Australian Government

Consumer Data Right

Compliance Guidance for Data Holders

Banking sector

April 2021

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 any 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 the Director Publishing, ACCC, GPO Box 3131, Canberra ACT 2601, or publishing.unit@accc.gov.au.

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 will improve a consumer's ability to compare and switch between products and services and encourage competition between service providers, leading to more innovative products and services for consumers and the potential for lower prices. Banking is the first sector to be brought into the CDR.

Data holders need to do four main things under the CDR. They must:

- provide the necessary CDR infrastructure to enable requests to be made for product and consumer data, including joint account data;
- disclose general product data about products they offer, covering interest rates, fees and charges, discounts and other features;
- securely transfer, with a consumer's authorisation, a consumer's data in a machine-readable format when they receive a valid request; and
- manage 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.

You can find a glossary of common terms 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 consumer data rules and standards are made, the role of the Data Recipient Accreditor and the Accreditation Registrar
- 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 (**Rules**)
    - You can find directions to the most recent version of the CDR Rules on the CDR Support Portal.
- Consumer Data Standards made under the Rules (**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, Rules and Standards impose a range of requirements that data holders, Accredited Data Recipients (**ADRs**) and intermediaries need to comply with. This guide is designed to assist data holders to understand and comply with their obligations.

The focus of this guide is on the obligations arising under the Rules and Standards.

The guide does not cover in any detail a data holder's obligations under the Privacy Safeguards. Information about these obligations can be found in the Privacy Safeguard guidelines issued by the Australian Information Commissioner. Those guidelines provide guidance to entities on avoiding acts or practices that may breach the Privacy Safeguards (the safeguards are set out in Division 5, Part IVD, CCA). Data holders can also refer to the Office of the Australian Information Commissioner's (**OAIC**) *Guide to privacy for data holders*, for further information on how to comply with the privacy and confidentiality-related Rules outlined in this guide.

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 ADR in addition to being a data holder. ADR 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, Rules, Standards and other compliance guidance material referred to throughout this document.

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 regulators

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. Consumer focused outcomes are paramount for both regulators. We work together to jointly monitor compliance with the CDR regulations, respond to issues and take enforcement action if necessary.

1.1.4. Compliance and Enforcement Policy

The ACCC and OAIC have developed a Compliance and Enforcement Policy, which aims to help data holders and accredited persons (**CDR participants**) and consumers to understand the approach that 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, a data holder is an Authorised Deposit-taking Institution (**ADI**) or an **ADR** that holds CDR data about:

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

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 Rules as '**initial data holders**'. Initial data holders were required to share CDR data earlier than other ADIs.

All remaining ADIs that are not an ADR, 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.

ADRs

ADRs having requested and received CDR data under the Rules will be required to share CDR data, in accordance with reciprocal data sharing obligations. ADIs that become ADRs will need to share data at an earlier stage than would otherwise have been required if they were not accredited. These ADRs are referred to in the commencement table in the Rules (clause 6.6 of Schedule 3) as **reciprocal data holders**.

An ADR is generally[1] not a data holder if it only holds CDR consumer data that was disclosed to it by another data holder under the Rules.

Commencement of obligations

The date that a data holder's obligations commence under the CDR will depend on which group they fall into. Obligations will also commence at different times for different products, depending under which 'phase' the product is categorised (see clauses 6.2 and 6.6 of Schedule 3 of the Rules for the commencement table and clause 1.4 of Schedule 3 of the Rules for the list of phased products). As a summary:

Initial data holders

- have been required to share product data since 1 February 2020
- have been required to share consumer data for their primary brands since 1 July 2020
- are required to share consumer data for their non-primary brand products from 1 July 2021.

All other ADIs

- are currently required to share Phase 1 and 2 product data. This will extend to include Phase 3 products from 1 July 2021

[1] In some circumstances, if conditions in the Rules are met, an ADR can become a data holder of CDR data it has received under the Rules. The only condition that applies as at the time of this publication is if an ADI has provided a CDR consumer with a product and the CDR consumer agrees to the ADI being a data holder of that CDR data (*see clause 7.2 of Schedule 3 of the Rules*).

- will be required to share Phase 1 consumer data from 1 July 2021. This will extend to include all listed products by 1 February 2022.

ADRs

- have been required to share Phase 1 consumer data since 1 March 2021 and will be required to share Phase 2 and 3 consumer data from 1 July 2021.

1.1.6. Obligations under the CDR Scheme

Under the CDR, subject to the commencement table, 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.

These requirements are set out in the CCA, Rules and Standards. This guide explains broadly how to comply with each of these obligations and provides links to further guidance on relevant topics.

This guide is currently restricted to data holder obligations in relation to sharing data with consumers through an ADR. It does not cover obligations relating to sharing data directly with consumers. These obligations have not yet commenced.

1.1.7. Exemptions under s56GD of the CCA

CDR participants can seek an exemption from complying with their obligations under the CDR. 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.

You can view the exemption register for details on all exemptions granted by the ACCC and the Guidance for applicants seeking exemption under s56GD for more information about how to apply for an exemption and when an exemption might be appropriate.

2. Data holders' obligations under the Standards

The Rules set out specific obligations for disclosing data. The Standards particularise some of those obligations.

The Rules require the making of Standards including for the format and process by which data holders must respond to requests for CDR data received from consumers and ADRs and the processes for the handling and protection of CDR data. The full list is set out in Rule 8.11.

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

- Where the Rules require compliance with the Standards, non-compliance with the Standards may constitute a breach of the Rules.
- Where the Standards are specified as binding standards as required by the Rules for the purposes of s56FA of the CCA, they apply as under contract between a data

holder and an ADR. The legal effect of binding standards as between data holders and ADRs is fully set out in s56FD and s56FE of the CCA.

The Standards are made by the Data Standards Chair with the assistance of the Data Standards Body (**DSB**). The current version of the Standards is available here. The Standards are a "living" document, subject to continual change, in order to adapt to changing demands for functionality and available technology 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 Rules, the 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 ADRs. These specifications must be implemented by a data holder.
Receiving and responding to CDR data requests	
Standards	Contains high level standards that govern the technical standards as a whole. These high level standards apply to all CDR participants.
Industry Specific APIs	Sets out API end point specifications - such as methods, paths and schemas - which allow an ADR 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.
Authorisation scopes	Sets out the level of authority the ADR 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	
CX Standards	Sets out what data holders need to 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 (NFRs)	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. Note: the NFRs have not yet commenced.

2.1. References to the Standards in this Guide

This guide contains references to particular aspects of the Standards throughout, as part of the guidance on a data holder's compliance obligations.

These references are:

- noted by way of general guidance only, to assist data holders in complying with the Rules and Standards
- included to point out particular aspects of the Standards that are relevant to the obligation being described in the Guide
- at a high level of generality, e.g. by the section heading that appears in the Standards, because changes to the content of the Standards are anticipated.

These references are not a comprehensive statement of all the Standards that are 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 particular parts of the Standards throughout this Guide are in the following format:

Standards: whether the relevant Standard is a technical Standard or Consumer Experience (CX) Standard; 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, Authenticate and Authorise Standards	Authenticate – One Time Password

No reference will be provided if Standards have not been developed on a particular topic.

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 the obligations are signified within the Standards by the use of 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 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 will be applied 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 to be not held and a null 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 Guidelines (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 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)*). Data holders therefore should use the CX Guidelines as a model approach for guiding a CDR consumer through the authorisation process.

The CX Guidelines demonstrate 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 below.

CX Standards and Guidelines resources

Resource	Description
CDR Support Portal	The CDR Support Portal publishes guides on technical and compliance-related matters: see, for example, Guidance for data holders – CDR Products and eligible consumers; and FAQ-page for the Standards.
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 Noting Paper 143 – CDR conventions.
CX Checklist	Items on the CX Checklist are being released iteratively from December 2020. It is intended to be a list of requirements in the Rules, privacy safeguards, Standards, CX Standards and CX Guidelines to assist with implementation and compliance.
CDR Standards GitHub pages	The DSB conducts consultation on the Standards online through this website. DSB decision papers and other resources are also available.

3. Disclosing product data

3.1. When do obligations commence?

CDR Rules: see Schedule 3 clause 6.6

To comply with the CDR, data holders need to make specified information about their products available through an online request service, from the time their obligations commence (see Section 1.1.5 of this guide).

This obligation applies to:

- Products that are 'publicly offered' meaning those that are generally advertised and available to customers as 'standard form contracts.' They will have terms and conditions that are subject to low levels of negotiation, if any. It does not mean that the product has to be available to any member of the public – products may be subject to eligibility requirements and are still considered publicly offered. It does not include grandfathered products that are no longer available. 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; URI Structure; HTTP Headers; HTTP Response Codes; Payload Conventions; Common Field Types; Pagination; ID Permanence; Extensibility
Standards	Security Profile	Transaction Security, CORS
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 clause 3.1

Product data is further 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 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,

- 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 eg. data held only in a PDF would not need to be shared.

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; URI Structure; HTTP Headers; HTTP Response Codes; Payload Conventions; Common Field Types; Pagination; ID Permanence; Extensibility
Standards	Security Profile	Transaction Security, CORS
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 typically created and operated by one entity (a white labeller), and branded and retailed to consumers by another entity (a 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), that data holder is required to respond to product data requests 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 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 CDR data

4.1. Who is an eligible CDR consumer?

Under the Rules, data holders are required to enable consumer data sharing 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 or over;
  - a person who is not an individual (e.g. a corporation); or
  - a partner in a partnership.

4.2. When do obligations commence?

To comply with the CDR, data holders need to share specified consumer data with an ADR if a consumer requests and authorises this to occur.

Products have been divided into three groups and the obligation to share this data will arise in three corresponding phases. The following timeline outlines the implementation timeframes for data holders to enable consumer data sharing for **individual** consumers.

Consumer data requests made by accredited persons on behalf of individual CDR consumers

Data holders	1 July 2020	1 Nov 2020	1 Feb 2021	1 March 2021	1 July 2021	1 Nov 2021	1 Feb 2022
Initial data holders	Phase 1	Phase 1 and 2	All product phases				
Reciprocal data holders				Phase 1*	All product phases		
All other ADIs					Phase 1*	Phase 1 and 2	All product phases

**does not include consumer data from joint accounts, closed accounts, direct debits, scheduled payments or payees or 'get account detail' or get customer detail' data as defined in the Standards.*

The dates in the above table are the dates by which data holders must commence sharing particular types of consumer data. Data holders are able to commence sharing consumer data earlier than required if desired. Sharing data earlier has no impact on obligation dates for subsequent phases.

CDR product phases

Phase 1 products **All data holders - 1 July 2021**	**Phase 2 products** **All data holders - 1 Nov 2021**	**Phase 3 products** **All data holders - 1 Feb 2022**
• 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 **However, data holders are not required to disclose consumer data relating to:** • joint accounts • closed accounts • direct debits • scheduled payments • payees • 'get account detail' or 'get customer detail' data. **Consumer data from these products is required to be shared as part of phase 2.**	• 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.

Non-individuals, partnerships and secondary users

As noted above, there is a different timeframe for enabling consumer data sharing for non-individual consumers (including corporations), business partnerships, and secondary account users (i.e. individuals that have account privileges with an account held by another person) (s*ee Schedule 3 clause 6.7 of the Rules)*.

- Major banks are required to enable consumer data sharing for this group of consumers by 1 November 2021.

- Non-major banks are required to enable consumer data sharing for this group of consumer by 1 November 2022.

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 CDR participant portal User Guide provides further information about the portal and the registration process.

4.4. Required consumer data and voluntary consumer data

CDR Rules: see Schedule 3 clause 3.2

A CDR consumer can request access to their required consumer data, their voluntary consumer data, or both.

Required Consumer Data	Voluntary Consumer Data
Is CDR data that: • is dated after 1 January 2017 • is held in a digital form in a format compatible with sharing under the Standards eg. data held only in a PDF would not need to be shared • relates to one or more CDR consumers And is either: • customer data in relation to a CDR consumer • 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 (eg. Individually negotiated product prices or features).	Is 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 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 (e.g. 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?

Where there is a single data holder involved in providing a white label product (whether that is the white labeller or the brand owner), that 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 will be considered responsible for responding to consumer data request, to avoid unnecessary duplication
- unless the data holders have agreed in writing that the other data holder will respond to consumer data requests.

White labeller data holders will be able to register their white label brands on the CDR Register in advance of the commencement of consumer data sharing on 1 July 2021. If data holders 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 is not able to comply with their obligations.

Further guidance on the disclosure of consumer data from white labelled products is available here.

4.6. CDR 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
- 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; URI 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.

4.6.2. For individual accounts with additional authorised users

Data holders are required to provide a service (which can be online, but need not be) that can be used by an account holder to instruct the data holder to treat others who have account privileges with the account they hold, as a 'secondary user'. Secondary users are able to authorise consumer data sharing from the relevant account. The service must also allow the account holder to revoke such an instruction.

4.7. CDR Consumer dashboard

CDR Rules: see Rule 1.15

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:

- 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.
- 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 ADR it was disclosed to (s*ee Rule 7.9; see also Privacy Safeguard 10 - s 56EM of the CCA*)
    - if the disclosure is of corrected data in response to a request to correct previously disclosed data this should be noted (*see Privacy Safeguard 11 – s 56EN of the CCA*).

The data holder must update a consumer's dashboard as soon as practical after changes to the information contained in the dashboard (s*ee Rule 4.27*).

4.7.1. For non-individuals and partnerships

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

4.7.2. For joint accounts

CDR Rules: see Schedule 3 clauses 4.14 and 4.15

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 if a disclosure option applies or has applied to the 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

4.8. Joint accounts

Special rules apply to consumer data requests for CDR data from joint accounts. These rules only apply to joint accounts where all account holders are aged 18 years or older and hold an account with the data holder that can be accessed online (this could be the joint account or a different account).

This guide details the joint account rules, as updated in v2 of the Rules. Guidance on implementing the new version of the joint account rules is available on the CDR support portal. All banks must respond to requests for joint account data from November 2021. Initial data holders, already subject to the obligation to share joint account data, are to comply with the earlier version of the joint account rules until November 2021.

4.8.1. Disclosure options for joint accounts

Pre-approval option

Account holders can provide 'pre-approval' for the disclosure of CDR data from a joint account.

This means that CDR data can be disclosed in response to a request from one account holder without seeking approval from the other account holder(s) at the time of disclosure. For this to occur, all joint account holders need to have selected this option and not subsequently revoked that consent.

Data holders are required to offer a 'pre-approval' disclosure option.

Co-approval option

Joint account holders can elect to 'co-approve' each instance of the disclosure of CDR data from their account.

This means that CDR data in relation to the account will only be disclosed with the approval of all account holders at the time of disclosure. For this to occur, all joint account holders need to have selected this option and not subsequently revoked that consent.

Data holders may offer a co-approval disclosure option but are not required to do so.

4.8.2. Joint account management service

Data holders must provide a joint account management service that each joint account holder can use to select how they would like to disclose consumer data from their joint account under the CDR. This service:

- must be provided online and can be included in a data holder's consumer dashboard alongside accounts they hold individually
    - data holders may also provide an offline service
- must allow the joint account holder to select a disclosure option for this account out of:
    - the 'pre-approval option'
    - the 'co-approval option' (if offered by the data holder)
    - a different disclosure option, or
    - no disclosure option
- must give effect to a consumers chosen disclosure option as soon as practical
- must comply with the Standards.

See CDR Standards:

Standards	Standards	ID Permanence
CX Standards	Consent, Authenticate, and Authorise Standards	Authorise
CX Guidelines	Authorise	Joint Accounts
	Consent Management	Joint Account Management Service

4.8.3. Allowing joint account holders to select disclosure options

CDR Rules: see Schedule 3 clause 4.6

When allowing joint account holders to select disclosure options, the service must:

- explain the effect of each disclosure option
- explain how each disclosure option operates if there is a secondary user for the joint account

- inform the account holder that they can opt out of the disclosure option at any time including how to opt out and what the effect would be if they opted out
- explain the difference between the available disclosure options (if more than one is available)
- inform the account holder that both/all joint account holders must select the same disclosure option in order for data relating to the account to be shared under the CDR
- advise the account holder that once CDR data has been disclosed about the account, each joint account holder and secondary user will be able to see information about the disclosure through their consumer dashboard.

And the service must not:

- impose any additional process requirements on top of the Standards and the 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.

The service must also be in accordance with the Standards. No Standards currently apply.

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

CDR Rules: see Schedule 3 clause 4.7

If one joint account holder (account holder A) indicates through the service that they would like to change their choice of disclosure option for the joint account, the data holder must invite the other account holder(s) to indicate a disclosure option.

The data holder should use its ordinary methods for contacting the account holder(s) and must:

- explain the CDR to the account holder(s)
- inform them of account holder A's chosen disclosure option
- explain that no disclosure option will apply to the account unless all account holders select the same option
- invite the account holder(s) to indicate if they would like account holder A's chosen disclosure option to apply to the account
- if account holder A made their selection as part of a request to disclose CDR data on the joint account to an ADR, identify the ADR account holder A is seeking to disclose the data to.

4.8.5. Preventing physical or financial harm or abuse

CDR Rules: see Schedule 3 clauses 4.13, 4.14 and 4.16

A data holder, if it considers the following actions could lead to circumstances of physical or financial harm or abuse, is not required to:

- provide a joint account holder with a consumer dashboard

- reflect details of a request relating to a joint account in a relevant account holder's dashboard
- invite a joint account holder to select a disclosure option
- seek a joint account holder's authorisation to release CDR data on a joint account where the 'co-approval' option applies or
- notify a relevant account holder that a joint account holder has given, amended or withdrawn an authorisation for sharing CDR data.

4.9. Requesting consumer authorisation to disclose CDR data

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

- 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 ADR (s*ee Rule 4.5(1)(b)*).
    - If the data holder has a current authorisation from a consumer to disclose to a particular ADR, but receives a request from them which is subject to a new consent, 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 all of 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)*) 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, below*).
- The process for seeking authorisation should be easy to understand for consumers (*see Rule 4.22(b)*).

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

- the name of the ADR that made the request
- 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)
- that the consumer can withdraw their authorisation at any time and instructions on how to do so.

CDR Rules: see Rule 4.23

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, and Authorise Standards	Authenticate; Authorise
CX Guidelines	Authenticate; Authorise	

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 scheme
- offer additional or alternative services to the consumer
- include or refer to other documents.

CDR Rules: see Rule 4.24

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

If the request relates to a joint account

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

1. If the account holder that initiated the request has not already selected a disclosure option for the joint account:

- The data holder must ask the initiating account holder to indicate their preferred disclosure option for the account, using the joint account management service.
- This must be done in accordance with the Standards.

CDR Rules: see Schedule 3 clause 4.10

See CDR Standards:

CX Standards	Consent, Authenticate, and Authorise Standards	Authorise
CX Guidelines	Consent Management	Joint Account Management Service

2. If the initiating account holder has authorised the disclosure of joint account data and all account holders have selected the co-approval option, the data holder must contact the other joint account holders to:

- Inform them about the request, including:
    - that an accredited person has requested disclosure of CDR data relating to their account upon the request of the initiating joint account holder, including:
        - the name of the ADR that made the request

        - 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)
    - 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.
- 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.

The data holder must notify the initiating account holder and other relevant account holders when a joint account holder gives an approval, removes an approval, or does not provide an approval within the specified timeframe.

CDR Rules: see Schedule 3 clause 4.11

When a consumer amends their consent

CDR Rules: see Rule 4.22A

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

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 ADR of the withdrawal in accordance with the Standards.

See CDR Standards:

CX Standards	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

The data holder must inform each relevant joint account holder of this change as soon as practical.

If the requesting account holder was a secondary user and no disclosure option applies to the account, the data holder must ask the relevant account holders to select a disclosure option for the account through the joint account management service in accordance with the Standards. No Standards currently apply.

If an account holder has amended an authorisation for an account subject to the 'co-approval' disclosure option, the data holder must inform the relevant account holders of the nature of the amendment and how they can withdraw their approval to prevent further CDR data from the account from being disclosed.

CDR Rules: see Schedule 3 clause 4.16

4.10. 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 ADR, the data holder must disclose, to the accredited person, the required consumer data it is authorised to disclose, and may (but is not required to) disclose the voluntary consumer data it is authorised to disclose.

The data needs to be disclosed in 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; URI 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 (*see Privacy Safeguard 10 - s 56EM of the CCA and Rule 7.9*).

4.10.1. Joint accounts

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
- all joint account holders have selected the 'pre-approval' option OR
- all joint account holders have selected the 'co-approval' option and have authorised the disclosure of this data.

CDR Rules: see Schedule 3 Divisions 4.2 and 4.3

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

CDR Rules: see Rule 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;
- it relates to an account that is blocked or suspended; or
- circumstances set out in Standards.

If this occurs, the data holder must inform the ADR of the refusal in accordance with the Standards.

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

4.12. Disclosing incorrect data

CDR Rules: see Rule 7.10

See also: Privacy Safeguard 11 – s 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.

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 ADR.

4.12.1. Disclosing the corrected data

Under Privacy Safeguard 11, a data holder must disclose the corrected data to the ADR if the consumer requests, in accordance with the Rules.

Currently, the Standards only permit a data holder to disclose CDR data in response to a request from an ADR. Therefore in these circumstances we recommend the data holder inform the consumer that if they want the corrected data to be resent to the ADR, they need to ask the ADR to make a new request to the data holder for the corrected data.

The ACCC is working to develop a simplified process for re-disclosure of corrected data and, once this is finalised, the Standards and Rules will be updated accordingly. See here for additional information.

4.13. Correcting incorrect CDR data

CDR Rules: see Rule 7.15

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

If the consumer believes there is an error in their CDR data, they can request that the data holder correct the previously disclosed data.

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 services

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 (**IDR**) process that complies with the current version of the Australian Securities and Investments Commission's Regulatory Guide 165 *Licensing: Internal and External Dispute Resolution*, which is tailored to their business.

Relevant provisions of ASIC's Regulatory Guide 165

Matters to be dealt with	**Relevant paragraphs of Regulatory Guide 165 Licensing: Internal and external dispute resolution current as at September 2019**
Guiding principles or standards the applicant's IDR procedures must meet	165.82 – 165.84
Outsourcing IDR procedures	165.76
Responding to complaints (including maximum timeframes for a response)	165.80 – 165.81 165.86 – 165.88 165.90 – 165.94
Multi-tiered IDR procedures	165.121 – 165.123
Tailoring IDR procedures to the applicant's business	165.68
Documenting internal facing IDR processes,	165.126 – 165.129

policies and procedures	
Establishing links between IDR procedures and external dispute resolution	165.130

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 consumer 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.

Data holders should also note that they still need to record the number of complaints received from other CDR participants to report on these under item 2.7 of the reporting form (see Section 8 of this guide).

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 – s 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 disclosed CDR data and the 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
    - 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 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 kept for the purposes of this rule should only contain personal information where it is necessary to comply with the 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.

The ACCC can audit data holder's compliance with the CCA, 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 (s*ee Rule 9.6)*.

8. Reporting requirements

8.1. 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 commence from the date they start sharing product data, that is, from the date they make their product data endpoints available to the public. If a data holder chooses to share their product data endpoints prior to the relevant compliance date stated in the Commencement Table in the Rules, their obligation to report begins from that earlier date.

The reports must be in the approved format and contain specific information.[2]

The approved reporting form template covers both product and consumer data. Data holders who only had product data-related obligations during the reporting period can refer to additional guidance on completing the reporting form under these circumstances.

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 on what should be included in a data holder's report.

8.1.1. CDR complaint data summary

'CDR complaint data', 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 have different systems for categorising CDR complaints as part of their respective complaint handling processes.
- The number of CDR consumer complaints resolved.
- 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.

[2] While the current reporting form is available on the ACCC website, please note that the ACCC has approved a new form for reporting. This new form will be a web form embedded in the RAAP. Industry participants will be provided with further information about the new form once it becomes available (anticipated for late May 2021).

- 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.[3]

The reporting form requires each of these items to be reported on individually. The reporting form also includes an optional reporting item, which asks data holders to separate the number of complaints received and resolved in the relevant reporting period, and the number of complaints received in an earlier reporting period but resolved in the current reporting period.

Regarding the recording of complaints, it is encouraged that all CDR consumer complaints received and resolved should be recorded and included in reporting. However, it is understood that it is not currently industry practice for banks to record complaints resolved within 5 business days. For this reason, data holders will only be required to record and report on complaints that go through their full internal dispute resolution processes, meaning they will not be required to record and report on CDR consumer complaints resolved within 5 business days.

8.1.2. 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
- consumer data requests made by accredited persons on behalf of consumers

it received during the relevant reporting period.

'Received' means the request for CDR data reached the data holder's system and the data holder is able to provide a response to the request. As such, data holders are expected to report on both "successful" CDR data requests (i.e. requests that resulted in the requested CDR data being shared) and "unsuccessful" ones (i.e. 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.

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

The reporting form requires data holders to set out the number of times they have refused to disclose required CDR data in response to product data requests, consumer data requests made directly by consumers, and consumer data requests made by accredited persons on behalf of a consumer. It also requires the data holder to set out the rule or

[3] The Rules currently only stipulate internal dispute resolution requirements for handling complaints from CDR consumers, not CDR product data complaints, 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 is 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.

data standard relied upon to refuse disclosing the CDR data, and the number of times they relied on that rule or standard as a ground of refusal.

At a principles-level, the ACCC considers a 'refusal to disclose' required CDR data 'in response to the request' for such data means that a data holder receives a valid request for product or consumer data but, for one of a variety of reasons (e.g. traffic thresholds are being exceeded or there are reasonable grounds to suspect a security threat) they do not provide the requested data. The following table provides a non-exhaustive list of reasons a data holder may have for refusing CDR data disclosure. The table also sets out the rule and/or data standard that would likely correspond to the reason for refusal. Where there are multiple reasons for a CDR data request being refused, none of which is the primary or dominant reason for the refusal, it is expected that the data holder would refer to each of the refusal reasons in their report.

Type of refusal	**Relevant rule**	**Relevant Standard**
Traffic thresholds, as described in the Standards, are being exceeded	For product data requests: Rule 2.5(1) For consumer data requests made by an accredited person: Rule 4.7(1)(d)	HTTP response code: 429-Too Many Requests
Data holder's CDR system is being attacked by a distributed denial of service or equivalent form of attack	For product data requests: Rule 2.5(1) For consumer data requests made by an accredited person: Rule 4.7(1)(b)(ii) and/or Rule 4.7(1)(d)	HTTP response code: 429-Too Many Requests
The data holder identifies a situation where there is potential for physical or financial harm or abuse	For consumer data requests made by an accredited person: Rule 4.7(1)(a)	HTTP response code: 403-Forbidden
The data holder has reasonable grounds to believe disclosing the requested data would adversely impact the Register's security, integrity or stability	For consumer data requests made by an accredited person: Rule 4.7(1)(b)(i)	HTTP response code: 403-Forbidden
The data holder has reasonable grounds to believe the requestor is a malicious actor and that there is a genuine threat to the data holder's information and communication technology systems if the CDR data is disclosed	For consumer data requests made by an accredited person: Rule 4.7(1)(b)(ii)	HTTP response code: 403-Forbidden

The requested consumer data relates to an account that is blocked or suspended	For consumer data requests made by an accredited person: Rule 4.7(1)(c)	HTTP response code: 404 - Not Found (Included in normative standards); HTTP response code: 422 - Unprocessable Entity

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, this reporting item does not require data holders to record and report information regarding instances where they have refused to ask for an authorisation.

8.1.4. Submitting the reporting form

While previous reports were required to be submitted via email to both the ACCC and the OAIC, the ACCC has introduced a more streamlined approach for report submissions for future reports. This new process will involve data holders completing an online web form which will be accessible via the Register and Accreditation Application Platform (**RAAP**) portal. Once completed, the data holder can then submit the form to the ACCC and the OAIC at the same time via the RAAP portal. More information about submitting the new reporting forms via the RAAP will be provided when the web form is made available.

Data holders that have multiple brands are not currently required to submit separate reports for each brand, though this option is available if the data holder prefers.

8.2. Updating the accreditation 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.

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, i.e. the CDR Register calls the data holders' Get Metrics endpoints. In practice, we expect this to occur at 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 their 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	ResponseMetricsListV2

The ACCC could 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 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).

Version 2 of the Get Metrics endpoint must be implemented by 31 July 2021. For more information regarding the Get Metrics API, see the CDR Support Portal.