Australian Government

Consumer Data Right

Compliance guide for data holders

Banking and non-bank lenders sectors

July 2025

Version Control

April 2021	Version 1	First version of Guide
June 2022	Version 2	Updated references to CDR Rules and Standards, included new text on secondary user instruction and reciprocal data holders and revised text on joint accounts and internal dispute resolution.
June 2023	Version 3	Revised text to clarify that the term 'in a digital form' has its ordinary meaning.
December 2023	Version 4	Updated Guide to reflect amendments made in the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2023*.
June 2024	Version 5	Minor updates to links
February 2025	Version 6	Updated Guide to reflect amendments made in the *Competition and Consumer (Consumer Data Right) Amendment (2024 Measures No. 1) Rules 2024*.
July 2025	Version 7	Updated Guide to reflect amendments made in the *Competition and Consumer (Consumer Data Right) Amendment (2025 Measures No. 1) Rules 2025*.

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.

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.

It is the responsibility of each CDR participant to be fully aware of its obligations under the CDR regulatory framework. We recommend that CDR participants obtain professional advice on how the CDR framework applies to their specific circumstances.

Guidance revision history

Version 7 of this Guide, published in July 2025, includes changes to reflect amendments made to the *Competition and Consumer (Consumer Data Right) Rules 2020* (CDR Rules) by the *Competition and Consumer (Consumer Data Right) Amendment (2025 Measures No. 1) Rules 2025* (the Amending Rules), as well editorial changes and minor updates to links.

Version 6 of this Guide, published in February 2025, includes the following changes made to reflect amendments made in the *Competition and Consumer (Consumer Data Right) Amendment (2024 Measures No. 1) Rules 2024*:

- minor updates to substitute the texts 'revoke' and 'manage' with 'withdraw' in the context of authorisations given by nominated representatives
- minor revisions to reflect updates to consumer dashboard requirements.

Version 5 of this Guide, published in June 2024, includes minor updates to links.

Version 4 of this Guide, published in December 2023, includes changes to reflect amendments made in the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2023.*

Version 3 of this Guide, published in June 2023, includes updated text on the meaning of required product data and sharing data from offline accounts to clarify that 'in a digital form' has its ordinary meaning.

Version 2 of this Guide, published in June 2022, includes changes that were made to the CDR Rules and Standards since the Guide was first published in April 2021 and new text clarifying the operation of certain provisions.

1. Background

Key points

- The *Competition and Consumer Act 2010* (CCA), the CDR Rules and Consumer Data Standards impose a range of requirements on data holders, including to:
  - provide the infrastructure to enable requests to be made for product and consumer data
  - disclose product data about products they publicly offer
  - securely disclose consumer data in response to a valid request.
- This guide aims to assist data holders in the banking and non-bank lenders sectors understand how to comply with these requirements.

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 already applies in the banking and energy sectors. The Amending Rules, which commenced on 4 March 2025, extend the operation of CDR to the non-bank lenders sector and narrow the scope of CDR data for the banking and non-bank lenders sectors.

A glossary of common terms is published on the CDR website.

1.1.1. The CDR agencies

The CDR is a dual-regulator model, with the ACCC and the Office of the Australian Information Commissioner (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 about the CDR. 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.

1.1.2. 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)[1] and consumers to understand the approach the regulators will adopt to encourage compliance and prevent breaches of the CDR regulatory framework.

[1] *Competition and Consumer Act 2010* (Cth) s 56AL(1).

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.

1.2. Regulatory framework

In relation to the banking and non-bank lenders sectors, the CDR is regulated by a framework that consists of:

- primary 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 provisions in relation to the roles of the CDR Accreditor[2] and the Accreditation Registrar
- designation instruments made under the CCA, including the *Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019* and the *Consumer Data Right (Non-Bank Lenders) Designation 2022*, which designate the banking and non-bank lenders sectors as subject to the CDR
- the *Competition and Consumer (Consumer Data Right) Rules 2020* made under the CCA (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 Standards contain technical requirements for disclosing data to data recipients, as well as consumer experiential requirements about what data holders need to do in their consumer facing interactions. More information about the Standards is set out below.

1.3. 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 solely on the obligations for data holders arising under the CDR Rules and Standards in relation to the banking and non-bank lenders sectors.

The OAIC has certain privacy-related regulatory responsibilities under the CDR regime, in particular the enforcement of the Privacy Safeguards under Part IVD of the CCA. 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 6.4 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.

[2] The term 'Data Recipient Accreditor' was amended and replaced with the term 'CDR Accreditor' in the CCA on 26 August 2024. This term was replaced in the CDR Rules on 4 March 2025.

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.

2. Data holders

Key points

- Authorised deposit-taking institutions are data holders in the banking sector, and 'relevant non-bank lenders' are data holders in the non-bank lenders sector.
- The CDR Rules specify the data holders in the banking sector and the non-bank lenders sector that have, or will have, data sharing obligations under the CDR.

2.1. Data holders' roles and obligations

2.1.1. Roles

Banking and non-bank lender data holders have four main roles under the CDR:

- providing the necessary CDR infrastructure to enable requests to be made for product and consumer data
- disclosing generic 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.

2.1.2. Obligations

Data holders have obligations under CDR that include:

- disclosing required product data
- disclosing required consumer data
- establishing dispute resolution services
- keeping appropriate records
- reporting at scheduled intervals, and
- complying with the relevant Privacy Safeguards.[3]

Obligations have commenced for data holders in the banking sector (except in relation to Buy Now, Pay Later (BNPL) products), and obligations commence in stages for data holders in the non-bank lenders sector depending on their classification. Further information on commencement dates for data holder obligations in the banking and non-bank lenders sectors can be found in section 3 of this guide.

When undertaking their roles and responsibilities, data holders need to meet legal and technical requirements.

[3] These requirements are set out in the CCA, *Competition and Consumer Regulations 2010*, CDR Rules and Standards.

2.2. Who is a data holder?

2.2.1. Designated data holders in the banking sector and non-bank lenders sector

Under the CDR, an entity will be a data holder in the banking sector if it is an 'Authorised Deposit-taking Institution (ADI)'.[4] An ADI is a body corporate that is authorised to carry on banking business in Australia under section 9(3) of the *Banking Act 1959*.[5]

Under the CDR, a data holder in the non-bank lenders sector is a 'relevant non-bank lender'. A 'relevant non-bank lender'[6] is a corporation that:

- is a registrable corporation under section 7 of the *Financial Sector (Collection of Data) Act 2001*, or
- would be a registrable corporation without the $50 million threshold in that section applying.

This means that, for the purpose of determining whether a corporation is a CDR data holder, a corporation will be considered to be a relevant non-bank lender even if it is not a registrable corporation under the *Financial Sector (Collection of Data) Act 2001* because the value of specified assets, and the sum of the principal amounts on outstanding loans or other financing, fall below the $50 million threshold set out in paragraph 7(2)(i) of that Act.

2.2.2. Data holders in the non-bank lenders sector with CDR data sharing obligations

Not all entities that meet the definition of a 'data holder' in the non-bank lenders sector will have obligations under the CDR Rules. The flowchart below is designed to help non-bank lenders determine if they have data sharing obligations under the CDR Rules, with further detail provided in the subsequent sections of this guide.

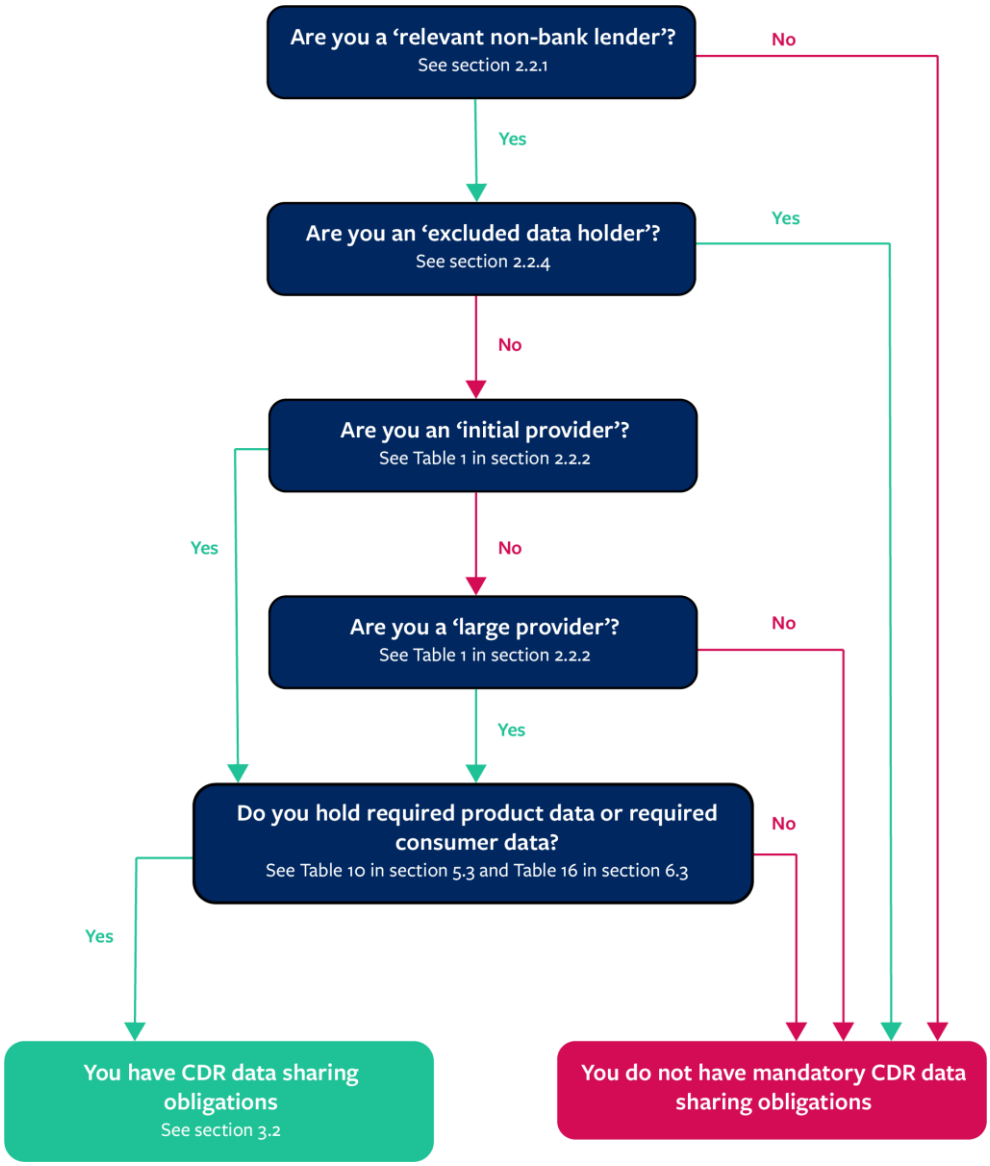
---

4 *Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019*, section 5(2).

5 *Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019*, section 4(1).

6 *Consumer Data Right (Non-Bank Lenders) Designation 2022*, section 4.

Figure 1: Do you have CDR data sharing obligations? (non-bank lenders sector)



Initial providers and large providers

In the non-bank lenders sector, only data holders that are an 'initial provider' or a 'large provider' (but are not an 'excluded data holder') under the CDR Rules will have mandatory data sharing obligations under the CDR Rules. 'Excluded data holders' are described in section 2.2.4 of this guide. Initial providers and large providers are described in Table 1 below.

Table 1: Initial providers and large providers in the non-bank lenders sector

Initial provider	Large provider

A relevant non-bank lender is an initial provider if, on 4 March 2025, the combined total value of resident loans and resident finance leases reported to the Australian Prudential Regulation Authority (APRA) under the applicable APRA reporting standards by the lender and each of its associated non-bank lenders:
• is over $10 billion in relation to the most recent calendar month for which a report was given to APRA, and
• averaged over $10 billion during the previous 12 months.[7]
	A relevant non-bank lender is a large provider if, on 4 March 2025, or on a 1 July after that day:
	• it is not an initial provider,
	• the combined total value of resident loans and resident finance leases reported to APRA under the applicable reporting standards by the lender and each of its associated non-bank lenders:
	  ○ is over $1 billion in relation to the most recent calendar month for which a report was given to APRA, and
	  ○ averaged over $1 billion during the previous 12 months, and
	• it has more than 1,000 customers on that day[8]
	OR
	• it is not an initial provider, and
	• is an accredited person.[9]

A relevant non-bank lender must notify the ACCC (via email to accc-cdr@accc.gov.au) as soon as practicable if, on any 1 July from 2025 onwards, it meets the requisite value of resident loans and resident finance leases for a large provider but has 1,000 customers, or less than 1,000 customers, on that day.[10] This is a civil penalty provision.

More information on the meaning of 'associated non-bank lender' and how to calculate resident loan and resident finance lease values can be found in the ACCC's fact sheet on non-bank lenders with CDR obligations.

Typically, once a relevant non-bank lender has met the criteria to be a large provider, it will permanently remain a large provider even if it subsequently ceases to meet any of the criteria.[11]

However, a lender who is a large provider because it is an accredited person[12] (see Table 1 above) will stop being a large provider if it ceases to be accredited and has not otherwise qualified as a large provider at any time before that day.[13]

7 CDR Rules, Schedule 3, clause 6.2(1).
8 CDR Rules, Schedule 3, clauses 6.2(2) and 6.2(3).
9 CDR Rules, Schedule 3, clauses 6.2(2) and 6.2(4).
10 CDR Rules, Schedule 3, clause 6.3(2).
11 CDR Rules, Schedule 3, clause 6.2(2).
12 CDR Rules, Schedule 3, clause 6.2(4).
13 CDR Rules, Schedule 3, clause 6.2(5).

Initial providers and large providers with no 'required consumer data' or 'required product data'

The CDR Rules define the types of data that are required to be shared on request. This is known as 'required consumer data' and 'required product data'. See sections 5.3 and 6.3 for more information on what is required consumer data and required product data.

Some entities which meet the criteria to be an initial provider or a large provider may not have any required data to share. Entities in these circumstances are not expected to meet CDR obligations such as providing data request services, undertaking ACCC registration processes, or building and testing for data sharing, despite meeting the criteria to be an initial provider or a large provider. However, if an entity later holds 'required consumer data' or 'required product data' (for example, by becoming an accredited person or by offering a new type of product for which there is required consumer data or required product data), it will be required to meet these obligations.[14]

2.2.3. Reciprocal data holders

An accredited data recipient[15] may be considered a data holder in respect of CDR data it holds (or is held on its behalf) that was not disclosed to it under the CDR Rules.[16] This means that, at times, they may be required to share CDR data in accordance with the obligations of a data holder under the CDR Rules, separate from their obligations as an accredited person. Accredited data recipients that become data holders in this way are sometimes called **reciprocal data holders**.

If an accredited data recipient that is not an ADI or relevant non-bank lender (and therefore already a data holder) does become a reciprocal data holder in this way, it will be required to share the relevant CDR data at the request of a CDR consumer.

In certain circumstances, an accredited data recipient may also become a data holder of data that it has received under the CDR Rules (see clause 7.2 of Schedule 3).

2.2.4. Excluded data holders

The CDR Rules do not apply to the following kinds of data holders:

- a body corporate that is a registered religious body offering one or more covered products in advancing its charitable purposes
- a foreign ADI for the purposes of the *Banking Act 1959* (Cth)
- a foreign branch of an Australian ADI
- a restricted ADI.[17]

However, a data holder who moves from the non-bank lenders sector to the banking sector, including those that become a restricted ADI, must comply with clause 8.1 of Schedule 3 of the CDR Rules. This applies even though restricted ADI's fall within the definition of excluded data holder. Clause 8.1 of Schedule 3 is explained in section 3.5 of this guide.

---

[14] Competition and Consumer (Consumer Data Right) Amendment (2025 Measures No. 1) Rules 2025, Explanatory Statement, paragraphs 65-66.

[15] CCA, see section 56AK for the meaning of 'accredited data recipient'.

[16] CCA, section 56AJ(3).

[17] CDR Rules, Schedule 3, clause 1.1A.

2.2.5. Voluntary participation

Not all entities that meet the definition of a 'data holder' in the banking or non-bank lenders sector will have obligations under the CDR Rules.

Under clause 6.11 of Schedule 3 the CDR Rules, a data holder in the banking sector or the non-bank lenders sector that has no mandatory CDR obligations and is not an excluded data holder may notify the ACCC that it wishes Part 2 or Part 4 of these rules to apply to it from a specified date. An entity can notify the ACCC by emailing the ACCC's CDR team at accc-cdr@accc.gov.au.

If an entity chooses to participate in the CDR, it must comply with all relevant CDR obligations. For instance, a data holder would need to provide the consumer dashboard in accordance with subrule 1.15(1) upon receiving a request under Part 4, and would need to meet the internal and external dispute resolution requirements.

Initial and large providers in the non-bank lenders sector may also choose to voluntarily disclose CDR data in accordance with the CDR Rules before their compliance date. For example, the provider may choose to enable early data sharing for testing purposes.

3. Staged implementation of the CDR Rules

Key points

- Data sharing obligations have started for all covered products in the banking sector, other than Buy Now, Pay Later (BNPL) products.
- The CDR Rules provide for the staged application of data sharing obligations to BNPL products in the banking sector.
- The CDR Rules also provide for the staged application of data sharing obligations for entities that become an unrestricted ADI on or after 4 March 2025.
- In the non-bank lenders sector, the CDR Rules provide for the staged application of data sharing obligations to initial providers and large providers, starting with product data sharing from 13 July 2026.
- Initial providers and large providers in the non-bank lenders sector do not currently have CDR data sharing obligations in relation to complex requests.
- Data holders in both sectors are not currently required to comply with CDR data sharing obligations in relation to:
  - a covered product while it is a trial product, or
  - a direct request from a CDR consumer under Part 3 of the CDR Rules.

3.1. Application of the CDR Rules to the banking sector

Data holder obligations have commenced for all covered products in the banking sector, except for BNPL products.

3.1.1. Buy Now, Pay Later (BNPL) products

The Amending Rules introduce new data sharing obligations for data holders in the banking sector that offer BNPL products.

Key characteristics of a BNPL product are intended to include, but are not limited to, the following:

- the involvement of a third-party financing entity
- the provision of finance for consumers which can be used to pay for purchases of goods, services and bills (but not for the purposes of supplying cash)
- the imposition of a fixed charge for providing credit under a prescribed limit instead of charging interest
- the imposition of a fixed charge for missing a payment.[18]

The CDR Rules provide for the staged implementation of data holder obligations in relation to BNPL products, depending on the date a data holder in the banking sector starts offering a BNPL product.

[18] Competition and Consumer (Consumer Data Right) Amendment (2025 Measures No. 1) Rules 2025, Explanatory Statement, paragraph 21.

Table 2: Commencement dates for data sharing for BNPL products in the banking sector

Date started offering BNPL products	CDR data type	Commencement date of CDR data sharing
Offered a BNPL product on or before 13 July 2026[19]	Product data requests under Part 2 of the CDR Rules	On and from 13 July 2026
	Consumer data requests under Part 4 of the CDR Rules other than complex requests	On and from 9 November 2026
Offered a BNPL product after 13 July 2026[20]	Product data requests under Part 2 of the CDR Rules	12 months after the day it first offered the BNPL product
	Consumer data requests under Part 4 of the CDR Rules other than complex requests	15 months after the day it first offered the BNPL product

Consumer data sharing obligations do not currently apply to complex requests for CDR data in relation to BNPL products. This means that data holders in the banking sector are not currently required to respond to these requests.

Complex requests are consumer data requests that are:

- made on behalf of a secondary user
- relate to a joint account
- relate to a partnership account, or
- are made on behalf of a CDR consumer who has a nominated representative[21].[22]

Information on secondary users, joint accounts and nominated representatives can be found in the Secondary users in the banking sector fact sheet, the Joint account implementation guide and the Nominated representatives of non-individuals and partnerships in CDR fact sheet.

3.1.2. New unrestricted ADIs

An entity may become an unrestricted ADI after the commencement of the Amending Rules on 4 March 2025 and as a result become a CDR data holder. This includes a person who was a restricted ADI and was therefore previously an excluded data holder.

The CDR Rules provides for the staged application of data sharing obligations for new unrestricted ADIs.[23] See the following table for details.

[19] CDR Rules, Schedule 3, clause 6.10(2).

[20] CDR Rules, Schedule 3, clause 6.10(3).

[21] A 'nominated representative' engages with a data holder on behalf of non-individuals (for example, corporations) and partners in a partnership.

[22] CDR Rules, Schedule 3, clause 6.1.

[23] CDR Rules, Schedule 3, clause 6.9.

Table 3: Commencement dates for new unrestricted ADIs

CDR data type	CDR data sharing commencement dates
Product data requests under Part 2 of the CDR Rules	On and from the day that is 12 months after the person became an unrestricted ADI
Consumer data requests under Part 4 of the CDR Rules other than complex requests	On and from the day that is 15 months after the person became an unrestricted ADI
Complex requests made by an accredited person	On and from the day that is 18 months after the relevant day after the person became an unrestricted ADI.

Information on what 'complex requests' are under the CDR Rules can be found in section 3.1.1 of this guide.

3.2. Application of the CDR Rules to the non-bank lenders sector

3.2.1. Commencement dates for data sharing in the non-bank lenders sector

The commencement date for data sharing obligations for data holders in the non-bank lenders sector depends on the type of data holder they are and the type of request they receive.[24] See the following table for details:

Table 4: Commencement dates for data sharing in the non-bank lenders sector

Data holder	CDR data sharing type	Commencement date
Initial providers	Product data obligations	13 July 2026
	Consumer data obligations – other than complex requests	9 November 2026
Non-bank lenders that become large providers on or before 13 July 2025	Product data obligations	13 July 2026
	Consumer data obligations – other than complex requests	10 May 2027
Non-bank lenders that become large providers after 13 July 2025	Product data obligations	12 months after the non-bank lender becomes a large provider
	Consumer data obligations – other than complex requests	15 months after the non-bank lender becomes a large provider

3.2.2. Complex requests

Data sharing obligations do not currently apply to complex requests for initial and large providers.[25] This means initial and large providers will not be required to respond to complex requests, or to provide the services needed to be able to respond to complex

[24] CDR Rules, Schedule 3, clauses 6.4 and 6.5.

[25] CDR Rules, Schedule 3, clauses 6.4(2) and 6.5(4).

requests (i.e. the services referred to in clauses 1.13(1)(c) to (e) of the CDR Rules). The policy intent of carving out complex requests is to avoid unnecessary or duplicative compliance burden for how non-bank lenders may be required to comply with this obligation in the future.[26]

Information on what 'complex requests' are under the CDR Rules can be found in section 3.1.1 of this guide.

3.3. Trial products

Data holders are not required to comply with CDR data sharing obligations in relation to a covered product while it is a trial product.[27] A covered product is a trial product if it is:

- for the purposes of the trial, supplied to 1000 customers or less
- offered with the description 'pilot' or 'trial', and
- offered with a statement specifying:
  - a trial period of 6 months or less, and
  - the product may be terminated before the end of the trial period, in which case CDR data in relation to the product may not be available for data sharing under the CDR Rules.

A product will be subject to data sharing obligations if it ceases to be a trial product. That is, if the product continues to be offered after the end of the trial period, or is supplied to over 1000 customers. In these circumstances, a data holder is required to comply with its CDR data sharing obligations in relation to the product. This involves responding to consumer or product data requests, including in relation to any required CDR data generated while the product was a trial product.

3.4. Direct requests from CDR consumers

Data sharing obligations currently do not apply in relation to direct requests from CDR consumers under Part 3 of the CDR Rules.[28] This means that CDR consumers who want to access their own CDR data must do so through an accredited person who would make a consumer data request to a data holder on the CDR consumer's behalf.

3.5. Entities that move from the non-bank lenders sector to the banking sector

A data holder might stop being a data holder in the non-bank lenders sector, and soon after become a data holder in the banking sector.

In these circumstances, if:

- a product or consumer data request was in progress in the non-bank lenders sector, or
- a current authorisation or consent relating to a product or consumer data request for non-bank lenders sector data was in place,

---

[26] Competition and Consumer (Consumer Data Right) Amendment (2025 Measures No. 1) Rules 2025, Explanatory Statement, paragraph 74.

[27] CDR Rules, Schedule 3, clauses 1.5 and 6.12.

[28] CDR Rules, Schedule 3, clauses 6.7 and 6.8.

that request, consent or authorisation remains effective as though it had been made by the data holder in the banking sector, and the non-bank lenders sector data was banking sector data.[29]

The data holder must deal with such requests, consents or authorisations in accordance with the CDR Rules.[30]

As soon as practicable after becoming a data holder in the banking sector, the data holder must notify CDR consumers whose product or consumer data requests are in progress in the non-bank lenders sector that:

- the data holder has ceased to operate in the non-bank lenders sector
- the data holder is now operating in the banking sector
- the data requested is now banking sector data, and
- the CDR consumer may, under rules 4.13, 4.20J and 4.25 of the CDR Rules, choose to withdraw an authorisation or consent given in respect of their existing data requests.[31]

The data holder must also notify each accredited person who made a current consumer data request that the data holder has ceased to operate in the non-bank lenders sector and the data holder is now operating in the banking sector.[32]

3.6. Exemptions from compliance with obligations

CDR participants can seek exemptions from complying with their obligations under the CDR, for example in relation to a particular product line.[33] 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.

[29] CDR Rules, Schedule 3, clauses 8.1(1)-(3).

[30] CDR Rules, Schedule 3, clauses 8.1(3)-(4).

[31] CDR Rules, Schedule 3, clauses 8.1(5).

[32] CDR Rules, Schedule 3, clauses 8.1(6).

[33] CCA, section 56GD.

4. Data holders' obligations under the Standards

Key points

- Under the CDR Rules, data holders must comply with the Standards. These set out the technical requirements for data sharing under the CDR.
- Data holders must also be familiar with the current version of the Consumer Experience Guidelines (CX Guidelines).
- The CDR Rules require CDR participants to have regard to the CX Guidelines when asking a CDR consumer to give or amend an authorisation.

Under the CDR Rules, data holders must comply with the Standards. These set out the technical requirements for data sharing under the CDR.

Under the CDR Rules, the Data Standards Chair, who is assisted by the DSB, must make standards for things such as:

- the format and process that data holders must use to respond to CDR consumer data requests
- the format and process that data holders must use to respond to accredited data recipients' requests for CDR data
- the processes for handling and protection of CDR data.[34]

The Standards are regularly revised to adapt to changing demands for functionality and available technological solutions. CDR participants may raise a Change Request or query regarding the Standards on the Standards Maintenance repository. Please refer to guidance on Standards Maintenance for more information.

Data holders should ensure they are consulting the current version of the Standards. For further information about what has changed when a new version of the Standards is released, see the Consumer Data Standards Changelog and archives and CDR Support Portal. If there is an inconsistency between the Standards and the CDR Rules on any point, the CDR Rules prevail on that point.

See Table 6 for an overview of the Standards.

4.1. 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.

[34] Rule 8.11 of the CDR Rules sets out all of the matters that the Data Standards Chair must make standards for.

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:

Table 5: Format of references to the Standards in this guide

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:		
Technical Standards	Banking APIs	Get Products
CX Standards	Authorisation Standards	Authorisation – Account selection

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

4.2. Overview of the Standards

Table 6: Overview of the Data 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	
High Level Standards	Contains high level standards that govern the Data Standards as a whole. These high-level standards apply to all CDR participants.
Industry Specific Application Programming Interfaces (APIs)[35]	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

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

	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.

4.3. Understanding the obligations contained in the Standards

CDR participant obligations to apply the Standards work in 2 ways:

- If the CDR Rules require compliance with the Standards, non-compliance with the Standards may constitute a breach of the CDR Rules.
- If the Standards are specified as binding Standards as required by the CDR Rules under section 56FA of the CCA, they apply as a contract between a data holder and each accredited data recipient.[36] A failure to comply with a binding Standard can be enforced through an application to the Federal Court by a person aggrieved by that failure or by the ACCC.[37]

4.3.1. Language used to describe obligations

There are different types of obligations in the Standards. They are identified 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
- the Consumer Experience section of the Standards provides - If unavailable accounts cannot be shown in the account selection step, data holders MAY display a generic explanation and instructions.

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.

[36] CCA, section 56FD.

[37] CCA, section 56FE.

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

- RFC 2119 provides that "SHOULD" or "RECOMMENDED" mean that there may be valid reasons for not conforming with that item in some circumstances, but the full implications must be understood and carefully weighed before doing so.
- As a matter of compliance and enforcement, where binding Standards stating a data holder "SHOULD" do something, the ACCC expects that CDR participants operate in accordance with the Standard unless the circumstances and implications indicate that conformance would not give effect to the intention of the Standard.

4.3.2. 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.[38]
- **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:
  - 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.

4.3.3. 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.

4.4. Consumer Experience (CX) Guidelines

Data holders must be familiar with the current version of the CX Guidelines. The CX Guidelines provide a model approach for guiding a CDR consumer through the authorisation process.

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 or amend

[38] See knowledge article on Data formats – schemas for more information on required fields.

an authorisation must, having regard to the CX Guidelines, be as easy to understand as practicable, including by the use of concise language and where appropriate, visual aids.[39]

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.

4.5. Other guidance material

Further resources regarding the Standards and CX Guidelines are included in the table below.

Table 7: Standards and guidelines resources

Resource	Description
CDR Support Portal	The CDR Support Portal publishes guides on technical and compliance-related matters.
Consumer Experience (CX) Checklist	The CX Checklist is a complete list of items referenced in the CX Guidelines including relevant rules, privacy safeguards, and CX standards. 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.

[39] CDR Rules, rule 4.22(b).

5. Product data obligations

Key points

- Data holders must provide an online service that can be used to make product data requests in relation to data that it holds, that discloses data in machine-readable form and conforms with the Standards.
- Any person may use a data holder's product data request service to request disclosure of 'required product data' or 'voluntary product data' held by the data holder.
- In response to a valid request to a data holder's product data request service a data holder must disclose required product data and may disclose voluntary product data.

5.1. Product data request service

CDR Rules: see rules 1.12 and 2.3

A person may use a data holder's product data request service to request disclosure of required product data or voluntary product data held by the data holder.[40]

Data holders must provide an online service that:

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

Table 8: Standards

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

5.2. Product data and covered products

In the banking and non-bank lenders sectors, required product data and voluntary product data is 'product specific data' about certain 'covered products'.

Product specific data is information that identifies or describes the characteristics of the 'covered product'. This includes information such as the type, name, price, features and eligibility requirements of a product.

[40] CDR Rules, rule 2.3.

A covered product in a particular sector is a product that is:

- listed in clause 1.4 of Schedule 3 the CDR Rules for that sector (see Table 9 below),
- publicly offered by or on behalf of a data holder, and
- offered to consumers by way of standard form contracts.[41]

5.2.1. What products may be a covered product?

The following products may be covered products if they are publicly offered by or on behalf of a data holder to consumers by way of a standard form contract.

Table 9: Products that may be a covered product

In the banking and non-bank lenders sectors	
• a personal credit or charge card account	• a line of credit (business)
• a business credit or charge card account	• an overdraft (personal)
• a residential home loan	• an overdraft (business)
• a home loan for an investment property	• asset finance (including standard vehicle financing and leases)
• a mortgage offset account	• a consumer lease
• a personal loan	• a reverse mortgage
• business finance	• a buy now, pay later product
• a loan for an investment	
• a line of credit (personal)	

In the banking sector only	
• a savings account	• a GST or tax account
• a call account	• a cash management account
• a term deposit	• a farm management account
• a current account	• a pensioner deeming account
• a cheque account	• a retirement savings account
• a debit card account	• a trust account
• a transaction account	• a foreign currency account.
• a personal basic account	

5.2.2. When is a product publicly offered by way of standard form contract?

The CDR Rules do not define when a product is considered to be 'publicly offered'. However, the ACCC generally considers this criteria should be interpreted broadly to make the benefits of CDR as widely available to consumers as is practicable.

A product does not need to be available to every member of the public to be considered publicly offered.[42] This means that a product offered to consumers who meet certain eligibility requirements, such as small business consumers, may be considered publicly offered.

[41] CDR Rules, Schedule 3, clause 1.4.

[42] CDR Rules, Schedule 3, clause 1.4(2).

The CDR Rules do not provide a definition of a 'standard form contract'. However, by way of example, the definition of a 'covered product' notes that section 27 of the Australian Consumer Law (ACL) sets out matters that a court may take into account when determining whether a contract is a standard form contract. Some of the relevant considerations, as set out at section 27 of the ACL, include:

- the level of bargaining power between the parties to the contract,
- whether there was an effective opportunity to negotiate the terms, and
- that the opportunity to negotiate changes to the terms of the contract was not merely minor or insubstantial in effect.

Individually tailored products are unlikely to be considered publicly available. Typically, these products are:

- not offered generally (and might only be available through 'invite')
- highly customised and negotiated, and
- not offered by way of standard form contract.

Additional information on covered products in the banking and non-bank lenders sectors can be found in the article Assessing whether a banking or non-bank lending product is in scope for CDR.

5.3. 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' in the banking and non-bank lenders sectors.

The meaning of these terms is the same in both sectors, however, the list of covered products in each sector is different (see section 5.2.1 of this guide for the products that may be covered products in each sector).

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

- must disclose the required product data, and
- may disclose the voluntary product data.

The below table describes what is considered to be 'required product data' and 'voluntary product data' in the banking sector and the non-bank lenders sector following the commencement of the Amending Rules on 4 March 2025:

Table 10: '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), and • is product specific data about a covered product (specifically data about the eligibility criteria, terms and conditions, price, or publicly available data about availability or performance)[43], and • is held in a digital form but does not relate to any of the following covered products: • a foreign currency account • a consumer lease • a reverse mortgage • a margin loan • asset finance that is non-standard vehicle finance.	Is all other CDR data that: • does not relate to a particular consumer(s), and • is product specific data about a covered product (i.e. information that identifies or describes the characteristics of the covered product)[44], and • is not required product data.

'Covered products' are described in section 5.2 of this guide.

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 4 of this guide).

5.4. Disclosure of product data

5.4.1. 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[45]
- the data must be disclosed in accordance with the Standards.

[43] See Note of clause 3.1(1) in Schedule 3 to the CDR Rules.

[44] Product specific data for voluntary product data includes all of the following information about the covered product: its type, its name, its price, including fees, charges and interest rates (however described), the features, and any associated benefits of the product (such as discounts and bundles), any terms and conditions applicable to the product, any customer eligibility requirements.

[45] CCA, section 56BD(2).

Table 11: Standards

Standards/ Guidelines	Section	Sub-section
Technical Standards	Banking APIs	Get Products, Get Product Detail and related payload schemas
Technical Standards	High Level Standards	Versioning; Uniform Resource Indicator Structure; HTTP Headers; HTTP Response Codes; Payload Conventions; Common Field Types; Pagination; ID Permanence; Extensibility
Technical Standards	Security Profile	Transaction Security, Cross-origin Resource Sharing
Technical 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.[46]

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.

Table 12: Standards

Standards/ Guidelines	Section	Sub-section
Technical Standards	High Level Standards	HTTP Response Codes – HTTP Status: 429 Too Many Requests
Technical Standards	Non-functional Requirements	Exemptions to Protect Service

5.5. 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.

If a data holder elects to disclose the data:

- the data must be disclosed using the data holder's product data request service

[46] CDR Rules, rule 2.5.

- a data holder can charge a fee for providing the data, but the fee should be reasonable[47]
- the data must be disclosed in accordance with the Standards.

Standards relevant to requests for voluntary product data include:

Table 13: Standards

Standards/ Guidelines	Section	Sub-section
Technical Standards	Schemas	*As relevant to the product data request*

5.6. 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.

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

CDR Rules: see rule 2.4 and Schedule 3, clause 7.1A

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.

The data holder that has the contractual relationship with the consumer (e.g. the white labeller) may agree with the other data holder (e.g. 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.[48]

The Amending Rules now also allow two data holders that are related bodies corporate to transfer data sharing obligations to each other.[49] For example, there may be situations where a consumer facing entity would not ordinarily be required to comply with data sharing obligations, but where it may be more appropriate that they are the entity that complies.

---

[47] See paragraph 1.136 of the *Treasury Laws Amendment (Consumer Data Right) Act 2019* (Cth), Explanatory Memorandum which states "the Government expects the person to determine and set their own reasonable fee".

[48] CDR Rules, rule 2.4. For further context for this rule, see the Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020, Explanatory Statement.

[49] CDR Rules, Schedule 3, clause 7.1A.

This ability to transfer data sharing obligations is also available between a data holder in the non-bank lenders sector and a data holder in the banking sector (i.e. both data holders do not need to be part of the same sector).

Where an election is made (either under rule 2.4 or clause 7.1A of Schedule 3), both data holders must agree to this in writing.

The approach to sharing consumer data for white label products is outlined in section 6.5 of this guide. The ACCC understands that there are a wide variety of white label arrangements in the banking and non-bank lenders sectors and that particularly complex arrangements could pose compliance issues. The ACCC is open to discussing these issues with data holders and may consider potential exemption applications where a white labeller is not able to comply with CDR obligations.

6. Consumer data

Key points

- Data holders must provide an 'accredited person request service' for accredited persons to make consumer data requests for eligible consumers.
- Data holders must also provide a 'CDR consumer dashboard' for CDR consumers to manage authorisations to disclose CDR data.
- Additional requirements apply in relation to accounts held by non-individuals or partnerships, joint accounts, and individual accounts with additional authorised users.
- If a consumer authorises disclosure, data holders must disclose required consumer data and may disclose voluntary consumer data in accordance with the CDR Rules and Standards.
- Data holders must take reasonable steps to ensure the data they disclose through the CDR is correct, and comply with the CDR Rules when they become aware that disclosed data is inaccurate, out of date, or incomplete.

6.1. 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 and non-bank lenders sectors, a CDR consumer is 'eligible' if:

- they are an account holder or secondary user for an open account with the data holder, and
- 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.

6.2. Consumer data request service

CDR Rules: see rule 1.13

6.2.1. Accredited person request service

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 in relation to a relevant account, and
- discloses data in machine-readable form, and
- conforms with the Standards.

The relevant Standards include the following:

Table 14: Standards

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

6.2.2. Additional requirements for non-individual and partnership consumers

Data holders in the banking sector are 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 partners in a partnership to nominate one or more individuals (known as 'nominated representatives') that can give, amend and withdraw authorisations on their behalf.[50] Data holders in the non-bank lenders sector are not currently required to provide such a service.[51]

Detailed guidance on nominated representatives and business consumers is available in this Nominated representatives, non-individuals and partnerships fact sheet.

6.2.3. Additional requirements for individual accounts with additional authorised users

CDR Rules: see rules 1.13 and 1.15(5)(b)

In the banking sector, an individual CDR consumer who is an account holder can nominate someone to be a secondary user who can authorise data sharing from the account.[52] Data holders in the non-bank lenders sector are not currently required to provide this functionality.[53]

A person is a 'secondary user' of an account if the person:

- is at least 18 years of age,
- has 'account privileges' for the account, and
- is the subject of a 'secondary user instruction' — an instruction from the account holder (who is also at least 18 years of age) to the data holder to treat the individual as a secondary user.[54]

---

50 CDR Rules, rules 1.13(1)(c)(i) and 1.13(1)(d)(i).

51 For further information, see section 3.2 of this guide - Application of the CDR Rules to the non-bank lenders sector.

52 For example, a secondary user can consent to AP disclosure consents, trusted adviser disclosure consents and insight disclosure consents. See CDR Rules, rule 1.10A(2) for further examples of disclosure consent categories.

53 For further information, see section 3.2 of this guide - Application of the CDR Rules to the non-bank lenders sector.

54 CDR Rules, rule 1.7(1), see definitions of 'secondary user' and 'secondary user instruction'.

A person has account privileges in relation to an account the person holds with a data holder, if:

- the account is for a covered product, and
- the person is able to make transactions on the account.[55]

In the banking sector:

- 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 1.15(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 at any time (rule 1.15(5)(b)). Rule 1.15(5) applies once there is a secondary user on an account (i.e. where a secondary user instruction is in place).

The ACCC encourages data holders in the banking sector 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).

Standards and CX Guidelines relating to secondary user instructions include:

Table 15: Standards and CX Guidelines

Standards/ Guidelines	Section	Sub-section
Technical standards	Withdrawal standards	Withdrawal: Secondary User Instruction
CX Guidelines	Consent Management (Data Holder)	Account permissions (Secondary User)

Additional information on secondary users can be found in the Secondary users in the banking sector fact sheet and the Joint account implementation guide.

6.3. What data can be requested?

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 relation to a relevant account.

A relevant account, in relation to a CDR consumer, means an account that is held with a data holder of banking sector data or non-bank lenders sector data and is, or is for, a covered product[56], and that:

- is in the name of the CDR consumer alone
- is a joint account of which the CDR consumer is one of the account holders
- is a partnership account for a partnership in which the CDR consumer is a partner, or

[55] CDR Rules, Schedule 3, clause 2.2.

[56] See sections 5.1.1 and 5.1.2 of this guide for information on covered products.

- is an account for which the CDR consumer is a secondary user.[57]

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.

The terms 'required consumer data' and 'voluntary consumer data' have the same meaning in both sectors. However, the list of covered products in each sector is different (see section 5.2 of this guide for information on what covered products are in each sector).

The following table describes what 'required consumer data' and 'voluntary consumer data' are in the banking sector and the non-bank lenders sector:

Table 16: Required consumer data and voluntary consumer data

Required consumer data	Voluntary consumer data
Is CDR data in relation to a 'relevant account' that: • is dated after 1 January 2017 for banking sector data or 1 January 2020 for non-bank lenders sector data • is held in a digital form • relates to one or more CDR consumers And is either: • customer data, or • account data (except for account data that relates to an authorisation for a direct debit from the account that occurred more than 13 months before that time), or • transaction data (except in relation to a transaction that occurred more than 2 years before that time), or • product specific data,[58] But is <u>not</u> data that relates to: • a foreign currency account • a consumer lease • a reverse mortgage • a margin loan • an asset finance that is non-standard vehicle finance (for example a novated lease), or	Is CDR data in relation to a 'relevant account' that: • is dated after 1 January 2017 for banking sector data, or 1 January 2020 for non-bank lenders sector data • relates to one or more CDR consumers, and • is not required CDR data.

[57] CDR Rules, Schedule 3, clause 3.2(1).

[58] See CDR Rules, Schedule 3, clause 1.3 for definitions of consumer data, account data, transaction data and product specific data. Product specific data would cover any product prices that were negotiated individually with a CDR consumer, the interest rates current at the time of the request, any other interest rates applicable and any terms and conditions associated with those interest rates, and any features and benefits negotiated individually with a CDR consumer (see Note 1 of clause 3.2(2) in Schedule 3 to the CDR Rules).

- a closed account.[59]

The following CDR data is neither required consumer data nor voluntary consumer data:

- Account, transaction or product specific data in relation to a joint account or partnership account for which any of the individuals who are account holders or partners in the relevant partnership is less than 18 years at that time.
- CDR data relating to a debt of a CDR consumer, if the data was acquired by a data holder acting in its capacity as a debt collector or debt buyer.
- For a consumer data request made by or on behalf of a particular person, customer data in relation to any account holder or secondary user other than that person.
- For a CDR consumer that is an individual, the CDR consumer's date of birth.[60]
- Financial hardship information,[61] or repayment history information,[62] where the information was disclosed by or to a credit reporting body.

6.3.1. 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.[63]

Data holders are required to share this data if it is held in a digital form, even if it is not available to the consumer digitally.[64] 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).

6.3.2. Changes to the meaning of required consumer data and voluntary consumer data

Before 4 March 2025, the meaning of the terms 'required consumer data' and 'voluntary consumer data' were slightly different. The below table outlines key changes to these terms made by the Amending Rules:

[59] CDR Rules, Schedule 3, clauses 3.2(3) and (7).

[60] CDR Rules, Schedule 3, clause 1.3(1).

[61] Within the meaning of subsection 6QA(4) of the *Privacy Act 1988*.

[62] Within the meaning of subsection 6V(1) of the *Privacy Act 1988*.

[63] See section 6.1 of this guide for information on 'eligible' consumers and Note 2 of clause 3.2(2) in Schedule 3 to the CDR Rules.

[64] CDR Rules, Schedule 3, clause 3.2(2).

Table 17: Recent changes to the terms 'required consumer data' and 'voluntary consumer data'

Type of CDR data	Current classification (which commenced on 4 March 2025)	Previous classification (before 4 March 2025)
Data relating to the following covered products • a foreign currency account • a consumer lease • a reverse mortgage • a margin loan • an asset finance that is non-standard vehicle finance (such as a novated lease or fleet finance).[65]	Voluntary consumer data	Required consumer data
Data relating to accounts that have been closed for less than 2 years	Voluntary consumer data	Required consumer data
Data from a transaction that occurred more than 2 years ago but less than 7 years ago	Voluntary consumer data	Required consumer data

The above changes do not have a retrospective impact on a consent that a consumer has given before the commencement of the Amending Rules on 4 March 2025.[66]

This means that a consent to disclosure of required consumer data given by a CDR consumer before 4 March 2025 in relation to data listed in Table 17 will remain effective until the consent expires in accordance with CDR Rule 4.14, even if that data is now classified as voluntary consumer data.

6.4. Registration on the CDR participant portal

Data holders are 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. 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.

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

CDR Rules: see Schedule 3, clause 7.1A

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

[65] CDR Rules, Schedule 3, clauses 3.2(2) and (3).

[66] Competition and Consumer (Consumer Data Right) Amendment (2025 Measures No. 1) Rules 2025, Explanatory Statement, paragraph 39.

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 (e.g. where a brand owner bank distributes a credit card on behalf of a white labeller bank) each data holder may have data sharing obligations in relation to the product. This would depend on the facts of each case, such as whether the consumer is eligible in relation to the data holder and whether the data holder holds required consumer data.[67]

However, to avoid unnecessary duplication and to ensure a consistent approach with rule 2.4 (relating to product data), the ACCC generally considers the data holder that has the contractual relationship with the consumer (e.g. the white labeller):

- is responsible for responding to consumer data requests, and
- may agree with the other data holder (e.g. the brand owner) that the brand owner will perform that obligation on behalf of the white labeller.

In this example, the ACCC generally considers that 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.

For additional certainty, the Amending Rules now allow a data holder in the banking or non-bank lenders sector to elect to comply with the CDR Rules in the place of another data holder in the banking or non-bank lenders sector in relation to a covered product, where either:

- the first-mentioned data holder enters into the contract with the consumer to provide the product, but the second-mentioned data holder offers the product on behalf of the first-mentioned data holder, or
- both data holders are related bodies corporate for the purposes of the CCA.[68]

Both data holders must agree to this in writing.

The ability to transfer data sharing obligations is available between a data holder in the non-bank lenders sector and a data holder in the banking sector (i.e. both data holders do not need to be part of the same sector).

The ACCC understands there are a wide variety of white label arrangements in the banking and non-bank lenders sectors and that particularly complex arrangements could pose compliance issues. The ACCC is open to discussing these issues with data holders and may consider potential exemption applications where a white labeller is not able to comply with CDR obligations.

Further guidance on white label products can be found in the following:

- Brands in the Consumer Data Right Ecosystem
- ADI responsibility for Data Holder Brands
- White Labelled brands in the CDR

For additional guidance on how white label brands are currently registered, see the CDR participant on-boarding guide.

---

[67] CDR Rules, see rule 1.10B for the meaning of 'eligible' and clause 3.2 of Schedule 3 for the meaning of 'required consumer data'.

[68] CDR Rules, Schedule 3, clause 7.1A and the Competition and Consumer (Consumer Data Right) Amendment (2025 Measures No. 1) Rules 2025, Explanatory Statement, paragraph 97.

6.6. 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:

- allow a consumer to withdraw authorisations to disclose CDR data at any time
- be simple and straightforward to use and no more complicated than the process for authorising the disclosure of CDR data
- be prominently displayed and readily accessible to the CDR consumer
- display a message as part of the withdrawal process, explaining the consequences of withdrawing an authorisation in accordance with the Standards
- contain the following details of each authorisation to disclose CDR data:
    - 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 or expired
    - details of any amendments that have been made to the authorisation[69]
    - what data was disclosed
    - when data was disclosed
    - the accredited data recipient data was disclosed to[70]
- 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).

The ACCC generally considers the consumer dashboard does not need to contain details of authorisations to disclose CDR data where the authorisation was given more than 6 years ago. This timing aligns with data holders' record keeping obligations under rule 9.3 of the CDR Rules.

Standards and CX Guidelines relevant to CDR consumer dashboards include:

[69] Data holders are required to include this information from 1 July 2024 – see rule 1.15(3A). The Data Standards Chair has approved the decision to make Standards to reflect this requirement as well as the requirement to include a note on data holder dashboards advising consumers to check with relevant data recipients for more information on how their CDR data is being handled – see Decision 334: Data holder dashboards.

[70] CDR Rules, rule 7.9 and CCA, section 56EM (Privacy Safeguard 10).

Table 18: Standards and CX Guidelines

Standards/ Guidelines	Section	Sub-section
CX Standards	Dashboard Standards	Data holder dashboards
CX Standards	Withdrawal Standards	Withdrawing authorisation: Consequences; Withdrawing authorisation: Redundant data
CX Guidelines	Consent Management (Data holder)	Authorisations; Withdrawal

6.6.1. Additional requirements for non-individuals and partnerships

In the banking sector, data holders must only allow nominated representatives to use the CDR consumer dashboard to manage authorisations on behalf of a non-individual or partnership.[71] A non-individual consumer or partnership that does not have a nominated representative will not be able to give or amend authorisations, or use the dashboard to manage authorisations.[72] Accordingly, the data holder will be neither required nor permitted to disclose the requested CDR data under these rules.[73]

Section 6.2.2 of this guide contains information on how non-individual consumers and partners in a partnership can nominate one or more individuals as a nominated representative. Further information is also available in the Nominated representatives of non-individuals and partnerships in the CDR fact sheet.

These additional requirements do not apply in the non-bank lenders sector as initial and large providers are not required to meet data holder obligations relevant to data sharing for non-individuals and partnerships.[74]

6.6.2. Additional requirements for individual accounts with secondary users

In the banking sector, once there is a secondary user on an account (i.e. where a secondary user instruction is in place),[75] the consumer dashboard provided by the data holder to the account holder must have additional functionality.[76] This includes the ability to withdraw a secondary user instruction at any time.[77]

See section 6.2.3 of this guide for additional information on secondary user instructions.

These additional requirements do not apply in the non-bank lenders sector as initial and large providers are not required to meet data holder obligations relevant to secondary users.[78]

---

71 Data holders in the non-bank lenders sector are not currently required to provide this service. For further information, see section 3.2 of this guide - Application of the CDR Rules to the non-bank lenders sector.

72 CDR Rules, rule 1.15(2A).

73 CDR Rules, rule 1.13(1), Note 3.

74 For further information, see section 3.2 of this guide - Application of the CDR Rules to the non-bank lenders sector.

75 See section 6.2.3 of this guide for additional information on secondary user instructions.

76 Data holders in the non-bank lenders sector are not currently required to provide this service. For further information, see section 3.2 of this guide - Application of the CDR Rules to the non-bank lenders sector.

77 CDR Rules, rule 1.15(5)(b).

78 For further information, see section 3.2 of this guide - Application of the CDR Rules to the non-bank lenders sector.

6.6.3. Additional requirements for joint accounts

CDR Rules: see rule 4A.13

Data holders in the banking sector 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.

Data holders in the non-bank lenders sector are not currently required to meet data holder obligations relevant to data sharing for joint accounts.[79] Standards and CX Guidelines relevant to joint accounts include:

Table 19: Standards and CX Guidelines

Standards/ Guidelines	Section	Sub-section
CX Standards	Withdrawal standards	Withdrawal: Joint accounts
	Notification standards	Notifications: Joint Account Alerts; Alternative Notification Schedules for Joint Accounts
Technical 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
CX Guidelines	Authorise	Authorisation to disclose joint account data
	Consent Management	Withdrawal (Default and Withdrawing approvals); Account permissions (Joint account disclosure option management service); Joint account notification settings

6.7. Joint accounts

Special rules apply to consumer data requests for CDR data from joint accounts. These rules apply to data holders in the banking sector. Data holders in the non-bank lenders sector are not required to support consumer data sharing for joint accounts.[80]

6.7.1. Eligibility

To be able to share joint account data, all joint account holders must be 'eligible' consumers in their own right.[81] This means, for example, that if a relevant joint account

[79] For further information, see section 3.2 of this guide - Application of the CDR Rules to the non-bank lenders sector.

[80] For further information, see section 3.2 of this guide - Application of the CDR Rules to the non-bank lenders sector.

[81] CDR Rules, rule 1.7(1), see definition of '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 – 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 6.1 of this guide.

6.7.2. 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.

6.7.3. 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.[82]

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.[83] These changes are made using the disclosure option management service.

6.7.4. 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

[82] CDR Rules, rule 4A.7.

[83] CDR Rules, rule 4A.8.

- 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.

Relevant Standards and CX Guidelines include those set out in Table 19 in section 6.6.3 of this guide.

6.7.5. 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.[84] 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.

Relevant Standards and CX Guidelines include those set out in Table 18 in section 6.6 of this guide.

6.7.6. Joint account obligations and preventing physical, psychological 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).[85]

For more information on joint accounts, see the Joint accounts implementation guidance and Notification Standards in relation to Joint account notifications & Alternative Notification Schedules.

6.8. 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.

---

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

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

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.[86]

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

- the name of the accredited data recipient that made the request[87]
- 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.[88]
- 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,[89] 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[90] and the request for authorisation itself must be in accordance with the Standards on voluntary consumer data[91] and required consumer data[92] (subject to rule 4.7 of the CDR Rules which is explained in section 6.10 below).
- The process for seeking authorisation should be easy to understand for consumers.[93]

---

86 CDR Rules, rule 4.5.

87 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'.

88 While certain consents given by a CDR business consumer to an ADR can have a duration of up to 7 years, the corresponding authorisations with a data holder continue to have a maximum duration of 12 months before renewal – for more information, see guidance on CDR business consumers.

89 This scenario is distinct from when a consumer amends an existing consent. See rule 4.12B of the CDR Rules.

90 CDR Rules, rule 4.22(a).

91 CDR Rules, rule 4.5(2)(b).

92 CDR Rules, rule 4.5(3)(b).

93 CDR Rules, rule 4.22(b).

Relevant Standards and CX Guidelines include:

Table 20: Standards and CX Guidelines

Standards/ Guidelines	Section	Sub-section
Technical 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
	Authorisation Scopes	All sub-sections
CX Standards	Data Language Standards: Common	Language to be used; Detailed scope requests
	Customer Language: Common	All sub-sections
	Profile Scope and Standard Claims: Common	All sub-sections
	Authentication Standards	All sub-sections
	Authorisation Standards	All sub-sections
CX Guidelines	Authenticate	Redirect with One Time Password
	Authorise	Authorisation to disclose; Amending authorisations; Authorisation to disclose joint account data

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 6.8.1 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)).

6.8.1. 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:
        - the information described above 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.[94]
3. if the **non-disclosure** option applies, the data holder must refuse to disclose the requested CDR data.

6.8.2. 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.

[94] For more information about the withdrawal of approvals, see our Joint Account implementation Guidance.

Table 21: Standards and CX Guidelines

Standards/ Guidelines	Section	Sub-section
CX Standards	Amending Authorisation Standards	All sub-sections
CX Guidelines	Amending Authorisations	All sub-sections

6.8.3. When a consumer withdraws their authorisation

CDR Rules: see rules 4.25 and 4.26A

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.

A data holder must also notify the accredited data recipient in accordance with the Standards where an authorisation otherwise expires– for example when relevant authorisations expire because a CDR consumer ceases to be eligible in relation to the data holder.[95]

Table 22: Standards and Guidelines

Standards/ Guidelines	Section	Sub-section
CX Standards	Withdrawal Standards	Withdrawing authorisation: Consequences; Withdrawing authorisation: Redundant data
CX Guidelines	Consent Management (Data holder)	Withdrawal (default example)

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.

[95] CDR Rules, rule 4.26(1)(c).

Where a joint account holder withdraws an authorisation:

- 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[96]
- consumer dashboards must be updated to reflect the withdrawal[97]
- the data holder must notify joint account holders that the authorisation has been withdrawn through its ordinary means of contacting them[98]
- the data holder must notify the accredited person that the authorisation has been withdrawn, in accordance with the Standards.[99]

6.9. 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.

Table 23: Standards:

Standards/ Guidelines	Section	Sub-section
Technical Standards	Industry Specific APIs	As relevant to the consumer data requested
Technical Standards	DCR APIs	All API definitions are applicable to commence sharing of consumer data
Technical Standards	Admin APIs	Admin APIs impact the reporting of consumer data sharing
Technical Standards	High Level Standards	Versioning; URI Structure; HTTP Headers; HTTP Response Codes; Payload Conventions; Common Field Types; Pagination; ID Permanence; Extensibility
Technical Standards	Security Profile	Tokens; Identifiers and Subject Types; Transaction Security
Technical 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.[100]

---

96 CDR Rules, rule 4.25.

97 CDR Rules, rules 1.15 and 4A.13(1)(c).

98 CDR Rules, rule 4A.14(1).

99 CDR Rules, rule 4.26A.

100 CDR Rules, rule 7.9 and CCA, section 56EM (Privacy Safeguard 10). The OAIC's CDR privacy safeguard guidelines contain further information about Privacy Safeguard 10.

6.9.1. Joint accounts

CDR Rules: see rule 4A.10

See also sections 6.6.3 and 6.7 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.

6.10. 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, psychological 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 provision in the CDR Rules provides that the requested CDR data must not be disclosed.

Relevant standards include:

Table 24: Standards

Standards/ Guidelines	Section	Sub-section
Technical Standards	High Level Standards	HTTP Response Codes – HTTP Status: 403 Forbidden, HTTP Status: 429 Too Many Requests
Technical Standards	Non-functional Requirements	Exemptions to Protect Service

6.11. 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, in any event, within 5 business days after the data holder becomes 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.

6.12. 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.

7. Data holders must establish dispute resolution processes

Key points

- A data holder in the banking or non-bank lenders sectors 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.
- A data holder in the banking or non-bank lenders sectors must be a member of the recognised external dispute resolution scheme operated by the Australian Financial Complaints Authority.

7.1. 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 271: Internal Dispute Resolution, which is tailored to their business.

Table 25: Relevant Provisions of ASIC Regulatory Guide 271

Matters to be dealt with	Relevant paragraphs of Regulatory Guide 271: Internal dispute resolution current as at July 2025
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.

7.2. External dispute resolution

CDR Rules: see rules 1.7(1), 6.2 and Schedule 3, clause 5.2

A data holder must be a member of a recognised external dispute resolution scheme in relation to CDR consumer complaints. For the banking and non-bank lenders sectors, a data holder meets the external dispute resolution requirements if it is a member of the recognised external dispute resolution scheme operated by the Australian Financial Complaints Authority Limited for the relevant sector.[101]

[101] Note, the *Competition and Consumer (Consumer Data Right—Recognised External Dispute Resolution Schemes) Instrument 2021* has not yet been updated to include the non-bank lenders sector.

8. CDR policy

CDR Rules: see rule 7.2

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

Key points

- Data holders must have a CDR Policy and make the policy available to consumers free of charge.
- Data holders must take reasonable steps to establish and maintain internal practices, procedures and systems to ensure compliance with their CDR obligations.

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.

9. Record keeping requirements

CDR Rules: see rule 9.3

Key points

- Data holders must keep certain records.
- CDR consumers can request copies of the data holder's records that relate to the consumer's authorisations or complaints.
- The ACCC can request copies of the records through an audit or for other compliance purposes.

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 under rule 2.4(5) the data holder has entered into regarding the obligation to disclose product data for white labelled products
- any election by the data holder under clause 7.1A(1) of Schedule 3 to comply with the CDR Rules in place of another data holder
- 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 consumer complaints and CDR complaint data, as defined by rule 1.7
    - CDR consumer complaint means any expression of dissatisfaction made by a CDR consumer to or about a CDR participant or CDR representative that relates to:
        - that person's CDR obligations or compliance with those obligations; or
        - the provision to the CDR consumer, by that person, of goods and services the CDR consumer has consented to;

        where a response or resolution could reasonably be expected.
    - CDR complaint data 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 7.1 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 certain data holder 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).

10. Reporting requirements

Key points

- Data holders must submit CDR reports twice a year to the ACCC and OAIC.
- 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.
- Data holders must make the Get Metrics API available so the ACCC can obtain operational statistics.

10.1. Reporting requirements

10.1.1. Biannual CDR reporting

CDR Rules: see rule 9.4

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

Table 26: Report due dates

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, their obligation to report begins from that earlier date.

The reports must be in the approved format and contain specific information.[102]

10.1.2. 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 12 of the Participant Portal User Guide for more details.

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

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

[102] A template of the approved reporting form is available on the CDR website.

10.1.3. CDR complaint data summary

'CDR complaint data'[103], 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.[104]

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

Further information on CDR consumer complaints can be found in the ACCC's article on *Recording and reporting on CDR consumer complaints*.

10.1.4. 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[105], and
- consumer data requests made by accredited persons on behalf of consumers received during the relevant reporting period.[106]

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.

---

[103] See the definition in rule 1.7 of the CDR Rules.

[104] 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.

[105] This refers to direct-to-consumer data sharing requests made under Part 3 of the CDR Rules. However, we note that direct-to-consumer obligations have not been enabled and there is currently no timeframe for when these obligations will apply to data holders. As such, we currently expect data holders to report a 0 or null value for this field in their reports.

[106] 'Received' means the request for CDR data reached the data holder's system and the data holder can provide a response to the request.

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.

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

Normally a data holder must share required data in response to a valid request that it receives. However, in some circumstances a data holder may refuse to disclose CDR data in response to a request.[107]

A data holder must inform the requester, CDR consumer, or accredited person if they are refusing a request in accordance with the Standards.[108] The Standards enable data holders to provide error codes to indicate the reason that CDR data has not been disclosed.

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

Table 27: CDR Rules relating to refusal to disclose CDR data and corresponding error codes

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 CDR data under the CDR Rules.

[107] CDR Rules, rules 2.5(1), 3.5(1) and 4.7(1).

[108] CDR Rules, rules 2.5(2), 3.5(2) and 4.7(3).

If a request is not received, or not valid, data holders cannot provide CDR 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 on the CDR Support Portal, such as the article on Refusals to disclose during outages and the Consumer Data Standards Guide on Outages. A summary table can be found below:

Table 28: Summary of HTTP codes

Request attribute		Data holder obligation	HTTP code provided to requester
Valid	Received		
Yes	Yes	Must disclose required CDR 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 requests outside the /cds-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 in rule 4.7 of the CDR Rules, such as for the avoidance of harm or abuse[109]).

10.2. Updating the CDR register

CDR Rules: see rules 5.24 and 5.25

The ACCC, as Accreditation Registrar, must create and maintain a database that includes certain information required for CDR data requests to be processed, including a list of data holders and certain details relating to those data holders, e.g. a hyperlink to data holder's web site and CDR policy. The Accreditation Registrar may require a data holder to provide this information or updates to that information.

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.

[109] For further information, see section 6.10 of this guide – Circumstances in which a data holder can refuse to disclose required consumer data.

10.3. 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.[110]

Table 29: Standards

Standards/ Guidelines	Section	Sub-section
Technical Standards	Admin APIs	ResponseMetricsListV5

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, or has provided data that does not meet the requirements of the Standards.[111]

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 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/.

[110] The Admin API Standard, specifically Get Metrics API and associated Schema include requirements to be met by CDR participations in relation to the performance and availability of systems to respond to requests, and public reporting of information relating to compliance with those requirements. The DSB is required to make related Standards as set out in rule 8.11(1)(f).

[111] The DSB may develop binding data standards and if a person who is under an obligation to comply with those standards fail to meet that obligation, an application to the Court may be made by the ACCC or a person aggrieved by the failure. See sections 56FD and 56FE of the CCA.