 'initial data holders'. Initial data holders commenced sharing CDR data earlier than other ADIs.

All remaining ADIs that are not an accredited data recipient, foreign ADIs, foreign branches of domestic banks or restricted ADIs are categorised as 'any other relevant ADI' for the purposes of the commencement of CDR obligations. We refer to this group as 'all other ADIs' in this guide.

Accredited data recipients

Accredited data recipients are required to share CDR data, in accordance with reciprocal data sharing obligations, where that CDR data is generated and held by or on behalf of the CDR consumer. This includes data from publicly offered products such as transaction accounts (see clause 1.4 of Schedule 3 of the CDR Rules for the full list of products).

If an accredited data recipient holds this kind of CDR data, it will be required to share this data at the request of a CDR consumer as of the dates set out in the CDR Rules (see the commencement table at clause 6.6 of Schedule 3 with respect to 'reciprocal data holders'). In certain circumstances, an accredited data recipient may become a data holder of data that it has received under the CDR Rules (see clause 7.2 of Schedule 3). See section 4.7 of this guide for further information about reciprocity.

1.1.6. Data Holder obligations under the CDR

Under the CDR, subject to particular specified commencement dates, data holders are required to:

- disclose product data
- disclose consumer data
- establish dispute resolution services
- keep appropriate records
- report at scheduled intervals, and
- comply with the relevant Privacy Safeguards.

[1] In this context 'banking product' means one of the products that is listed in sch 3, cl 1.4 of the CDR Rules.

1.1.7. Exemptions under section 56GD of the CCA

CDR participants can seek exemptions from complying with their obligations under the CDR, for example in relation to a particular product line. Where an exemption is sought, the ACCC will assess each on a case-by-case basis, having regard to the facts and circumstances relevant to the particular entity and the exemption being sought.

The exemption register lists all exemptions granted by the ACCC and the Guidance for applicants seeking an exemption under section 56GD provides more information about how to apply for an exemption and when an exemption might be appropriate.

2. Data holders' obligations under the Standards

The CDR Rules set out specific obligations for disclosing data including to act in accordance with the relevant Standards.

The CDR Rules and the CCA require the making of standards including for the format and process by which data holders must respond to requests for CDR data made by accredited data recipients and the processes for obtaining consumer authorisation to disclose CDR data. The full list is set out in rule 8.11 of the CDR Rules.

The obligations on CDR participants to apply the Standards work in two ways:

- where the CDR Rules require compliance with the Standards, non-compliance with the Standards may constitute a breach of the CDR Rules, and
- where the Standards are specified as binding standards under the CDR Rules for the purposes of section 56FA of the CCA, they apply as under a contract between a data holder and an accredited data recipient. The legal effect of binding standards as between data holders and accredited data recipients is set out in sections 56FD and 56FE of the CCA.

The Standards are made by the Data Standards Chair with the assistance of the DSB. The current version of the Standards is available here. The Standards are a 'living' document and are regularly revised to adapt to changing demands for functionality and available technological solutions.

Data holders should ensure they are consulting the current version of the Standards. Further information on understanding what has changed when a new version of the Standards is released is available on the CDR Support Portal. If there is an inconsistency between the Standards and the CDR Rules, the CDR Rules prevail to the extent of any inconsistency.

General overview of the Standards

Security requirements	
Security profile	Sets out the security specifications that data holders must implement to facilitate data sharing with accredited data recipients. These specifications must be implemented by a data holder.
Receiving and responding to CDR data requests	
Standards	Contains high level standards that govern the Standards as a whole. These high level standards apply to all CDR participants.

Industry Specific Application Programming Interfaces (APIs)[2]	Sets out API end point specifications - such as methods, paths and schemas - which allow an accredited data recipient to request data from a data holder. These APIs are categorised according to the industry that they are applicable to. For instance, 'Banking APIs' are applicable to the banking sector and 'Common APIs' are applicable to multiple sectors. There are also APIs related to 'Dynamic Client Registration' (DCR APIs), which is the process used by accredited data recipients and data holders for obtaining credentials about one another and is a prerequisite for consumer data sharing to occur.
Authorisation scopes	Sets out the level of authority the accredited data recipient has in accessing the consumer's data. The Banking APIs specify which authorisation scope is applicable to each type of data request.
CDR consumer-facing interactions	
Consumer Experience (CX) Standards	Sets out what data holders must do in their direct interactions with consumers, including setting out what a data holder must do when seeking a consumer's authorisation and how it must communicate when a consumer wishes to withdraw an authorisation.
Reporting	
Admin APIs	Allows the ACCC to obtain operational statistics from data holders on the operation of their CDR compliant implementation. These standards also set out how a data holder must respond to such requests from the ACCC.
Service and performance levels	
Non-functional requirements	Sets out a range of performance and service level requirements data holders are expected to meet in delivering their CDR solution. For example, minimum CDR platform availability and performance levels.

2.1. References to the Standards in this Guide

This guide contains references to aspects of the Standards throughout.

These references are:

- included to point out aspects of the Standards that are relevant to the compliance obligations being described in this guide
- noted by way of general guidance only, to assist data holders to comply with the CDR Rules and the Standards
- mentioned at a high level of generality, for example, by referencing the section heading that appears in the Standards, because changes to the content of the Standards are anticipated.

[2] APIs are the technology behind the data transfer process in the CDR and allow data to be transferred electronically and automatically.

This guide does not include a comprehensive statement of all the Standards that may be relevant to a data holder's compliance with a particular obligation. A reference to one aspect of the Standards does not mean that is the only aspect a data holder must comply with in respect of the relevant obligation.

References to aspects of the Standards throughout this guide are in the following format:

Standards: whether the relevant Standard is a technical standard or CX Standard, and/or **CX Guidelines**: whether there is a relevant CX Guideline.	**Section:** the relevant content heading within the Standard.	**Sub-section:** relevant content sub-headings within the Standard and contextual information.
For example:		
Standards	Banking APIs	Get Products
CX Standards	Consent, Authentication and Authorise Standards	Authentication – 'One Time Password'

The headings and sub-headings indicated can be used to navigate to the sections of the Standards being referred to.

2.2. Understanding the obligations contained in the Standards

Language used to describe obligations

Different types of obligations are signified in the Standards by using uppercase words such as: "MUST", "SHOULD" and "MAY".

For example, the Security Profile section of the Standards provides:

- Refresh tokens MUST be supported by data holders.
- Data holders MAY cycle Refresh Tokens when an Access Token is issued.

Uppercase terms in the Standards (MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY and OPTIONAL) should be interpreted in accordance with RFC 2119.

For example, if a Standard states that a data holder "SHOULD" do something:

- RFC 2119 provides that "SHOULD" or "RECOMMENDED" mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- As a matter of compliance and enforcement policy, the ACCC expects that binding Standards stating a data holder "SHOULD" do something apply except in the circumstances provided for in RFC 2119.

Mandatory, optional and conditional fields

When describing API payload schemas, the Standards also contain requirements for individual data fields that are expressed as "mandatory", "optional" and "conditional".

"Optional" payload fields are not the same as obligations that a data holder "MAY" or "SHOULD" adhere to or an obligation that is described as "OPTIONAL" under the RFC 2119 interpretation.

- **Mandatory fields** MUST be present and have a non-null value in a request or response payload for the payload to be considered valid. Where the Standard has a mandatory field, data holders are required to share that field; but where they do not have the data it must be represented as a default or empty value as applicable.
- **Optional fields** MAY be present, and it is also valid for these fields to be present but to have a null value. Optional fields indicate that data may sometimes not be held by a data holder, and this is an expected scenario. Optional fields are not considered optionally implementable by a data holder, but optional in this context refers to the following:
    - If a data holder holds optional data, it must be provided.
    - If a data holder does not hold optional data, a null value may be provided for the optional field, or the field can be excluded entirely in the response.
    - If any optional field is not held in a form that can be translated into the Standards, then it should be considered not held and a null value should be returned (or the field left out of the payload).

Conditional fields are mandatory in circumstances defined by the Standards. If the statement is true in a specific request or response the field is considered mandatory. If the conditional statement is false, then the field is considered optional.

Normative Standards

The Standards, particularly the Security Profile, refer to foundational standards as normative. These normative standards, as specifically referenced in the Standards, are considered binding to the same degree as the Standards themselves.

2.3. Consumer Experience (CX) Guidelines

The CX Guidelines are in addition to CX Standards. The CX Guidelines are not enforceable in the same way as Standards. However, the CDR Rules require that a data holder's processes for asking a CDR consumer to give an authorisation must, having regard to the CX Guidelines, be as easy to understand as practicable, including by use of concise language and where appropriate, visual aids (see rule 4.22(b) of the CDR Rules). Data holders therefore should use the CX Guidelines as a model approach for guiding a CDR consumer through authentication, authorisation, and dashboards.

The CX Guidelines demonstrate how to apply various CDR requirements and recommendations and provide guidance in relation to the Consent Model aspect of the CDR framework.

References to the CX Guidelines in this guide are by way of general guidance only and are not a comprehensive statement of all CX Guidelines that may be relevant to a particular obligation.

Data holders should consult the current version of the CX Guidelines.

2.4. Other guidance material

Further resources regarding the Standards and CX Guidelines are included in the table on the following page.

Standards and guidelines resources

Resource	Description
CDR Support Portal	The CDR Support Portal publishes guides on technical and compliance-related matters.
Conventions	The DSB supplements the Standards with conventions, which document broadly accepted interpretations of the Standards but do not impose compliance obligations. Conventions are published on the CDR Support Portal. CDR community members can request a convention by raising an issue in the CDR GitHub standards maintenance repository. For more information about the development of conventions, see the relevant convention articles.
Consumer Experience (CX) Checklist	The CX Checklist is a complete list of items referenced in the CX Guidelines including relevant rules, privacy safeguards, and data standards (CX and technical). This list has been created for the purposes of assisting implementation and compliance but should not be seen as a complete list of CDR Participant obligations.
Standards Consultation	The DSB conducts consultation on the Standards through GitHub. Decision Proposals and Noting Papers are typically published here for consultation.
Standards Maintenance	Change requests to the Standards published by the DSB can be made via GitHub. Standards maintenance is also conducted and change proposals are publicly consulted on.

3. Product data

3.1. What product data must be disclosed?

To comply with the CDR, data holders need to make specified information about their products available through an online request service. Please see section 3.3 of this guide for what product information is required and what may voluntarily be provided.

This obligation applies to:

- Products that are 'publicly offered'. A product will generally be considered publicly offered if it is available to customers, or a group of eligible customers. Most banking products available to consumers will be publicly offered products. In particular, if the product is available to customers as a 'standard form contract' that involves only low levels of negotiation (for example, in relation to interest rates or fees) then it is very likely to be publicly offered and within scope for the CDR. A product does not have to be available to any member of the public to be considered publicly offered – products may be subject to eligibility requirements. Further guidance on determining whether a product is in or out of scope for the CDR is available on the CDR Support Portal.
- Publicly offered products where the data is held in digital form even if the product is not available online.
- Products branded by an ADI but distributed to consumers via alternative channels (known as 'white labelled' products). See sections 3.7 and 4.5 of this guide for additional information on white labelled products.

3.2. Product data request service

CDR Rules: see rule 1.12

Data holders must provide an online service that:

- can be used to make product data requests;
- discloses data in machine-readable form; and
- conforms with the Standards.

CDR Standards:

Standards	Banking APIs	Get Products, Get Product Detail and related payload schemas
Standards	Standards	Versioning; Uniform Resource Indicator Structure; HTTP Headers; HTTP Response Codes; Payload Conventions; Common Field Types; Pagination; ID Permanence; Extensibility
Standards	Security Profile	Transaction Security, Cross-origin Resource Sharing
Standards	Non-functional Requirements	Non-functional requirements specifically applicable to public (or unauthenticated) APIs

3.3. Required product data and voluntary product data

CDR Rules: see Schedule 3, Part 3

Product data is divided into 'required product data' and 'voluntary product data'.

Required product data	Voluntary product data
Is CDR data that: • does not relate to a particular consumer(s) • identifies or describes the characteristics of a product • is about the eligibility criteria, terms and conditions, features, benefits, price, availability or performance of a product • is publicly available (for data about availability or performance), and • is held in a digital form in a format compatible with sharing under the Standards for example, data held only in a PDF would not need to be shared.	Is all other CDR data that: • does not relate to a particular consumer(s) • identifies or describes the characteristics of a product, and • is about the eligibility criteria, terms and conditions, features, benefits, price, availability or performance of a product.
Voluntary and required product data are not the same as the data fields shown as "mandatory" and "optional" in the Standards. Required product data and voluntary product data refer to data clusters to be disclosed on receipt of a valid request, as defined above. Mandatory and optional data fields referred to in the Standards relate to the parameters for the APIs used to request and disclose CDR data (see Section 2.2 of this guide).	

3.4. Requests for required product data

CDR Rules: see rules 2.3 and 2.4

If a person requests required product data through a data holder's product data request service:

- a data holder must disclose the data
  - this includes any data on the data holder's website or in a product disclosure statement, key fact sheet or similar document that is relevant to the request
- the data must be disclosed using the data holder's product data request service
- a data holder cannot charge a fee for providing the data
- the data must be disclosed in accordance with the Standards.

See CDR Standards:

Standards	Banking APIs	Get Products, Get Product Detail and related payload schemas
Standards	Standards	Versioning; Uniform Resource Indicator Structure; HTTP Headers; HTTP Response Codes; Payload Conventions; Common Field Types; Pagination; ID Permanence; Extensibility
Standards	Security Profile	Transaction Security, Cross-origin Resource Sharing
Standards	Non-functional Requirements	Non-functional requirements specifically applicable to public (or unauthenticated) APIs

A data holder may refuse to disclose the requested data (required product data) in response to a request in circumstances set out in the Standards (if any) and must inform the requester of such a refusal, in accordance with the Standards *(*see rule 2.5*)*.

Examples of such circumstances include:

- When the number of requests the data holder is receiving is above their service level thresholds defined in the non-functional requirements section of the Standards.
- When there is a valid security reason that prevents sharing product data temporarily or for requests considered as suspicious.

A 'refusal to disclose' should be taken to mean that the data holder has received a valid request, but the data holder, for one of a variety of reasons (for example, traffic thresholds in the Standards have been exceeded or the data holder considers there to be a real security risk to their system) does not disclose the data.

See CDR Standards:

Standards	Standards	HTTP Response Codes – HTTP Status: 429 Too Many Requests
Standards	Non-functional Requirements	Exemptions to Protect Service

3.5. Requests for voluntary product data

CDR Rules: see rule 2.4

If a person requests voluntary product data through a data holder's product data request service:

- a data holder may disclose the data
- the data must be disclosed using the data holder's product data request service
- a data holder can charge a fee for providing the data, but the fee should be reasonable (see s 56BV CCA)
- the data must be disclosed in accordance with the Standards.

See CDR Standards:

Standards	Schemas	*As relevant to the product data request*

3.6. Limitations on use of disclosed data

CDR Rules: see rule 2.6

The data holder must not impose conditions or restrictions on the use of the disclosed data by the recipient.

3.7. Who is responsible for disclosing white label product data?

CDR Rules: see rule 2.4(4)

White label products are products typically supplied by one entity (the 'white labeller') and retailed to consumers by another entity (the 'brand owner').

Where there is a single data holder for a white label product (whether that is the white labeller or the brand owner) in partnership with a non-data holder, that data holder is required to respond to product data requests in relation to the product.

Where there are two data holders for a white label product (for example, where a brand owner bank distributes a credit card on behalf of a supplying bank and both entities hold data):

- the data holder that has the contractual relationship with the consumer is required to respond to product data requests
- unless the data holders have agreed in writing that the other data holder will respond to product data requests.

White label products are subject to the same phasing timeline as all other products.

Further guidance on the disclosure of product data for white labelled products is available on the CDR website.

The approach to sharing consumer data for white label products is outlined in section 4.5 of this guide.

4. Consumer data

4.1. Who is an eligible CDR consumer?

CDR Rules: see rule 1.10B and Schedule 3, clause 2.1

Under the CDR Rules, data holders are required to enable sharing of required consumer data for eligible CDR consumers. For the banking sector, a CDR consumer is 'eligible' if:

- they are an account holder or secondary user for an open account with the data holder
- that account is set up so it can be accessed online; and
- they are:
    - an individual who is 18 years of age or over
    - a person who is not an individual (for example, a corporation), or
    - a partner in a partnership.

4.2. When do obligations commence?

CDR Rules: see Schedule 3, Part 6

To comply with the CDR, data holders need to share specified consumer data with an accredited data recipient if a consumer requests and authorises this to occur. As of 1 February 2022, all products listed in the below table are in-scope for the CDR and data holders must share consumer data relating to these products, subject to the limited exemptions in section 4.2.1. of this guide. These products are also known as Phase 1, Phase 2 and Phase 3 products based on the phasing in of banking products into the CDR over time.

In scope CDR products in the banking sector

- a savings account
- a call account
- a term deposit
- a current account
- a cheque account
- a debit card account
- a transaction account
- a personal basic account
- a GST or tax account
- a personal credit or charge card account
- a business credit or charge card account.
- a residential home loan
- a home loan for an investment property
- a mortgage offset account
- a personal loan
- the following account types and data for phase 1 products:
    - joint accounts
    - closed accounts
    - direct debits
    - scheduled payments
    - payees
    - 'get account detail' or 'get customer detail' data.
- business finance
- a loan for an investment
- a line of credit (personal or business)
- an overdraft (personal or business)
- asset finance (including leases)
- a cash management account
- a farm management account
- a pensioner deeming account
- a retirement savings account
- a trust account
- a foreign currency account
- a consumer lease.

The timetable for the obligation to disclose consumer data in response to direct requests from CDR consumers (Part 3 of the CDR Rules) has not commenced.

4.2.1. Non-individuals, partnerships, nominated representatives and secondary users

There is a different timeframe for enabling consumer data sharing for non-individual consumers (including corporations), business partnerships, and secondary account users (for example, individuals that have account privileges with an account held by another person) (see Schedule 3 clause 6.7 of the Rules).

- Major banks have been required to share consumer data for this group of consumers since 1 November 2021.
- Non-major banks are required to enable consumer data sharing for this group of consumers by 1 November 2022.
- Non-major banks and reciprocal data holders are also required to enable consumer data sharing on joint accounts by 1 October 2022 but may choose to commence sooner.[3]

4.3. Registration on the CDR participant portal

A data holder is required to be registered on the CDR Register to share CDR data in response to a request from an accredited person. Data holders will need to complete this registration process via the CDR participant portal. The registration and onboarding process is outlined on the CDR website here. The CDR participant portal User Guide provides further information about the portal and the registration process. Please read this guide together with the CDR participant on-boarding guide.

4.4. Required consumer data and voluntary consumer data

CDR Rules: see rules 4.6, 4.6A and 4.7, and Schedule 3 clause 3.2

A request can be made by an accredited person on behalf of a CDR consumer for required consumer data, voluntary consumer data, or both. In response, if the CDR consumer authorises the disclosure, the data holder must disclose any required consumer data to the accredited person who made the request, subject to rule 4.6A and rule 4.7 (see section 4.12 of this guide) and may (but is not required to) disclose the voluntary consumer data.

Required consumer data	Voluntary consumer data
CDR data that: • is dated after 1 January 2017 • is held in a digital form • relates to one or more CDR consumers And is either: • customer data in relation to a CDR consumer	CDR data that relates to one or more CDR consumers and is either: • data from a transaction that occurred more than 7 years ago • direct debit authorisations that occurred more than 13 months prior • direct debit authorisations on closed accounts • if an account was closed less than 2 years ago – transaction data from 12

[3] See *Competition and Consumer Amendment (Consumer Data Right Measures No. 1) Regulations 2022* (Cth) reg 28RB.

- account data in relation to an account held by a single CDR consumer, a joint account or a partnership account
- transaction data for such accounts, or
- product specific data in relation to a product a CDR consumer uses (for example, individually negotiated product prices or features).

months or more before the account was closed
- all account, transaction and product specific data on accounts closed more than 24 months ago, or
- any other data that is not required CDR data.

The following consumer data is not required or voluntary CDR consumer data:

- Account, transaction or product specific data for an account that is not held by a single person individual, a joint account or a partnership account.
- Account, transaction or product specific data for an account where any of the account holders are under 18.
- Customer data in relation to another account holder (on a joint or partnership account) or a secondary user.

4.4.1. Can consumers share data from offline accounts?

An eligible consumer can make data sharing requests to share data from their online accounts and they can also request to share data from other accounts they hold which are not available via online banking.

Data holders are required to share this data if it is held in a digital form in a format compatible with sharing under the Standards, even if it is not available to the consumer digitally. This includes account data about the offline account and product specific data (for example, interest rate and terms and conditions for the product the consumer uses).

4.5. Who is responsible for disclosing consumer data from white label products?

White label products are typically supplied by one entity (the 'white labeller') and branded and retailed to consumers by another entity (the 'brand owner'). Where there is a single data holder involved in providing a white label product (whether that is the white labeller or the brand owner), in partnership with a non-data holder, the data holder must comply with consumer data sharing obligations in relation to the product.

Where there are two data holders involved in providing a white label product (for example, where a brand owner bank distributes a credit card on behalf of a white labeller bank) the data holder that has the contractual relationship with the consumer is considered responsible for responding to consumer data requests, to avoid unnecessary duplication. The data holder that has the contractual relationship with the consumer (for example, the white labeller) may agree with the other data holder (for example, the brand owner) that the brand owner will perform that obligation on behalf of the white labeller. In this example, the white labeller, as the data holder that has the contractual relationship with the consumer, remains accountable for the performance of the obligation by the brand owner.

White labeller data holders must register their white label brands on the CDR Register. If two data holders are involved in providing a white label product and they have agreed that the brand owner will respond to data requests, then the brand owner will register the brand.

The ACCC understands that there are a wide variety of white label arrangements in the banking sector and that particularly complex arrangements could pose compliance issues. The ACCC is open to discussing these issues with data holders and considering potential exemption applications where a while labeller considers it is not able to comply with CDR obligations.

Please find below a list of further guidance on white label products:

- Disclosure of product data for white label products
- Disclosure of consumer data for white label products
- Brands in the Consumer Data Right Ecosystem
- ADI responsibility for Data Holder Brands
- White Labelled brands in the CDR
- Noting Paper 169 – White Label Conventions

4.6. Consumer data request service

CDR Rules: see rule 1.13

Data holders must provide an online service, known as an 'accredited person request service', that:

- can be used by accredited persons to make consumer data requests on behalf of eligible consumers
- discloses data in machine-readable form, and
- conforms with the Standards.

See CDR Standards:

Standards	Industry Specific APIs	All APIs definitions except those that are related to the product data request service
Standards	Standards	Versioning; Uniform Resource Indicator Structure; HTTP Headers; HTTP Response Codes; Payload Conventions; Common Field Types; Pagination; ID Permanence; Extensibility
Standards	Security Profile	The entire security profile is applicable
Standards	Non-functional Requirements	The majority of the non-functional requirements impact the consumer data request service

4.6.1. For non-individual and partnership consumers

Data holders are also required to provide a service (which can be an online service, but is not required to be) that can be used by non-individual consumers and business partnerships to nominate one or more individuals (known as 'nominated representatives') that can give, amend and manage authorisations on their behalf. The service must also allow these types of consumers to revoke such a nomination. More detailed guidance on nominated representatives and business consumers is available here.

4.6.2. For individual accounts with additional authorised users

CDR Rules: see rules 1.13 and 1.15

Rule 1.13(1)(e) requires a data holder to provide a service an account holder can use to make or withdraw a secondary user instruction. This service may be provided online or offline. Rule 1.13(1)(e) applies where a person has **account privileges**[4] in relation to an account.

Rule 1.15(5) requires the data holder to provide an online service to the account holder with a variety of functionality, including the ability to withdraw a secondary user instruction (rule 1.15(5)(b)(ii)). Rule 1.15(5) applies once there is a **secondary user** on an account (i.e. where a secondary user instruction is in place).

We encourage data holders to provide online functionality for making and withdrawing a secondary user instruction from the outset, in addition to any offline service that may be provided. Facilitating the withdrawal of a secondary user instruction through an online service will satisfy rule 1.13(1)(e)(ii) and rule 1.15(5)(b)(ii).

4.7. Reciprocal data holders

An accredited person may be considered a data holder with reciprocal obligations in respect of CDR data that it holds that was not disclosed to it under the CDR Rules (s 56AJ(3) of the CCA). If so, this means that an accredited person may be required as a 'reciprocal data holder' to share that data.

- For the banking sector, an accredited person will have reciprocal obligations as a data holder in respect of CDR data that is: generated and held by or on behalf of an accredited person; and
- where the data is generated in respect of a product that is publicly offered by the accredited person to consumers and generally known as one of the types of products in Phase 1, Phase 2 or Phase 3 products (clause 1.4 of Schedule 3).

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

4.8. CDR consumer dashboard

CDR Rules: see rule 1.15 and Schedule 3, clause 2.3

Data holders must provide a consumer dashboard that CDR consumers can use to manage authorisations to disclose CDR data to an accredited person on their behalf.

The consumer dashboard must also:

- include functionality that allows a consumer to withdraw authorisations to disclose CDR data at any time. This feature must be simple and straightforward to use, prominently displayed and no more complicated than the process for authorising the disclosure of CDR data. A message must be displayed as part of the withdrawal process, explaining the consequences of withdrawal in accordance with the Standards.

[4] A person has account privileges in relation to an account with a data holder if:

a) The account is for a phase 1, phase 2 or phase 3 product; and

b) The person is able to make transactions on the account.

See Schedule 3, clause 2.2 of the CDR Rules.

- contain the following details of each authorisation to disclose CDR data within the past six years:
    - details of the CDR data that has been authorised to be disclosed
    - when the consumer gave the authorisation and what period it was given for
    - when the authorisation is scheduled to expire/expired
    - details of any amendments that have been made to the authorisation
    - if CDR data has been disclosed – what data was disclosed, when it was disclosed and the accredited data recipient it was disclosed to (s*ee* Privacy Safeguard 10 - section 56EM of the CCA and rule 7.9 of the CDR Rules)
    - if the disclosure is of corrected data in response to a request to correct previously disclosed data this should be noted.

The data holder must update a consumer's dashboard as soon as practicable after changes to the information contained in the dashboard (see rule 4.27 of the CDR Rules).

4.8.1. For non-individuals and partnerships

Data holders must only allow nominated representatives to use the CDR consumer dashboard to manage authorisations on behalf of a non-individual or partnership.

4.8.2. For joint accounts

CDR Rules: see rule 4A.13

Data holders must provide all relevant account holders with a consumer dashboard for managing approvals to disclose CDR data in relation to their joint account.

- The consumer dashboard must meet the requirements for individual account dashboards outlined above.
- All joint account holders should be able to see the same details about each approval as the requesting account holder.

See CDR Standards:

CX Standards	Withdrawal standards	Withdrawing consent; Consequences; Redundant Data
CX Guidelines	Consent Management	
Standards	Security Profile	The arrangement revocation end point is to be used for the notification of revocation between parties. Note also the multiple statements related to the handling of expired or revoked tokens in the Security Profile

4.9. Joint accounts

Special rules apply to consumer data requests for CDR data from joint accounts. To be able to share joint account data, all joint account holders must be 'eligible' consumers in their own right. This means, for example, that if a relevant joint account holder does not have online access to any of their accounts, then the joint account is not eligible for data sharing by any of the joint account holders. Similarly, a relevant joint account holder need not have online access to their joint account for the joint account to be eligible (see section 4.4.1 of this guide) – provided they have online access to other accounts with that

data holder. The criteria used to define a CDR consumer as 'eligible' in the banking sector is set out in section 4.1 of this guide.

4.9.1. Disclosure options for joint accounts

CDR Rules: see rule 4A.5

The CDR Rules provide three disclosure options that can apply to joint accounts: the pre-approval, co-approval and non-disclosure options. Data holders must offer joint account holders the pre-approval option and the non-disclosure option. The co-approval option is an option that data holders may offer.

Pre-approval option

The pre-approval option means joint account data can be disclosed on receipt of a valid consumer data request from any account holder of the account without approval from other joint account holders. This option applies by default.

Co-approval option

A co-approval option is a more restrictive sharing preference. It means that all joint account holders must approve the request before the joint account data can be disclosed. This is an optional implementation for data holders.

Non-disclosure option

The non-disclosure option is the most restrictive option and means that joint account data cannot be disclosed.

4.9.2. Changing disclosure options

The pre-approval option applies by default. While the pre-approval option applies to the joint account, the disclosure option can be changed to a more restrictive disclosure option by any joint account holder.

Once a more restrictive disclosure option has applied to the account, all joint account holders must agree before a less restrictive disclosure option can be applied to a joint account. These changes are made using the disclosure option management service.

4.9.3. Disclosure option management service

CDR Rules: see rule 4A.6

Data holders must provide an online disclosure option management service to each joint account holder that enables an account holder to:

- change the disclosure option that applies to the account to a more restrictive disclosure option, and
- propose to the other joint account holders to change the disclosure option that applies to the account to a less restrictive disclosure option, and
- respond to a proposal by another joint account holder to change the disclosure option.

Data holders must update the disclosure option management service as soon as practicable to give effect to:

- any disclosure option indicated by a joint account holder
- any changes to a disclosure option, and
- the withdrawal of a disclosure option.

The disclosure option management service must be provided online and may be included in the data holder's consumer dashboard. The service must indicate to the joint account holder which disclosure option currently applies and give effect to any change in the disclosure option as soon as practicable.

The service must not:

- impose any additional process requirements on top of the Standards and the CDR Rules
- offer additional or alternative services
- make the process more difficult to understand by referring to other documents or providing additional information
- offer any pre-selected options.

4.9.4. Informing other account holders when one account holder selects/changes a disclosure option

Changing to a more restrictive disclosure option (CDR Rules: see rule 4A.7)

If an individual joint account holder applies a more restrictive disclosure option, the data holder must contact the other account holders to:

- explain to each of them what the CDR is
- inform them which disclosure option previously applied to the account
- inform them that an account holder has changed the disclosure option, and of the disclosure option that now applies
- explain how they can change the disclosure option again.

Changing to a less restrictive disclosure option (CDR Rules: see rule 4A.8)

If an individual joint account holder makes a proposal to change to a less restrictive disclosure option, the data holder must contact the other joint account holders and:

- explain to each of them what the CDR is
- inform them of which disclosure option currently applies to the account
- inform them that an account holder has proposed that the co-approval or pre-approval option apply to the account, as the case may be
- explain that this change requires the agreement of all account holders
- explain any alternative options for change that are available and how they can be made
- invite them to either agree or to reject the proposal within a specified period.

The specified period of time should be consistent with time limits that apply to the data holder's equivalent non-CDR services and requests.[5] At the end of the specified period, the data holder must inform each joint account holder whether:

- all the joint account holders have agreed to the change and so the proposed disclosure option applies, or
- not all the joint account holders have agreed to the change and so the disclosure option is unchanged.

4.9.5. Joint account obligations and preventing physical or financial harm or abuse

CDR Rules: see rule 4A.15

Data holders will not be liable for failure to comply with their joint account holder obligations under Part 4A of the CDR Rules if it is considered that the relevant act or omission is necessary to prevent physical, psychological or financial harm or abuse to any person.

For example, data holders will not be liable for failing to undertake the following actions if they consider it necessary to prevent physical, psychological or financial harm or abuse:

- if the non-disclosure option is in place — invite relevant account holder(s) to choose a disclosure option before disclosing data on the joint account (which is ordinarily required under rule 4A.8 of the CDR Rules)
- where a co-approval disclosure option is in place — to seek the approval of the relevant account holder(s) before disclosing data on the joint account (which is ordinarily required under rule 4A.10(4) of the CDR Rules)
- to provide a relevant account holder(s) with a dashboard or to update an existing dashboard with details regarding a joint account (which is ordinarily required under rule 4A.13 of the CDR Rules).[6]

Please refer to the Joint accounts implementation guidance for further information on joint accounts.

4.10. Requesting consumer authorisation to disclose CDR data

When a data holder receives a consumer data request from an accredited data recipient, the data holder must seek the consumer's authorisation to disclose the data (whether required data or voluntary data) to the accredited data recipient, unless an exception applies.

CDR Rules: see rule 4.23

If there is no current authorisation in place, the data holder must ask the eligible CDR consumer to authorise the disclosure.[7]

When asking a consumer to authorise the disclosure of CDR data, the data holder must inform the consumer of the following:

---

5 Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021, Explanatory Statement: page 27, paragraph 3.

6 Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021, Explanatory Statement: page 28, paragraph 2 on vulnerable consumers.

7 CDR Rule 4.5

- the name of the accredited data recipient that made the request[8]
- the period of time the request covers
- the types of data to be disclosed
- whether the authorisation is to disclose data on a single occasion or over a period of time (and if so, how long that period is), noting that the period of time cannot exceed 12 months
- that the consumer can withdraw their authorisation at any time and instructions on how to do so
- any information that the Register of Accredited Persons holds in relation to the accredited person.

The data holder does not need to seek authorisation if the data holder already has a current authorisation from the consumer to disclose the requested data to the accredited data recipient (see rule 4.5(1)(b) of the CDR Rules).

- If the data holder has a current authorisation from a consumer to disclose to a particular accredited data recipient but receives a request from the accredited data recipient for which the consumer has provided a new consent,[9] the data holder will need to ask the consumer for new authorisation for any elements of the request that are not subject to the existing authorisation. In practice, this may mean the data holder will need to ask the consumer for a new authorisation for the requested data under the new consent.
- The data holder's process for asking a consumer to give or amend an authorisation must accord with the Standards (see rule 4.22(a) of the CDR Rules) and the request for authorisation itself must be in accordance with the Standards (see rules 4.5(2)(b) (voluntary consumer data) and 4.5(3)(b) (required consumer data – subject to rule 4.7 of the CDR Rules – see section 4.12 below).
- The process for seeking authorisation should be easy to understand for consumers (see rule 4.22(b) of the CDR Rules).

See CDR Standards:

Standards	Security Profile	The entire Security Profile is applicable to the process for the authorisation of consent for data sharing and the subsequent use of that authorised consent to make CDR data requests
CX Standards	Consent, Authenticate, Authorise Standards and Amending Authorisation	Authenticate; Authorise
CX Guidelines	Authenticate; Authorise	

[8] As noted in the CX guidelines, data holders must use the accredited data recipient's legal entity name as the 'name of the accredited data recipient'.

[9] This scenario is distinct from when a consumer amends an existing consent. See below section 4.10.1 for more detail on amending consents.

CDR Rules: see rule 4.24

When asking a consumer to authorise the disclosure of CDR data, the data holder must not:

- add any additional requirements to the authorisation process
- provide or request information outside of that specified under the CDR
- offer additional or alternative services to the consumer
- include or refer to other documents.

For example, a data holder should not include statements in this process that imply that the consumer's data will be less secure with the recipient accredited data recipient than it was with the data holder.

This process is distinct from a CDR consumer amending their collection consent, which will require the data holder to invite the CDR consumer to amend their corresponding authorisation (see section 4.10.1 of this guide and rule 4.22A for more information).

The same applies if the data holder is considering disclosing any requested voluntary consumer data (rule 4.5(2)).

If the request relates to a joint account

CDR Rules: see rules 4A.10 and 4A.11

When a data holder receives a consumer data request from an accredited data recipient in relation to a joint account:

1. if the **pre-approval** option applies to the joint account, the data holder must process the request as it would any other request on a non-joint account. However, if a relevant joint account holder withdraws their approval, the data holder must not disclose any or any further requested CDR data.
2. if the **co-approval** option applies, the data holder must seek the requester's authorisation and the relevant account holders' approval before disclosing the requested data. The data holder must contact the other joint account holders to:
    - inform them about the request, including:
        - provide the information, set out above in section 8.10, that a data holder must give the consumer when requesting authorisation to disclose CDR data for non-joint accounts
        - that an accredited person has requested disclosure of CDR data relating to the joint account upon the request of the initiating joint account holder
        - that the initiating account holder has authorised this disclosure of data from their joint account and that their co-approval is required before this data can be released.
    - ask whether the account holders approve the disclosure of the joint account data and when they need to give their approval by, and inform them that if an approval is not received by that time, the joint account data will not be disclosed

- inform them that any of the account holders can withdraw their approval at any time, including instructions on how to do so and an explanation of the impact this would have.

If a relevant joint account holder has withdrawn their approval, the data holder must not disclose any or any further requested CDR data.[10]

3. if the **non-disclosure** option applies, the data holder must refuse to disclose the requested CDR data.

4.10.1. When a consumer amends their consent

CDR Rules: see rule 4.22A

If a data holder is notified by an accredited data recipient that a consumer has amended their consent relating to the sharing of their CDR data by the data holder, the data holder must invite the consumer to amend their authorisation for the disclosure of CDR data accordingly.

4.10.2. When a consumer withdraws their authorisation

CDR Rules: see rule 4.25

Data holders must allow consumers to withdraw their authorisation at any time through the consumer dashboard and must also provide a simple alternative method of communication for this purpose, for example via telephone.

When a consumer withdraws their authorisation, the data holder must:

- cease sharing the consumer's data as soon as possible – at most within 2 business days of receiving the communication; and
- notify the accredited data recipient of the withdrawal in accordance with the Standards.

See CDR Standards:

CX Standards	Data Language; Withdrawal Standards	Withdrawing consent; Consequences; Redundant data
CX Guidelines	Consent Management	

When a joint account holder gives, amends or withdraws their authorisation or the authorisation expires

A joint account holder may withdraw their own authorisation to disclose CDR data to a particular accredited person at any time.

A joint account holder cannot withdraw the authorisations given by other account holders or secondary users.

Where a joint account holder withdraws an authorisation:

[10] For more information about the withdrawal of approvals, see paragraphs 9.5-9.8 of our Joint Account implementation Guidance.

- data sharing from the joint account under the authorisation must cease, along with data being shared from any other account that is associated with that authorisation (rule 4.25)
- consumer dashboards must be updated to reflect the withdrawal (rule 1.15 and rule 4A.13(1)(c))
- the data holder must notify joint account holders that the authorisation has been withdrawn through its ordinary means of contacting them (rule 4A.14(1))
- the data holder must notify the accredited person that the authorisation has been withdrawn, in accordance with the data standards (rule 4.25).

4.11. How to disclose consumer data

CDR Rules: see rule 4.6

Once a data holder has received authorisation from the consumer to disclose their data to the accredited person, the data holder must disclose the required consumer data it is authorised to disclose. The data holder may (but is not required to) disclose the voluntary consumer data it is authorised to disclose.

The data holder must disclose data in a machine readable form through the accredited person request service and in accordance with the Standards.

See CDR Standards:

Standards	Industry Specific APIs	As relevant to the consumer data requested
Standards	Standards	Versioning; Uniform Resource Indicator Structure; HTTP Headers; HTTP Response Codes; Payload Conventions; Common Field Types; Pagination; ID Permanence; Extensibility
Standards	Security Profile	Tokens; Identifiers and Subject Types; Transaction Security
Standards	Non-functional Requirements	The majority of the non-functional requirements impact the sharing of consumer data

A fee cannot be charged for the disclosure of required consumer data but may be charged for the disclosure of voluntary consumer data.

The data holder must update the consumer's CDR dashboard to show the CDR data that was disclosed, when it was disclosed and the accredited data recipient (see Privacy Safeguard 10 - s 56EM of the CCA and rule 7.9).

4.11.1. Joint accounts

CDR Rules: see rule 4A.10. See also section 4.9 of this guide for further detail.

In addition to the above, CDR data for a joint account can only be disclosed if:

- the requesting account holder has authorised the disclosure AND
- the 'pre-approval' option applies to the joint account OR
- the 'co-approval' option applies to the joint account and all joint account holders have approved the disclosure of this data.

4.12. Circumstances in which a data holder can refuse to disclose required consumer data

CDR Rules: see rules 4.6A and 4.7

A data holder can refuse to ask a consumer to authorise the disclosure of consumer data, or refuse to disclose the data if:

- the data holder considers it necessary in order to prevent physical or financial harm or abuse
- the data holder has reasonable grounds to believe that disclosure of some or all of that data would adversely impact the security, integrity or stability of the Register of Accredited Persons, or its own information and communication technology systems
- the request was made on behalf of a secondary user and the account holder has indicated that they no longer approve CDR data being disclosed to that accredited person in response to consumer data requests made by that secondary user
- it relates to an account that is blocked or suspended
- the refusal is permitted under circumstances set out in Standards, or
- a Schedule in the Rules provides that the requested CDR data must not be disclosed.

See CDR Standards:

Standards	Standards	HTTP Response Codes – HTTP Status: 403 Forbidden, HTTP Status: 429 Too Many Requests
Standards	Non-functional Requirements	Exemptions to Protect Service

4.13. Disclosing incorrect data

CDR Rules: see rule 7.10

See also: Privacy Safeguard 11 – section 56EN of the CCA

Data holders must take reasonable steps to ensure the data they disclose through the CDR is correct.

If after disclosing CDR data, a data holder becomes aware that some or all of the disclosed data was inaccurate, out of date, or incomplete, the data holder must notify the consumer of this. The data holder must provide the CDR consumer with a written notice that:

- identifies the accredited person to whom the CDR data was disclosed
- states the date of the disclosure
- identifies the CDR data that was incorrect, and
- states that the consumer can request the data holder disclose the corrected CDR data and if such a request is made, the corrected data will be disclosed.

This notice can be given through the CDR participant's consumer dashboard. It must be provided as soon as practicable and within 5 business days after the data holder is aware of disclosing the incorrect data.

See chapter 11 of the OAIC's Privacy Safeguard Guidelines for detailed information on these obligations, including how data holders should ensure information they are disclosing through the CDR is correct, when and how to advise a consumer if CDR data that was disclosed was incorrect, and when a data holder should disclose corrected CDR data to an accredited data recipient.

4.14. Correcting incorrect CDR data

CDR Rules: see rule 7.15

See also: Privacy Safeguard 13 – section 56EP of the CCA

Privacy Safeguard 13 applies in relation to data holders where a consumer has requested that a data holder correct their CDR data and the data holder was earlier required or authorised to disclose that data under the CDR Rules. See chapter 13 of the OAIC's Privacy Safeguard Guidelines for further information on how to acknowledge, action and respond to correction requests.

5. Data holders must establish dispute resolution processes

5.1. Internal dispute resolution

CDR Rules: see rule 6.1 and Schedule 3, clause 5.1

A data holder must have an internal dispute resolution process that complies with the current version of the Australian Securities and Investments Commission's Regulatory Guide 271: Internal Dispute Resolution, which is tailored to their business.

Relevant Provisions of ASIC Regulatory Guide 271

Matters to be dealt with	Relevant paragraphs of Regulatory Guide 271: Internal dispute resolution current as at January 2022
Guiding principles or standards the applicant's IDR procedures must meet	271.127 – 271.160
Outsourcing IDR procedures	271.45 – 271.48
Responding to complaints (including maximum timeframes for a response)	271.49 – 271.75
Multi-tiered IDR procedures	271.102 – 271.106
Tailoring IDR procedures to the applicant's business	271.34
Documenting internal facing IDR processes, policies and procedures	271.179 – 271.185
Consumer advocates	271.107 – 271.110
Establishing links between IDR procedures and external dispute resolution	271.111 – 271.116
Systemic issues	271.117 – 271.123

These requirements only currently apply to the handling of complaints from CDR consumers, and not to complaints from other industry participants. The complaint handling process applies to all complaints from CDR consumers, including complaints about CDR data.

Though this requirement does not extend to complaints from other industry participants, we do expect CDR participants to manage all complaints they receive reasonably and note that the ACCC is able to consider complaints it receives from other CDR participants.

5.2. External dispute resolution

CDR Rules: see rules 1.7(1) and 6.2

A data holder must be a member of a recognised external dispute resolution scheme in relation to CDR consumer complaints. The Australian Financial Complaints Authority is the recognised external dispute resolution scheme for the banking sector.

6. CDR policy

CDR Rules: see rule 7.2

See also: Privacy Safeguard 1 – section 56ED of the CCA

Data holders must have a CDR Policy that is distinct from any existing privacy or information security policy. The policy needs to be available to consumers free of charge and in their preferred format (hard copy / electronic). See the OAIC's Guide to developing a CDR policy for more information on the required format and contents for a CDR Policy.

Privacy Safeguard 1 also requires data holders to take reasonable steps to establish and maintain internal practices, procedures and systems to ensure they are complying with their obligations under the CDR. Further information is available in chapter 1 of the OAIC's Privacy Safeguard Guidelines.

7. Record keeping requirements

CDR Rules: see rule 9.3

Data holders must keep records of:

- consumer authorisations to disclose CDR data
- amendments or withdrawals of authorisations to disclose CDR data
- notifications of withdrawals of consent to collect CDR data
- disclosures of CDR data made in response to consumer data requests
    - Data holders are not expected to keep copies of the disclosed CDR data itself. A disclosure log evidencing the type of data that was disclosed, when it was disclosed and who it was disclosed to would be sufficient.
- any written agreements regarding the obligation to disclose product data for white labelled products
- instances when the data holder has refused to disclose CDR data and the CDR Rule or Standard relied on for this refusal
    - For each instance where the data holder has refused to disclose CDR data they must, at a minimum, keep a record of:
        - the relevant ground of refusal, and
        - the date and time they relied upon that ground of refusal.
- CDR complaint data, as defined by rule 1.7

    - This includes the number of CDR consumer complaints received by the CDR participant, the number of such complaints resolved and the average number of days taken to resolve CDR consumer complaints through internal dispute resolution, amongst other things. Further detail is available in section 8.1.2 of this guide and can also be found here.

- its processes for requesting a consumer's authorisation to disclose CDR data and for amendments to that authorisation
    - Data holders must keep a video record of each process. The video is expected to demonstrate what the typical end-to-end flow of the authorisation process, and of the amendment to authorise process, would be from the point of view of a CDR consumer. Data holders may choose to also keep and maintain records in the form of wireframes and screenshots of their processes if that would further assist with explaining their authorisation and amendment to authorise processes.

Each record must include the date and time when the record was made and, if applicable, the date and time when the event described by the record occurred.

If a record is kept in a language other than English, an English translation of the record must be made available within a reasonable time frame, if a person who is entitled to inspect the records requests an English translation.

Records must be kept for 6 years, beginning from the day each record was created.

Records should only contain personal information where it is necessary to comply with the CDR Rules.

CDR consumers can request copies of the data holder's records in relation to authorisations they have given to disclose CDR data, amendments to or withdrawals of those authorisations, disclosures of CDR data pursuant to those authorisations and CDR complaint data that relates to them (see rule 9.5 of the CDR Rules).

The ACCC can audit data holder's compliance with the CCA, CDR Rules and Standards at any time and can request copies of the records that are required to be kept under this provision through an audit or for other compliance purposes (see rule 9.6 of the CDR Rules).

8. Reporting requirements

8.1. Reporting requirements

8.1.1. Biannual CDR reporting

CDR Rules: see rule 9.4

Data holders must submit CDR reports twice a year to the ACCC and OAIC.

Reporting Period	Report due by
1 January – 30 June	30 July
1 July – 31 December	30 January

Data holders' reporting obligations under rule 9.4 of the CDR Rules commence from the date they are required to start sharing product data under the CDR Rules. If, however, a data holder chooses to enable product data sharing prior to the relevant compliance dates stated in clause 6.6 of schedule 3 to the CDR Rules, their obligation to report begins from that earlier date.

The reports must be in the approved format and contain specific information.[11]

The approved reporting form template covers both product and consumer data.

The information included in the report must be current as at the last day of the relevant reporting period. The following sections provide a detailed overview of the key sections of the reporting form and the ACCC's expectations about what should be included in a data holder's report.

8.1.2. CDR complaint data summary

'CDR complaint data'[12], in relation to a data holder, means:

- the number of CDR consumer complaints received by the data holder
- the number of CDR consumer complaints received for each of the data holder's CDR consumer complaints categories, noting that it is anticipated that data holders may have different systems for categorising CDR complaints as part of their respective complaint handling processes
- the number of CDR consumer complaints resolved (the data holder may choose to report this as one total number or as two numbers indicating whether the resolved complaints were reported in the current reporting period or a previous reporting period)
- the average number of days taken to resolve CDR consumer complaints through internal dispute resolution
- the number of CDR consumer complaints referred to a recognised external dispute resolution scheme
- the number of CDR consumer complaints resolved by external dispute resolution, and
- the number of CDR product data complaints received, that is, complaints made to the data holder about its required or voluntary product data for which a response or resolution could reasonably be expected.[13]

The reporting form requires each of these items to be reported on individually.

8.1.3. CDR data requests received

The report requires data holders to separately outline the total number of:

- product data requests
- consumer data requests made directly by consumers, and

[11] A template of the approved reporting form is available on the ACCC website.

[12] See the definition in s1.7 of the CDR Rules

[13] The CDR Rules only stipulate internal dispute resolution requirements for handling complaints from CDR consumers, not CDR product data complaints, (see clause 5.1(2)(a) of Schedule 3 and 5.1(4)(a) of Schedule 4 to the CDR Rules), as these can be made by the public at large. However, it is still expected that CDR participants reasonably manage all complaints they receive. It should also be noted that the ACCC is able to consider and investigate complaints it receives from other CDR participants and members of the public.

- consumer data requests made by accredited persons on behalf of consumers received during the relevant reporting period.

'Received' means the request for CDR data reached the data holder's system and the data holder can provide a response to the request. As such, data holders are expected to report on both "successful" CDR data requests (for example, requests that resulted in the requested CDR data being shared) and "unsuccessful" ones (for example, requests that did not result in the requested CDR data being shared). This means that data holders are expected to include in their report the number of requests that resulted in a rejection due to traffic thresholds, as described in the Standards, being exceeded.

It is not expected that a data holder will report on requests that did not reach the data holder's servers in situations where the data holder is unable to reasonably identify or categorise whether the request relates to a product data request or a consumer data request. For example, it is not expected that a data holder will report on requests that are blocked by their global firewall, where the firewall has been set-up to protect the data holder's entire system and the data holder is unable to readily identify whether the request is in fact a CDR-related request.

8.1.4. Refusals to disclose CDR data — total number and reasons

A data holder must share required data in response to a valid request that it receives, unless it is able to refuse to disclose CDR data in response to a request because CDR Rules 2.5(1), 3.5(1) and 4.7(1) apply in the circumstances.

CDR Rules 2.5(2), 3.5(2) and 4.7(3) require that a data holder must inform the requester, CDR consumer, or accredited person of such a refusal in accordance with the data standards. The data standards enable data holders to provide error codes to indicate the reason that data has not been disclosed.

The table below sets out the CDR Rules a data holder may rely upon to refuse to disclose data, and the corresponding HTTP error codes as set out in the Standards.

Circumstance	CDR Rule	HTTP error code
Requests received may cause physical, psychological, or financial harm or abuse	3.5(1)(a), 4.7(1)(a)	403 Forbidden
Requests received relate to an account that is blocked or suspended	3.5(1)(aa), 4.7(1)(c)	404 Not Found 422 Unprocessable Entity
Requests received would adversely impact the security, integrity or stability to the Register of Accredited Persons or the data holder's ICT systems (for example, during a potential distributed denial of service or equivalent form of attack)	2.5(1), 3.5(1)(b), 4.7(1)(b)	429 Too Many Requests
Requests received exceed the service level thresholds in the Non-Functional Requirements section of the Standards	2.5(1), 3.5(1)(b), 4.7(1)(d)	429 Too Many Requests
The consumer data request originated from a sanctioned country.	2.5(1) 4.7(1)(d)	Data holders should use general error codes for security reasons. It is expected that Data Holders would appropriately instrument their solutions so they can provide relevant information to regulators for audit purposes.

The return of a 403, 404, 422 and 429 HTTP error code in response to circumstances other than those set out in the above table does not constitute a refusal to disclose data under the CDR Rules.

If a request is not received, or not valid, data holders cannot provide data in response. Therefore, these instances do not constitute a refusal to disclose data, and do not need to be reported under rule 9.4 of the CDR Rules.

More information can be found in published Guidance and various articles on the CDR Support Portal, such as this and this. A summary table can be found below:

Request attribute		Data holder obligation	HTTP code provided to requester
Valid	**Received**		
Yes	Yes	Must disclose required data, except in circumstances set out above.	200 OK 403 Forbidden 404 Not Found 422 Unprocessable Entity 429 Too Many Requests
No	Yes	Unable to disclose required data in response to an invalid request.	400 Bad Request 401 Unauthorized 405 Method Not Allowed 406 Not Acceptable 415 Unsupported Media Type
Yes	No (due to outages)	The data holder is unable to disclose required data as the request is not received.	500 Internal Server Error 503 Service Unavailable 504 Gateway Timeout

It is not necessarily expected that data holders report on attacks or requests outside the /cdr au/ path of their CDR domain, particularly if the data holder is unable to reasonably identify whether the request is in fact CDR-related. It is also not expected that a data holder will report on requests they failed to respond to due to a scheduled maintenance, unexpected outage or during a period of system instability.

For the avoidance of doubt, data holders are not required to record and report information regarding instances where they have refused to ask for an authorisation (for example for the reasons listed at rule 4.7 of the CDR Rules, such as for the avoidance of harm or abuse).

8.1.5. Submitting the reporting form

Data holders must submit CDR Rule 9.4 reports to the ACCC and the OAIC, by completing an online web form which is accessible via the CDR Participant Portal. Please see section 9 of the Participant Portal User Guide for more details.

Data holders that have multiple brands are required to submit aggregated data covering all brands in one single report.

8.2. Updating the CDR register

CDR Rules: see rule 5.25

If a data holder becomes aware that information it has previously provided to the Accreditation Registrar is out of date or requires amendment, it must notify the Accreditation Registrar as soon as practicable. This notification can be made via email to the ACCC's CDR inbox ACCC-CDR@accc.gov.au.

8.3. Reporting to the CDR Register

The ACCC can use the Get Metrics API to obtain statistics from data holders on the operation of their CDR compliant implementation. The Get Metrics API is a sub-section within the Admin APIs section of the Standards.

The ACCC obtains these statistics by the CDR Register sending a request to data holders, for example, the CDR Register calls the data holders' Get Metrics endpoints. In practice, this occurs at approximately 5AM AEST daily. Each daily call collects one week of data.

The operational information that is called for is identified in the Admin APIs Standard.

To comply with the Admin APIs Standard, data holders must make Get Metrics API available to be called and the data provided in response must be complete and accurate in accordance with the Standards.

See CDR Standards:

Standards	Admin APIs	ResponseMetricsListV3

The ACCC can take enforcement action against a data holder that has not made the Get Metrics API available for the CDR Register to call.

As a matter of compliance and enforcement policy, the ACCC expects that data holders will make their Get Metrics API available to be called by the Register when they are added to the Register (and are therefore able to commence sharing consumer data).

The implementation date for Version 3 of the Get Metrics endpoint is 1 October 2022.

The ACCC also publishes this information on the CDR.gov.au website to provide transparency to consumers and other CDR participants about the performance and availability of data holder CDR solutions. See: https://www.cdr.gov.au/performance/.