Australian Government

Consumer Data Right

# Compliance guide for data holders

## Energy sector

June 2024

| Version Control | | |
|---|---|---|
| May 2022 | Version 1 | First version of Guide |
| February 2023 | Version 2 | Editorial changes |
| December 2023 | Version 3 | Updated Guide to reflect amendments made in version 5 of the CDR Rules. |
| June 2024 | Version 4 | Updated links. Amended text at section 1.5 to clarify product data sets in the energy sector. |

# Table of Contents


Compliance guide for data holders ..... 0

1. Introduction ..... 6

1.1. The Consumer Data Right ..... 6

1.1.1. The CDR agencies ..... 6

1.1.2. Compliance and Enforcement Policy ..... 6

1.2. Regulatory framework ..... 7

1.3. The CDR agencies ..... 7

1.4. Compliance and Enforcement Policy ..... 8

1.5. CDR in the energy sector ..... 8

1.6. This guide ..... 8

1.7. Data holders' roles and obligations ..... 9

1.7.1. Roles ..... 9

1.7.2. Obligations ..... 9

1.8. Commencement of obligations ..... 9

1.8.1. Exemptions from compliance with obligations ..... 9

1.8.2. Additional requirements for compliance with privacy safeguards ..... 10

1.8.3. Additional requirements for accredited data recipients ..... 10

2. Consumer Data Standards ..... 10

2.1. The Standards ..... 10

2.1.1. References to the Standards in this guide ..... 11

2.1.2. Overview of the Standards ..... 11

2.2. Understanding data holders' obligations under the Standards ..... 12

2.2.1. Language used to describe obligations ..... 12

2.2.2. Mandatory, optional and conditional fields ..... 13

2.2.3. Normative Standards ..... 14

2.3. Consumer Experience (CX) Guidelines ..... 14
2.4. Further information ..... 14
3. Product data ..... 15
3.1. Product data requests ..... 15
3.2. Required product data and voluntary product data ..... 15
3.3. Use of disclosed data ..... 16
3.4. Commencement of product data obligations ..... 16
4. Consumer data ..... 17
4.1. CDR consumers ..... 17
4.1.1. Eligible CDR consumers ..... 17
4.1.2. Energy arrangements and accounts ..... 18
4.2. Data holders ..... 18
4.2.1. Primary and secondary data holders ..... 18
4.3. Retailers ..... 19
4.3.1. Initial retailers ..... 20
4.3.2. Larger retailers ..... 20
4.3.3. Small retailers ..... 20
4.3.4. Complex requests ..... 21
4.3.5. Reciprocal data holders ..... 21
4.4. Commencement of consumer data obligations ..... 21
4.5. Registration on the CDR Participant Portal ..... 22
5. Consumer data requests ..... 22
5.1. Consumer data requests ..... 22
5.1.1. Required consumer data and voluntary consumer data ..... 23
5.1.2. Requests for consumer data from white label products ..... 24
5.2. Consumer data request service ..... 25
5.3. CDR consumer dashboard ..... 25
5.3.1. Offline customers ..... 26
5.3.2. Consumer dashboard requirements ..... 27

5.3.3. Non-individuals and partnerships ..... 27
5.3.4. Joint accounts ..... 27
5.4. Joint accounts ..... 28
5.4.1. Disclosure options for joint accounts ..... 28
5.4.2. Changing disclosure options ..... 29
5.4.3. Disclosure option management service ..... 29
5.4.4. Informing other account holders when one account holder selects/changes a disclosure option ..... 30
5.4.5. Joint account obligations and preventing physical, psychological or financial harm or abuse ..... 31
5.5. Secondary users ..... 31
5.5.1. Account privileges in the energy sector ..... 32
6. Disclosing consumer data ..... 32
6.1. Requesting consumer authorisation to disclose CDR data ..... 32
6.1.1. If the request relates to a joint account ..... 34
6.2. When a consumer amends or withdraws consent ..... 34
6.2.1. Amendment to consent ..... 34
6.2.2. Withdrawal of authorisation ..... 35
6.2.3. A joint account holder gives, amends or withdraws their authorisation or the authorisation expires ..... 35
6.3. How to disclose consumer data ..... 36
6.4. When can a data holder refuse to disclose required consumer data? ..... 37
6.5. Disclosing incorrect data ..... 38
6.6. Correcting incorrect CDR data ..... 38
7. Dispute resolution processes ..... 39
7.1. Internal dispute resolution ..... 39
7.2. External dispute resolution ..... 39
8. CDR policy ..... 40
9. Record-keeping requirements ..... 41
10. Reporting requirements ..... 42
10.1. Reporting requirements ..... 42

10.1.1. Biannual CDR reporting ..... 42
10.1.2. Submitting the reporting form ..... 43
10.1.3. CDR complaint data summary ..... 43
10.1.4. CDR data requests received ..... 44
10.1.5. Refusals to disclose CDR data – total number and reasons ..... 44
10.2. Updating the register ..... 46
10.3. Reporting to the CDR Register ..... 46

## Important notice

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

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

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

## Guidance Revision History

Version 3 of this Guide, published in December 2023, includes the following changes in relation to the amendments made in version 5 of the CDR rules:

- Minor revisions to reflect the corrected definition of a 'large customer' in v5 of the CDR rules (section 4.3.4)
- Removal of commencement dates for data sharing obligations which have since passed (section 4.4)
- Additional text stating that from 1 July 2024, data holders are required to include details about amendments to authorisations on a consumer's dashboard (section 5.3.2)
- Minor updates to the text regarding notification requirements when an authorisation is withdrawn or otherwise expires (section 6.2.2)
- Minor revisions to the text on the circumstances in which a data holder can refuse to disclose required consumer data (section 6.4)
- Revised text clarifying the requirements for external dispute resolution scheme membership by energy retailers that are also accredited persons (section 7.2)
- Revised text outlining the requirements for data holders to keep records of CDR consumer complaints, in addition to CDR complaint data (section 9)
- Minor updates to clarify the reporting of consumer data requests made directly by consumers (section 10.1.4)

Version 2 of this Guide, published in February 2023, includes the following changes that have been made since the Guide was first published in May 2022:

- Editorial changes to improve readability
- Removal of references to commencement dates that have since passed
- New text clarifying the CDR data sharing obligations for consumers with multiple energy accounts (section 4.4)
- New text detailing the criteria for secondary users in the energy sector (section 5.5)

# 1. Introduction

## 1.1. The Consumer Data Right

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

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

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

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

### 1.1.1. The CDR agencies

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

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

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

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

We use a risk-based approach to monitoring and assessing compliance matters and taking enforcement action. We cannot pursue all matters that come to our attention. Our role is

to focus on those circumstances that will, or have the potential to, cause significant harm to the CDR regime or result in widespread consumer detriment.

## 1.2. Regulatory framework

The CDR is regulated by a framework that consists of:

- legislation including the *Competition and Consumer Act 2010* (CCA), *Privacy Act 1988* and the *Australian Information Commissioner Act 2010*.
    - the core legislative provisions are contained in Part IVD of the CCA, including provisions under which the CDR rules and standards are made and provisions in relation to the roles of the Data Recipient Accreditor and the Accreditation Registrar are set out
- designation instruments made under the legislation, including the *Consumer Data Right (Energy Sector) Designation 2020* (the Energy Sector Designation), which designates the energy sector as subject to the CDR
- the *Competition and Consumer (Consumer Data Right) Rules 2020* made under the legislation (CDR Rules)
    - You can find the most recent version of the CDR Rules on the Federal Register of Legislation.
- laws relevant to the management of CDR data for the energy sector:
    - the National Electricity Law (NEL)
    - the National Energy Retail Law (NERL)
    - the *Electricity Industry Act 2000* (Vic) (the Victorian Act)
- the *Competition and Consumer Regulations 2010* made under the legislation (CC Regulations). Regulation 28RA deals with the application of privacy safeguards in the energy sector
- 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. For more information about the Standards, see section 2.3 below.

## 1.3. The CDR agencies

The Australian Competition and Consumer Commission (ACCC) and the Office of the Australian Information Commissioner (OAIC) are jointly responsible for monitoring compliance with CDR. The ACCC promotes competition and the OAIC protects privacy and confidentiality. As part of our joint role, we monitor compliance with the CDR regulatory framework, respond to issues and pursue enforcement activity if necessary.

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

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

## 1.4. Compliance and Enforcement Policy

The ACCC and OAIC Compliance and Enforcement Policy explains to data holders and accredited data recipients (CDR participants) the approach that the regulators will take to encourage compliance and prevent breaches of the CDR regulatory framework.

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

## 1.5. CDR in the energy sector

CDR in the energy sector applies to specified data sets in the National Electricity Market (NEM). This includes consumer data sets relating to the sale or supply of electricity, including where electricity is bundled with gas.[1] Product data sets for CDR in the energy sector include electricity, gas and dual fuel plans.

## 1.6. This guide

This guide has been produced by the ACCC. It is intended to help energy retailer data holders understand their obligations under:

- the CDR Rules, which provide the framework for how CDR operates
- the Standards, which specify requirements and provisions for consumer-facing content and interactions, such as data language, authentication and accessibility.

The guide focuses on:

- energy retailers' data holder obligations once registration and onboarding have been completed
- energy retailers' data holder obligations when sharing data with an accredited data recipient.

It provides information on the key obligations set out in section 1.4, as well as links to further guidance on relevant topics.

Data holders may need to meet other requirements that are not covered in this guide. See section 1.7.

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. It is not a comprehensive or exhaustive statement of all the obligations data holders need to comply with under CDR or of all the potential consequences of non-compliance. Please see the **Important notice** at the start of this guide.

---

[1] Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2021, Explanatory statement, page 1, paragraph 3.

## 1.7. Data holders' roles and obligations

### 1.7.1. Roles

Energy retailer data holders have 3 main roles under CDR:

- They provide the necessary CDR infrastructure for dealing with requests to share consumer data.
- With a consumer's authorisation and when they receive a valid request, they securely **transfer** the consumer's data in a machine-readable format.
- They manage a consumer's authorisation to disclose CDR data, and any amendment or withdrawal of that authorisation.

### 1.7.2. Obligations

Under CDR, subject to varying commencement dates, energy retailer data holders have obligations that include:

- disclosing consumer data
- establishing dispute resolution arrangements
- keeping appropriate records
- reporting at scheduled intervals
- complying with the relevant privacy safeguards.[2]

## 1.8. Commencement of obligations

The date on which a data holder's CDR obligations commence will depend on which type of data holder they are. See section 4.3 for more information about different types of energy retailer data holders.

Data holders will have different obligations at different times, depending on the complexity of the request[3] (see section 4.4).

For a summary of commencement dates for different energy retailer data holders, see Table 5.

### 1.8.1. Exemptions from compliance with obligations

CDR participants can seek an exemption from compliance with their obligations under CDR.[4] The ACCC assesses each application for exemption on a case-by-case basis, having regard to the facts and circumstances relevant to the particular entity and the exemption being sought.

---

2 These requirements are set out in the CCA, the Competition and Consumer Regulations 2010 (CC Regulations), the Competition and Consumer (Consumer Data Right) Rules 2020 (CDR Rules) and the Consumer Data Right Standards (Standards).

3 CDR Rules, Part 8, Schedule 4.

4 CCA, section 56GD.

For more information about how to apply for an exemption and when an exemption might be appropriate, see the Guidance for applicants seeking exemption under section 56GD. The Consumer Data Right Exemption Register lists all exemptions the ACCC has granted.

### 1.8.2. Additional requirements for compliance with privacy safeguards

Data holders must also comply with the CDR Privacy Safeguards.

The OAIC regulates the privacy aspects of the CDR scheme. For information on how to comply with privacy and confidentiality aspects of the CDR scheme, data holders should also read the OAIC's Guide to privacy for data holders and CDR privacy safeguard guidelines. These guidelines will help entities to avoid acts or practices that may breach applicable privacy safeguards and Australian Privacy Principles (APPs).[5]

### 1.8.3. Additional requirements for accredited data recipients

Some data holders may be accredited data recipients as well as data holders. Accredited data recipients must meet additional obligations that are not covered in this guide.

# 2. Consumer Data Standards

The Standards set out the technical requirements for sharing data under CDR.[6] Under the CDR Rules, data holders must comply with the Standards.

## 2.1. The Standards

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.[7]

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 Change Log 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 2 for an overview of the Standards.

---

5 Set out in the *Competition and Consumer Act 2010* (CCA), Division 5, Part IVD. Further details are set out in the CDR Rules.

6 CDR Rules, rule 8.11.

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

### 2.1.1. References to the Standards in this guide

This guide uses a referencing system to point out aspects of the Standards that are relevant to the compliance obligations being described (see Table 1).

These references are noted as general guidance only. The references are general and high-level – for example, they may reference the section heading that appears in the Standards – because it is likely that the more detailed content of the Standards will change.

This guide does not contain 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 to meet the relevant obligation.

**Table 1**

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

### 2.1.2. Overview of the Standards

**Table 2: Consumer Data Standards - overview**

| | |
|---|---|
| *Security requirements* | |
| **Security profile** | Sets out the security specifications that data holders must implement to facilitate data sharing with accredited data recipients. These specifications must be implemented by a data holder. |
| *Receiving and responding to CDR data requests* | |
| **Standards** | Contains high-level standards that govern the Standards as a whole. These high-level standards apply to all CDR participants. |
| **Industry Specific Application Programming Interfaces (APIs)**[8] | Set 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 |

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

| | |
|---|---|
| | are categorised according to the industry that they are applicable to. For instance, Common APIs' are applicable to multiple sectors while 'Energy APIs' and the 'Shared Responsibility' section of the Standards are applicable to the energy sector. |
| **Authorisation scopes** | Set out the level of authority the accredited data recipient has in accessing the consumer's data. The Energy APIs specify which authorisation scope is applicable to each type of data request. |
| CDR consumer-facing interactions | |
| **CX Standards** | Set out what data holders must do in their direct interactions with consumers, including what a data holder must do when seeking a consumer's authorisation and how it must communicate when a consumer wishes to withdraw an authorisation. |
| Reporting | |
| **Admin APIs** | Allows the ACCC to obtain operational statistics from data holders on the operation of their CDR compliant implementation. These standards also set out how a data holder must respond to such requests from the ACCC. |
| Service and performance levels | |
| **Non-functional requirements (NFRs)** | Set out a range of performance and service level requirements data holders are expected to meet in delivering their CDR solution - for example, minimum CDR platform availability and performance levels. |

## 2.2. Understanding data holders' obligations under 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 an accredited data recipient. The legal effect of binding Standards is set out in sections 56FD and 56FE of the CCA.

For information about when the data holder's obligations commence, see section 4.4.

### 2.2.1. 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 says:

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

RFC 2119 gives guidance on how uppercase terms (MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY and OPTIONAL) should be interpreted.

For example, if a Standard states that a data holder 'SHOULD' do something, the data holder should use RFC 2119 to interpret this as follows:

- RFC 2119 states that 'SHOULD' and '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 policy, where binding Standards state that 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.

### 2.2.2. Mandatory, optional and conditional fields

The Standards contain instructions for individual data fields in API payload schemas. These 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. Where they do not have the data, it must be represented as a default or empty value as applicable.[9]
- 'Optional' fields MAY be present, but this is not guaranteed. It is also valid for these fields to be present but to have a null value. Optional fields indicate that certain 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. That is, if a field is described as 'optional', it does not mean that the data holder has an option regarding whether to provide the information. 'Optional' in this context means:
  - 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, 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 in a specific request or response is true, the field is considered mandatory.
  - If the statement in a specific request or response is false, the field is considered optional.

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

### 2.2.3. 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.

## 2.3. Consumer Experience (CX) Guidelines

Data holders must be familiar with the current version of the Consumer Experience Guidelines (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 the Standards. However, a data holder's processes for asking a CDR consumer to give an authorisation must, having regard to the CX Guidelines, be as easy to understand as practicable, including by use of concise language and, where appropriate, visual aids.[10]

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

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

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

## 2.4. Further information

Other resources on the Standards and CX Guidelines are listed in Table 3.

**Table 3: Standards and CX Guidelines resources**

| Resource | Description |
|---|---|
| **CDR Support Portal** | The CDR Support Portal publishes guides on technical and compliance-related matters. Participants can also raise questions on the Support Portal which will be reviewed and responded to by the appropriate CDR agency. |
| **Conventions** | The DSB supplements the Standards with conventions, which document broadly accepted interpretations of the Standards but do not impose compliance obligations.<br>Conventions are published on the CDR Support Portal.<br>CDR community members can request a convention by raising an issue in the CDR Github standards maintenance repository. For more information about the development of conventions, see the relevant convention articles. |

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

| | |
|---|---|
| CX Checklist | The CX Checklist is a complete list of items referenced in the CX Guidelines, including relevant rules, privacy safeguards and data standards (CX and technical). This list has been created to assist CDR participants with implementation and compliance. However, they 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 in this location. Standards maintenance is also conducted and change proposals are publicly consulted on. |

# 3. Product data

Under the CDR Rules a person may use a data holder's **product data request service** to request disclosure of product data.

## 3.1. Product data requests

*CDR Rules: see rule 1.12 and Schedule 4, clauses 4.2 and 8.4.*

Energy retailers are holders of product data. As the NERL and the Victorian Act require energy retailers to provide this product data to the Australian Energy Regulator (AER) or the Victorian agency[11], those agencies are **designated data holders** for product data in the energy sector and must provide a product data request service.

Data holders (apart from the AER or the Victorian agency) are not required to provide a product data request service. However, they may choose to provide that service. If a data holder chooses to provide an online service that can be used to make these requests, it must comply with rule 1.12 of the CDR Rules.

Energy retailers interested in voluntarily sharing product data should email the ACCC's CDR team: ACCC-CDR@accc.gov.au.

## 3.2. Required product data and voluntary product data

*CDR Rules: see Schedule 4, clause 3.1.*

Product data can be divided into 2 types: **required product data** and **voluntary product** data. 'Required product data' and 'voluntary product data' refer to data to be disclosed when a valid request is received. See Table 4 for an explanation of the types of data included in each category.

These terms should not be confused with the labels given to the data fields, 'mandatory' and 'optional', in the Standards. Those fields are to do with the parameters for the APIs used to request and disclose CDR data (see section 2.2).

[11] Clause 1.2 of Schedule 4 to the CDR Rules defines the Victorian agency as the Department of State administered by the Minister of Victoria administering the *National Electricity (Victoria) Act 2005* (Vic). As at the date of publication, the current Victorian agency is the Victorian Department of Energy, Environment and Climate Action \.

**Table 4: Required product data and voluntary product data**

| Required product data | Voluntary product data |
|---|---|
| CDR data that:<br>• does not relate to a particular CDR consumer(s)<br>• falls within the class of information specified in section 9 or section 10 of the Energy Sector Designation<br>• is about certain characteristics of the product (such as the product's eligibility criteria, price, terms and conditions, availability or performance)<br>• is product specific data<br>• is held by the AER or the Victorian agency for the purpose of operating websites that provide such information to the public. | CDR data that:<br>• does not relate to a particular CDR consumer(s)<br>• is energy sector data; and<br>• is product specific data in relation to a plan offered by or on behalf of the data holder; and<br>• is not required product data. |

## 3.3. Use of disclosed data

*CDR Rules: see rule 2.6.*

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

## 3.4. Commencement of product data obligations

*CDR Rules: see Schedule 4, clauses 8.4 and 4.1.*

The AER has been required to comply with Part 2 of the CDR Rules (dealing with product data requests) since **1 October 2022**. The Victorian agency has also been required to participate as a data holder for product data since 15 November 2022.[12]

Under the CDR Rules, the AER and the Victorian agency can act on behalf of each other, at the other's request, for a product data request.

[12] See CDR rules, Schedule 4, clause 8.4(3) and Competition and Consumer (Consumer Data Right—Participating Victorian Government entity) Declaration 2022, Part 2, section 6.

# 4. Consumer data

## 4.1. CDR consumers

### 4.1.1. Eligible CDR consumers

*CDR Rules: see rule 1.10B and Schedule 4, clause 2.1.*

Under the CDR Rules, data holders must enable sharing of required consumer data for **eligible CDR consumers**. An 'eligible CDR consumer' is one who:

- fits within the definition of a 'customer' in the Energy Sector Designation
- is eligible under the CDR Rules (see below).[13]

Under the Energy Sector Designation, a customer is a person who purchases electricity or to whom electricity is supplied by an energy retailer.[14] An individual is not a customer if they supply electricity to the grid but do not purchase or receive electricity from the energy retailer. For example, an individual is not considered a customer if they only generate electricity using their solar panels and supply it to the grid.

Under the CDR Rules, a consumer is eligible in the energy sector if:

- they are an account holder or secondary user for an open account with the data holder
- 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
- they are a customer of the energy retailer and their account relates to an arrangement where the energy retailer sells or supplies electricity to them
- the energy consumed in association with their account is[15]:
  - less than 5GWh over the previous 12 months, or
  - for an account that has existed for less than 12 months, the estimated annual consumption is less than 5GWh
- their account relates to an arrangement that has at least one connection point or child connection point[16] for which there is a financially responsible market participant[17] in the NEM. That is, the consumer must be 'on market' in the NEM, rather than being sold electricity by a person that holds an exemption from the Australian Energy Regulator.

---

13 CDR Rules, rule 1.10B and Schedule 4, clause 2.1.

14 Consumer Data Right (Energy Sector) Designation 2020, section 5.

15 See section 4.1.2 for more information.

16 Child connection points occur where there are multiple end user connection points between the distribution network and end users, each with their own meters (e.g. this may be the case in apartment blocks).

17 The financially responsible market participant is the entity registered with AEMO that is responsible for making or receiving payments in relation to electricity transferred across a connection point (e.g. an energy retailer).

### 4.1.2. Energy arrangements and accounts

As explained in section 4.1.1, a consumer's actual or estimated energy consumption must be below the 5GWh consumption threshold for the consumer to be considered eligible for data sharing in the CDR.[18] This threshold applies to the energy account rather than the premises or specific connection point(s) for the premises. For example, the aggregated consumption for multiple locations under a single account must be less than 5GWh over the previous 12 months. Where an account has existed for less than 12 months, the estimated annual consumption of multiple locations under a single account must be less than 5GWh.

If a CDR consumer has one or more accounts with an energy retailer and the energy consumed is more than 5GWh per annum per account, it will be excluded from the CDR. However, if a consumer has multiple accounts with the same retailer and at least one of those accounts has less than 5GWh consumption, the energy retailer will be required to make all accounts available for data sharing.

Please refer to our guidance on Eligibility criteria for CDR consumers in the energy sector for more information.

## 4.2. Data holders

*CDR Rules: see rule 1.22 and Schedule 4, clauses 4.3 and 4.4.*

### 4.2.1. Primary and secondary data holders

Under the CDR, a **primary data holder** in the energy sector is an energy retailer with whom the consumer has a direct relationship. The primary data holder holds data sets including:

- customer data
- account data
- billing data
- tailored tariff data.[19]

The Australian Energy Market Operator (AEMO) is a **secondary data holder**. AEMO has no direct relationship with the consumer, but it holds important consumer data that is not held by the consumer's energy retailer. Specifically, AEMO holds:

- metering data
- National Metering Identifier (NMI) standing data
- Distributed Energy Resources (DER) Register data.[20]

The CDR Rules define this as 'AEMO data' or 'shared responsibility (SR) data'.[21]

An eligible CDR consumer or accredited person must make all consumer data requests to the primary data holder.

---

18 CDR Rules, Schedule 4, clause 2.1(1).

19 These data sets are defined in detail in Schedule 4 to the CDR Rules.

20 These data sets are defined in detail in Schedule 4 to the CDR Rules.

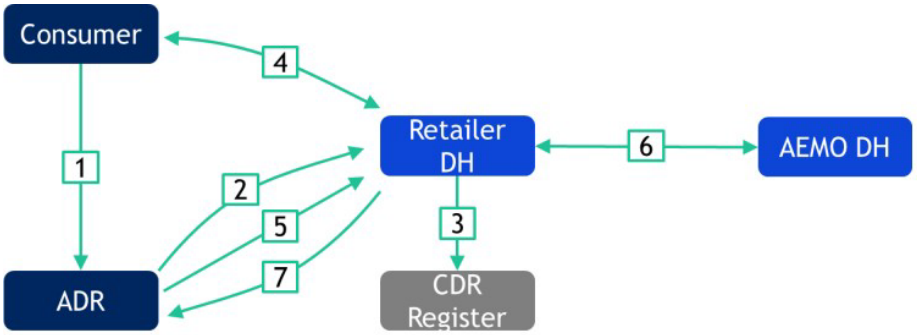
21 See the Shared responsibility section of the Standards for more information on shared responsibility data requests.

A consumer data request may cover data that is collected and held by the secondary data holder (AEMO) instead of the primary data holder. Primary data holders are responsible for requesting the relevant data from AEMO and responding to the consumer data request. AEMO cannot directly respond to requests from CDR consumers or any CDR participants other than primary data holders.

If AEMO does not disclose the data that the primary data holder has requested, it must notify the primary data holder of its refusal. The primary data holder is then relieved of its obligation to disclose the requested AEMO data to the consumer.

A peer-to-peer (P2P) model has been established to allocate the responsibilities of energy retailers and AEMO when responding to consumer data requests – see Figure 1.

**Figure 1: P2P model for responding to data requests in the energy sector**[22]




1. The consumer consents to an accredited data recipient (**ADR**) obtaining their data.
2. The ADR contacts the retailer Data Holder (**DH**), seeking access to the consumer's data.
3. The retailer DH authenticates the ADR using the CDR Register.
4. The consumer is redirected to the retailer DH's authentication and authorisation service. The retailer DH authenticates the identity of the consumer via a one-time password. The Consumer authorises the retailer DH to disclose their data to the ADR.
5. The ADR requests a specific set of data that is covered by the authorisation.
6. The retailer requests the relevant data, covered by the authorised consent, from AEMO as a data holder (**AEMO DH**). AEMO DH provides the requested data to the retailer DH. The retailer may also obtain relevant data from its own data holdings.
7. The consumer's data is shared between the retailer DH and the ADR.

## 4.3. Retailers

A **retailer** is a data holder of energy sector data that retails electricity to connection points in the NEM.[23] Only authorised or licensed retailers that operate through the NEM must meet data holder obligations.

[22] Treasury, *Peer-to-peer data access model in the energy sector – CDR rules and standard design paper*, April 2021, p 4.

[23] The NEM currently covers Queensland, New South Wales, Australian Capital Territory, Victoria, Tasmania and South Australia. Western Australia and the Northern Territory are not connected to the NEM.

### 4.3.1. Initial retailers

The following entities are **initial retailers**:

- The AGL Energy Group
  - AGL Sales (Queensland Electricity) Pty Limited
  - AGL South Australia Pty Ltd
  - AGL Sales Pty Limited
- The Origin Energy Group
  - Origin Energy Electricity Limited
  - any other subsidiary of Origin Energy Limited authorised or licensed to sell electricity in the NEM
- The Energy Australia Group
  - EnergyAustralia Pty Ltd.

Initial retailers must share consumer data earlier than other retailers.

### 4.3.2. Larger retailers

**Larger retailers** are retailers that:

- had 10,000 small customers or more on 16 November 2021, or
- have 10,000 small customers or more at all times during a financial year beginning after 16 November 2021.[24]

A **small customer** is a domestic or small business customer of the retailer.[25]

Once a retailer becomes a larger retailer, it continues to be one even if the number of small customers it has drops below 10,000.

### 4.3.3. Small retailers

**Small retailers** are retailers that have under 10,000 small customers. They will not have data holder obligations unless they become accredited as an accredited data recipient or wish to participate voluntarily as data holders.

If a small energy retailer is interested in participating in the CDR scheme voluntarily[26] as a data holder or accredited data recipient, it may notify the ACCC that it wishes to participate voluntarily. The energy retailer should email the ACCC's CDR team: ACCC-CDR@accc.gov.au and notify when it would like to participate on and from a specified date. Once a small retailer elects to participate voluntarily in the CDR, there is no mechanism for it to opt-out of participation.[27]

---

[24] The definition comes from the CDR Rules, Schedule 4, clause 8.3.

[25] A 'small customer' is defined in clause 8.3(2) of Schedule 4 to the CDR Rules.

[26] In this context, voluntarily refers to those energy retailers that are not already required to share data under the CDR Rules.

[27] Competition and Consumer Amendment (Consumer Data Right) Amendment Rules (No. 2) 2021, Explanatory statement, p 12.

### 4.3.4. Complex requests

If a consumer data request is made on behalf of a large customer (for example, commercial and industrial customers (C&I customers)) or secondary user, or it relates to a joint or partnership account, it will be considered a **complex request**.

A **large customer** of an energy retailer is a CDR consumer that is:

- in relation to a retailer that is subject to the Victorian Act - a customer that is not a 'relevant customer' for the purposes of the Victorian Act[28]; or
- otherwise - 'a large customer' for the purposes of the NERL.

### 4.3.5. Reciprocal data holders

An accredited person may be considered a data holder of CDR data that was not disclosed to it under the CDR Rules. This means that they may be required to share particular CDR data at particular times in accordance with the obligations of a data holder under the CDR Rules, separate from their obligations as an accredited person. Accredited persons that become data holders in this way are sometimes called **reciprocal data holders**.[29]

In the energy sector, a person who becomes an accredited person is unlikely to meet the requirements for reciprocal data holder obligations unless they are already an energy retailer (and therefore already a data holder). A non-retailer that generates and holds energy sector CDR data would likely be in breach of the national energy legislation. This makes it very unlikely that a non-retailer would generate and hold CDR data and therefore be considered a reciprocal data holder.

If an accredited data recipient that is not an energy retailer does become a reciprocal data holder in this way, the CDR Rules do not apply consumer data sharing obligations for energy sector data.[30]

## 4.4. Commencement of consumer data obligations

*CDR Rules: see Schedule 4, Part 8.*

If a consumer requests and authorises a data holder to share specified 'required consumer data' with an accredited data recipient, the data holder must do so.

Data sharing obligations in the energy sector will commence in 4 tranches. Table 5 sets out the commencement dates.

There are different commencement dates depending on the type of retailer (for example, whether the retailer is an initial or larger retailer – see section 4.3- and whether the request is complex or non-complex – see section 4.3.3).

Data holders will have different CDR obligations depending on the consumer data they receive and the complexity of the relevant account.

Initial retailers commenced their consumer data sharing obligations for non-complex and complex requests in Tranche 1 (15 November 2022) and Tranche 2 (15 May 2023)

---

28 See section 40SB of the *Electricity Industry Act* 2000 (Vic) for the meaning of 'relevant customer'.

29 CCA, section 56AJ(3).

30 See CDR Rules, Schedule 4, clause 3.2(5).

respectively. Larger retailers have been subject to consumer data sharing obligations for non-complex requests since Tranche 3 (1 November 2023) and will be required to share consumer data for complex requests in Tranche 4 (1 May 2024).

**Table 5 Commencement dates for data sharing in the energy sector**

| Tranche | CDR data type | Data holder | Commencement date |
|---|---|---|---|
| - | Consumer data obligations | AEMO | 15 November 2022 |
| **Tranche 1** | Consumer data obligations - non-complex request | Initial energy retailers | 15 November 2022 |
| **Tranche 2** | Consumer data obligations - complex requests | Initial energy retailers | 15 May 2023 |
| **Tranche 3** | Consumer data obligations - non-complex request | Larger energy retailers | 1 November 2023 |
| **Tranche 4** | Consumer data obligations - complex requests | Larger energy retailers | 1 May 2024 |
| - | Consumer data obligations - non-complex request | Small energy retailers that become accredited | 12 months after the day it becomes accredited |
| - | Consumer data obligations - complex requests | Small energy retailers that become accredited | 18 months after the day it becomes accredited |
| - | Consumer data obligations - non-complex request | Small energy retailers that wish to participate voluntarily | Date of its choosing but no earlier than 15 Nov 2022 |
| - | Consumer data obligations - complex requests | Small energy retailers that wish to participate voluntarily | Date of its choosing but no earlier than 15 May 2023 |

## 4.5. Registration on the CDR Participant Portal

A data holder must 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 through the CDR Participant Portal. The registration and on-boarding process is outlined in the Data holder user journey.

The CDR Participant Portal User guide gives further information about the portal and the registration process. Please read this guide together with the CDR participant On-boarding guide.

# 5. Consumer data requests

## 5.1. Consumer data requests

Consumer data requests are made by an accredited person to a primary data holder. The requests are made using the data holder's consumer data request service.

### 5.1.1. Required consumer data and voluntary consumer data

*CDR Rules: see rules 4.6, 4.6A and 4.7, and Schedule 4, clause 3.2.*

Accredited persons can request the CDR consumer's required consumer data, voluntary consumer data, or both from the data holder. The data holder **must** disclose any requested required consumer data to the accredited person who made the request (subject to rule 4.6A and rule 4.7 – see section 6.4 of this guide).

The data holder **may** (but is not required to) disclose the voluntary consumer data that it is authorised to disclose.

**Table 6 Required and voluntary consumer data**

| Required consumer data | Voluntary consumer data |
|---|---|
| CDR data that:<br>• is energy sector data<br>• relates to one or more CDR consumers<br>• relates to a time at which an account holder was associated with the premises to which the request relates<br>• relates to a transaction or event that occurred less than 2 years before the date of the request and<br>• is held in a digital form<br>and, in relation to a relevant open account, is either:<br>• customer data<br>• AEMO data<br>• account data<br>• tailored tariff data<br>• billing data.<br>and, in relation to a relevant closed account, is either[31]:<br>• metering data held by AEMO<br>• billing data held by a retailer. | CDR data that:<br>• is energy sector data<br>• relates to one or more CDR consumers<br>• relates to a time at which an account holder for the relevant account was associated with the premises to which the request relates<br>• is not required consumer data. |

Consumer data is not required or voluntary CDR consumer data if it:

- is held by a data holder that is not an energy retailer or AEMO (for example, an accredited person who becomes a reciprocal data holder[32] - see section 4.3.5 of this guide)
- is account data, billing data, tailored tariff data or AEMO data in relation to either:

[31] See Guidance for energy closed accounts for more information.

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

- an account that is not held in the name of a single person, a joint account or partnership account
- an account for which any of the account holders are less than 18 years of age at the time of the consumer data request

- relates to a consumer data request made on behalf of a particular person and the data is either:
  - customer data in relation to any account holder or secondary user other than that person
  - AEMO data in relation to premises that are not covered by the relevant arrangement at the time to which the data relates.

### 5.1.2. Requests for consumer data from white label products

**White label products** are products that are created and operated by one entity (a white labeller) and branded and retailed to consumers by another entity (a brand owner).

Where a single data holder (either the white labeller or the brand owner) is providing a white label product in partnership with a non-data holder, that single data holder must comply with consumer data sharing obligations for the product.

Where there are 2 data holders involved in providing a white label product (for example, where an energy retailer offers an eligible arrangement on behalf of another energy retailer), the data holder that has the contractual relationship with the consumer will be responsible for responding to consumer data requests.

The white labeller that has the contractual relationship with the consumer and the brand owner may agree that the brand owner will respond to consumer data requests. In this instance, the white labeller, as the data holder that has the contractual relationship with the consumer, remains accountable for the brand owner meeting this obligation.

White labeller data holders must register their white label brands on the CDR Register. If 2 data holders are involved in providing a white label product and they have agreed that the brand owner will respond to data requests, the brand owner will register the brand.

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

See the following resources for further guidance on white label products:

- Disclosure of product & consumer data for white label products
- Brands in the Consumer Data Right ecosystem
- ADI responsibility for data holder brands
- White labelled brands in the CDR
- Noting Paper 169 – White label conventions.

The above guidance is currently tailored to the banking sector. We welcome feedback on its applicability to the energy sector.

## 5.2. Consumer data request service

*CDR Rules: see rules 1.13 and 1.20.*

Primary data holders must provide an online service known as an 'accredited person request service' that:

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

AEMO must provide an online service that:

- primary data holders can use to request data from AEMO to respond to a consumer data request
- discloses data in machine-readable form
- conforms with the Standards.

**Table 7 Standards for online services**

| Standards/ Guidelines | Section | Sub-section |
|---|---|---|
| Standards | Industry Specific APIs | All API definitions except those that are related to the product data request service |
| Standards | High Level Standards | Versioning; URI Structure; HTTP Headers; HTTP Response Codes; Payload Conventions; Common Field Types; Pagination; ID Permanence; Extensibility |
| Standards | Shared Responsibility | The entire shared responsibility is applicable |
| Standards | Security Profile | The entire security profile is applicable |
| Standards | Non-functional Requirements | The majority of the NFRs impact the consumer data request service |
| Standards | DCR APIs | All API definitions are applicable |
| Standards | Admin APIs | All API definitions are applicable |

## 5.3. CDR consumer dashboard

*CDR Rules: see rules 1.15 and 1.21, and Schedule 4, clause 2.3.*

A CDR consumer dashboard is an online service that enables a consumer to manage their data sharing arrangements.

A primary data holder must provide a consumer dashboard if it receives a consumer data request from an accredited person on behalf of a CDR consumer who has online access to the relevant account. This applies to consumer data requests the energy retailer receives

for both retailer-held and AEMO-held data as if the energy retailer were the data holder for all the requested data.

### 5.3.1. Offline customers

An eligible CDR consumer in the energy sector may have online access to their energy account. However, this is not a prerequisite for eligibility – see section 4.1.1.

Consumers without online access to their energy account – also known as 'offline customers' – are also eligible to share data. So, while all eligible CDR consumers, including offline customers, will primarily engage with CDR online, they do not need to have online access to their energy account to do this.

Data holders must take reasonable steps to support data sharing for customers who do not have online access to their energy account. As part of this process, data holders must not impose additional eligibility requirements – for example, requiring a customer to register for online access to their account – before they can share data.

If the CDR consumer does not have a consumer dashboard because they do not have online access to the relevant account, the energy retailer data holder must offer the consumer a dashboard. Dashboards are expected to be offered to offline customers externally once they have completed authorisation. The CX Guidelines recommend that data holders provide CDR receipts to consumers. A data holder could use those to offer a dashboard to offline customers.

If the consumer accepts the offer, the data holder must provide them with a consumer dashboard.

The data holder can decide whether to make a dashboard accessible via an online account or another mechanism – for example, by issuing a one-time password to be used on a website set up by the data holder. The data holder should also provide instructions on how the consumer can continue to access the dashboard.

If the consumer declines the offer for a consumer dashboard, the data holder should explain the consequences of this and any alternatives available — for example, consumers should understand how they will receive relevant notifications.[33]

**Table 8 Guidelines for offline customers**

| Standards/ Guidelines | Section | Sub-section |
|---|---|---|
| CX Guidelines | Consent Management (Data holder) | Authorisations: Offline customers |
| CX Guidelines | Authenticate | Redirect with one time password |

[33] CDR Rules, rule 4.25(1)(b)).

### 5.3.2. Consumer dashboard requirements

The consumer dashboard must allow the CDR consumer to manage authorisations to disclose their CDR data to an accredited person.

The consumer dashboard must also:

- include functionality that allows a consumer to withdraw authorisations to disclose CDR data at any time. This feature must be simple and straightforward to use, prominently displayed and no more complicated than the process for authorising the disclosure of CDR data. A message must be displayed as part of the withdrawal process explaining the consequences of withdrawal in accordance with the Standards
- contain the following details of the CDR data that has been authorised to be disclosed:
  - 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 expired or is scheduled to expire
  - details of any amendments that have been made to the authorisation[34]
  - what data was disclosed
  - when it was disclosed
  - the accredited data recipient it was disclosed to[35]
- if the disclosure is of corrected data in response to a request under Privacy Safeguard 11 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.[36]

### 5.3.3. Non-individuals and partnerships

Data holders must only allow nominated representatives to use the CDR consumer dashboard to manage authorisations on behalf of a non-individual or partners in a partnership. See Nominated representatives of non-individuals and partnerships in the CDR for further information.

### 5.3.4. Joint accounts

*CDR Rules: see rule 4A.13.*

For joint accounts (see section 5.4), data holders must provide all relevant account holders with a consumer dashboard for managing approvals to disclose CDR data. This dashboard must:

- meet the requirements for individual account dashboards outlined above

---

[34] 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 Data 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.

[35] See CDR Rules, rule 7.9; see also Privacy Safeguard 10; CCA, section 56EM.

[36] See CDR Rules, rule 4.27.

- enable all joint account holders to see the same details of each approval as the requesting account holder.

**Table 9 Standards and CX Guidelines for joint accounts**

| Standards/ Guidelines | Section | Sub-section |
|---|---|---|
| CX Standards | Withdrawal standards<br>Authorisation standards<br>Notification standards | Withdrawing authorisation: Consequences; Withdrawing authorisation: Redundant Data; Withdrawal: Joint accounts<br>All Sub-sections<br>All Sub-sections |
| CX Guidelines | Authorise<br>Consent Management (Data holder) | Authorisation to disclose; Authorisation to disclose joint account data<br>Authorisations; Withdrawal (Default and Withdrawing approvals) ; Account permissions (Joint account disclosure option management service); Joint account notification settings |
| 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 |

## 5.4. Joint accounts

Consumer data requests related to joint accounts are considered complex requests in the energy sector.[37] Special rules apply to joint accounts. To be able to share joint account data, all joint account holders must be 'eligible' consumers in their own right (see section 4.1.1 of this guide for the definition of an eligible CDR consumer).

Energy accounts with more than one CDR consumer (each of which is an individual) may not always meet the CDR definition of a joint account. In these circumstances data holders should consider whether the secondary user rules may apply. Secondary users are not joint account holders and separate rules apply, see section 5.5 for further information.

### 5.4.1. Disclosure options for joint accounts

*CDR Rules: see rule 4A.5.*

The CDR Rules provide 3 disclosure options that can apply to joint accounts:

- pre-approval option - joint account data can be disclosed when a valid consumer data request is received from any account holder of the account without approval from other joint account holders. This option applies by default

[37] Clause 8.1 of Schedule 4, CDR rules.

- co-approval option - a more restrictive sharing preference. It means that all joint account holders must approve the request before the joint account data can be disclosed
- non-disclosure option - the most restrictive option. It means that joint account data cannot be disclosed.

Data holders must offer joint account holders the pre-approval option and the non-disclosure option. They can choose whether to offer the co-approval option.

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
- all joint account holders have agreed to the 'co-approval' option and have approved the disclosure of this data.

### 5.4.2. Changing disclosure options

The pre-approval option applies to the joint account by default. However, any joint account holder can make a change to a more restrictive disclosure option.

Once a more restrictive disclosure option has been applied to the account, all joint account holders must agree before a less restrictive disclosure option can be applied to a joint account. These changes are made using the **disclosure option management service** (see section 5.4.3).

### 5.4.3. Disclosure option management service

*CDR Rules: see rule 4A.6.*

A disclosure option management service enables an account holder to:

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

Data holders must provide each joint account holder with an online disclosure option management service.

The disclosure option management service must be provided online and may be included in the data holder's consumer dashboard. An offline method can be provided in addition to (not instead of) the online service.

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
- the withdrawal of a disclosure option.

The service must indicate to the joint account holder which disclosure option currently applies and must implement 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.

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

#### *Changing to a more restrictive disclosure option*

*CDR Rules: see rule 4A.7.*

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

- explain to each of them what CDR is
- inform them which disclosure option previously applied to the account
- inform them that an account holder has changed the disclosure option, and which disclosure option 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 wishes 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 CDR is
- inform them 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 (whichever one applies)
- 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.[38] At the end of the specified period, the data holder must inform them that either:

[38] Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021, Explanatory statement, p 27, paragraph 3.

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

### 5.4.5. Joint account obligations and preventing physical, psychological or financial harm or abuse

*CDR Rules: see rule 4A.15.*

A data holder will not be liable for failure to comply with their joint account holder obligations under Part 4A of the CDR Rules if it considered that the relevant act or omission was 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 the CDR Rules, rule 4A.8)
- 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 the CDR Rules, rule 4A.10(4))
- 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 the CDR Rules, rule 4A.13).

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

## 5.5. Secondary users

*CDR Rules: see rule 1.7*

Consumer data requests made on behalf of secondary users are considered complex requests in the energy sector.[39] The commencement of data sharing for complex requests will arise in corresponding phases as outlined in section 4.4.

An individual is a 'secondary user' for an account if:

- the person is at least 18 years of age
- the person has account privileges, and
- the account holder(s) is an individual(s) who is also at least 18 years of age and has given the data holder an instruction to treat the person as a secondary user for the purposes of the CDR rules (known as a 'secondary user instruction').[40]

[39] Clause 8.1 of Schedule 4, CDR rules.

[40] CDR Rules, rule 1.7.

### 5.5.1. Account privileges in the energy sector

*CDR Rules: see Schedule 4, clause 2.2.*

A person has account privileges in the energy sector if they are a customer authorised representative of the account holder for the purposes of rule 56A of the National Energy Retail Rules (NERR) or Chapter 7 of the National Electricity Rules (NER).[41] This means that a person has account privileges if the CDR consumer has authorised them to receive their metering data and, for small customers, their billing data.

Once a person meets the criteria to become a secondary user, and the account holder has provided a valid secondary user instruction, they are able to share data as a secondary user in accordance with the CDR rules. This is independent of any rights or obligations a customer authorised representative may have under the NERR or the NER.

For more information on secondary users, see the Secondary users in energy guidance.

# 6. Disclosing consumer data

## 6.1. Requesting consumer authorisation to disclose CDR data

When an energy retailer 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 (see section 6.4).

*CDR Rules: see rule 4.23.*

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

- the name of the accredited data recipient that made the request[42]
- 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.[43]
- that the consumer can withdraw their authorisation at any time, and how to do so
- specified information that the Register of Accredited Persons holds in relation to the accredited person.

The data holder does not need to seek authorisation if they already have a current authorisation from the consumer to disclose the requested data to the accredited data recipient.[44]

---

41 Clause 2.2 of Schedule 4, CDR rules.

42 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.

43 While certain consents given by a 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.

44 CDR Rules, rule 4.5(1)(b); See CX Guidelines on Authorisation to disclose.

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 which is subject to a new consent, the data holder will need to ask the consumer for new authorisation for any elements of the request that are not covered by the existing authorisation. In practice, this may mean the data holder will need to ask the consumer for a new authorisation for all of the requested data under the new consent.

The data holder's process for asking a consumer to give or amend an authorisation must comply with the Standards.[45] The request for authorisation must be in accordance with the Standards on voluntary consumer data[46] and on required consumer data[47] (subject to rule 4.7 of the CDR Rules – see section 6.4).

The process for seeking authorisation should be easy for consumers to understand.[48]

### Table 10 Standards and CX Guidelines for data sharing authorisation

| Standards/ Guidelines | Section | Sub-section |
|---|---|---|
| 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 | Authentication Standards | All Sub-sections |
| | Authorisation Standards | All Sub-sections |
| CX Guidelines | Authenticate; | Redirect with One Time Password |
| | Authorise | Authorise to disclose |

*CDR Rules: see rule 4.24.*

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

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

[45] CDR Rules, rule 4.22(a).
[46] CDR Rules, rule 4.5(2)(b).
[47] CDR Rules, rule 4.5(3)(b).
[48] CDR Rules, rule 4.22(b).

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 accredited data recipient than it was with the data holder.

### 6.1.1. 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 for 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 joint account holder has withdrawn their approval, the data holder must not disclose any (or any further) requested CDR data (see section 6.2).[49]
2. If the co-approval option applies, the data holder must seek the requester's authorisation and the other joint 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 set out above (section 6.1.1) 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 for their account at 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 the joint account data will not be disclosed unless an approval is received by that time
    - inform them that any of the account holders can withdraw their approval at any time; and provide instructions on how to do so and an explanation of the impact this would have.
3. If the non-disclosure option applies, the data holder must refuse to disclose the requested CDR data.

## 6.2. When a consumer amends or withdraws consent

### 6.2.1. Amendment to consent

*CDR Rules: see rules 4.18C and 4.22A.*

An accredited data recipient must notify a data holder in circumstances where it has received a collection consent to collect CDR data from the data holder, and the relevant CDR consumer amends the consent. The data holder must then invite the consumer to amend their authorisation for the disclosure of CDR data accordingly.

---

[49] For more information about the withdrawal of approvals, see paragraphs 9.5–9.8 of our Joint account implementation guidance.

### 6.2.2. Withdrawal of authorisation

*CDR Rules: see rule 4.25 and 4.26A.*

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

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

- stop 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.[50]

**Table 11 Standards and CX Guidelines for amendment and withdrawal of consent**

| Standards/ Guidelines | Section | Sub-section |
|---|---|---|
| CX Standards | Withdrawal Standards | Withdrawing authorisation: Consequences, Withdrawing authorisation: Redundant data |
| | Amending Authorisation Standards | All Sub-sections |
| CX Guidelines | Consent Management (Data holder) | Withdrawal (Default example) |
| | Authorise | Amending authorisations |

### 6.2.3. 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.

If a joint account holder withdraws an authorisation:

- the data holder must stop data sharing from the joint account under the authorisation, as well as data sharing from any other account associated with that authorisation[51]

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

[51] CDR Rules, rule 4.25.

- consumer dashboards must be updated to reflect the withdrawal[52]
- the data holder must notify joint account holders, through its ordinary means of contacting them, that the authorisation has been withdrawn[53]
- the data holder must notify the accredited person that the authorisation has been withdrawn, in accordance with the Standards.[54]

## 6.3. How to disclose consumer data

*CDR Rules: see rule 4.6.*

Once a primary data holder has received authorisation from the consumer to disclose their data to the accredited data recipient, the primary data holder must disclose the required consumer data it is authorised to disclose. This includes data it has received from AEMO.

The primary data holder must act as if it were the data holder for any AEMO data covered by an AEMO data request.

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 12 Standards for disclosing data**

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

The data holder cannot charge a fee for the disclosure of **required consumer data**, but they may charge a fee for the disclosure of **voluntary consumer data**.

[52] CDR Rules, rule 1.15 and rule 4A.13(1)(c).

[53] CDR Rules, rule 4A.14(1).

[54] CDR Rules, rule 4.26A.

The primary data holder must update the consumer's CDR dashboard to show:

- what CDR data was disclosed (including AEMO data)
- when it was disclosed
- the name of the accredited data recipient.[55]

AEMO is not required to notify the CDR consumer that it has disclosed their CDR data to an energy retailer.[56]

## 6.4. When can a data holder refuse to disclose required consumer data?

*CDR Rules: see rules 4.6A and 4.7.*

The data holder must not disclose requested CDR data if the request was made on behalf of a secondary user and the account holder has indicated that they do not approve CDR data being disclosed to a particular accredited data recipient in response to consumer data requests made by that secondary user. This is distinct to the data holder not disclosing requested data due to the withdrawal of a secondary user instruction.[57]

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 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
- it relates to an account that is blocked or suspended
- it 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.

This applies as if the primary data holder were the data holder of any AEMO data covered by a consumer data request. The consequence of this refusal will be that AEMO will not receive a request for its data from the primary data holder.

If the primary data holder refuses to disclose required consumer data, the primary data holder must inform the accredited data recipient of the refusal in accordance with the Standards.

---

55 See Privacy Safeguard 10, CCA, section 56EM; CDR Rules, rule 7.9. The OAIC's CDR privacy safeguard guidelines contain further information about Privacy Safeguard 10.

56 Regulation 28RA(2) of the CC Regulations states the specific privacy safeguards that AEMO is exempt from.

57 See knowledge article on Ceasing secondary user sharing for more information.

**Table 13 Standards for refusal to disclose requested CDR data**

| Standards/ Guidelines | Section | Sub-section |
|---|---|---|
| Standards | Standards | HTTP Response Codes |
| Standards | Non-Functional Requirements | Exemptions to Protect Service |

## 6.5. Disclosing incorrect data

*CDR Rules: see rule 7.10.*

*See also: Privacy Safeguard 11 — CCA, section 56EN.*[58]

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

If a data holder has disclosed CDR data and later becomes aware that some or all of the disclosed data was inaccurate, out of date or incomplete, they must notify the consumer of this. They must provide the 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
- states that the consumer can ask the data holder to disclose the corrected CDR data and that, if such a request is made, the corrected data will be disclosed.

This notice can be given through the data holder's consumer dashboard. It must be provided as soon as practicable and, in any event, within 5 business days after the data holder becomes aware of disclosing the incorrect data.

AEMO is not required to comply with Privacy Safeguard 11.[59]

## 6.6. Correcting incorrect CDR data

*CDR Rules: see rule 7.15 and Schedule 4, clause 6.1.*

*See also: Privacy Safeguard 13 – CCA, section 56EP.*[60]

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

Privacy Safeguard 13 deals with corrections to CDR data. It is modified in relation to energy retailers for data provided by AEMO to leverage the existing NER processes for correcting data. If an energy retailer data holder receives a request for correction of AEMO data, the retailer must:

---

58 The OAIC's CDR privacy safeguard guidelines contain further information about Privacy Safeguard 11.

59 Regulation 28RA of the Competition and Consumer Regulations exempts AEMO from Privacy Safeguards 1, 10, 11 and 13 of the CCA. Furthermore, the AER and Victorian agency only hold product data which is not subject to the Privacy Safeguards.

60 The OAIC's CDR privacy safeguard guidelines contain further information about Privacy Safeguard 13.

- initiate the relevant correction procedures under the NER for NMI standing data and metering data
- provide the requester with information about how the requester can contact the appropriate electricity distributor to have the data corrected if it relates to DER register data.

Also, if an energy retailer data holder receives a request for correction of retailer-held data, the retailer must respond in accordance with their obligations under the CDR Rules, rule 7.15.

AEMO is not required to comply with Privacy Safeguard 13.

# 7. Dispute resolution processes

## 7.1. Internal dispute resolution

*CDR Rules: see rule 6.1 and Schedule 4, clause 5.1(2).*

Retailers in the energy sector must establish an internal dispute resolution (IDR) process. Their process must satisfy the requirements that apply for the energy retailer's standard complaints and dispute resolution procedures under the NERL or the Energy Retail Code (Victoria). As from November 2022, these requirements include:

- An energy retailer or responsible person must develop, make and publish on its website a set of procedures detailing the energy retailer's or responsible person's procedures for handling small customer complaints and dispute resolution procedures.
- The procedures must be regularly reviewed and kept up to date.
- The procedures must be substantially consistent with the latest version of Australian Standard AS ISO 10002-2006 (Customer satisfaction – Guidelines for complaints handling in organisations).

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

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

## 7.2. External dispute resolution

*CDR Rules: see rule 6.2 and Schedule 4, clause 5.2.*

An energy retailer data holder must be a member of the relevant state or territory Energy and Water Ombudsman (EWO) scheme. The Ombudsman schemes are:

- Energy and Water Ombudsman (NSW) Limited
- Energy and Water Ombudsman (Victoria) Limited
- Office of the Energy and Water Ombudsman (Queensland)
- Energy and Water Ombudsman (SA) Limited.

If a jurisdiction does not have an EWO scheme (for example, the Australian Capital Territory), the data holder must take the necessary steps to participate in dispute resolution processes appropriate for CDR consumer complaints provided by that jurisdiction.

Whether or not an energy retailer that is an accredited person is required to also become a member of the Australian Financial Complaints Authority Limited (AFCA) – which is generally required for accredited persons – depends on whether it is a 'limited retailer'.

An energy retailer is a 'limited retailer' if it only uses energy sector CDR data that it collects to provide goods or services in the energy sector and does not use non-energy sector CDR data that it collects to provide goods or services outside the energy sector.

Please refer to Table 14 for a summary of external dispute resolution requirements for retailers that are also accredited persons.

**Table 14 External dispute resolution requirements for the energy sector**

| Circumstance | Required membership in external dispute resolution scheme |
|---|---|
| A retailer that is not an accredited person | EWO |
| A retailer that is also an accredited person, but not a limited retailer | AFCA and EWO |
| A retailer that is also an accredited person, and is a limited retailer | EWO |

# 8. CDR policy

*CDR Rules: see rule 7.2.*

*See also: Privacy Safeguard 1 – CCA, section 56ED.*

Data holders must have a CDR policy that is separate 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 or electronic). For more information on the required format and contents for a CDR policy, see the OAIC's Guide to developing a CDR policy.

Data holders must take reasonable steps to establish and maintain internal practices, procedures and systems to ensure they are complying with their obligations under CDR (Privacy Safeguard 1). For more information, see chapter 1 of the OAIC's Privacy safeguard guidelines.

AEMO is not required to comply with Privacy Safeguard 1.

# 9. Record-keeping requirements

*CDR Rules: see rule 9.3.*

Data holders must keep records of:

- consumer authorisations to disclose CDR data
- amendments or withdrawals of authorisations to disclose CDR data
- notifications of withdrawals of consent to collect CDR data
- if the data holder is a primary data holder, any consumer requests for shared responsibility (SR) data and any responses received, where the primary data holder requested AEMO to disclose SR data for the purpose of responding to a consumer's SR data request[61]
- if the data holder is a secondary data holder (for example, AEMO in the energy sector), any requests from primary data holders for SR data on behalf of a CDR consumer and any responses that were provided. Where the secondary data holder has refused to disclose the requested SR data, they must also retain records of the reasons relied upon to refuse to disclose the SR data, including any rule or data standard
- disclosures of CDR data made in response to consumer data requests. Data holders are not expected to keep copies of the disclosed CDR data itself. A disclosure log evidencing the type of data that was disclosed, when it was disclosed and who it was disclosed to would be sufficient
- any written agreements regarding the obligation to disclose product data for white labelled products
- instances when the data holder has refused to disclose CDR data; and the CDR rule or Standard relied on for this refusal. For each instance where the data holder has refused to disclose CDR data they must, at a minimum, keep a record of:
    - the relevant ground for refusal
    - the date and time they relied upon that ground for 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 10.1.2 of this guide and can also be found on the CDR Support Portal.

[61] CDR Rules, rule 1.23.

- 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 and a person who is entitled to inspect the records asks for an English translation, this must be made available within a reasonable timeframe.

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

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

CDR consumers can request copies of the data holder's records on:

- authorisations they have given to disclose CDR data
- amendments to or withdrawals of those authorisations
- disclosures of CDR data pursuant to those authorisations
- CDR complaint data that relates to them.

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

The OAIC can audit data holders' compliance with the privacy safeguards, and the CDR Rules to the extent they relate to the privacy safeguards or the privacy and confidentiality of CDR data.[62]

# 10. Reporting requirements

## 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.

[62] CDR Rules, rule 9.6.

**Table 15 CDR reporting periods and report due dates**

| Reporting period | Report due by |
|---|---|
| 1 January - 30 June | 30 July |
| 1 July - 31 December | 30 January |

Energy data holders' reporting obligations[63] commence from the date they are required to start sharing consumer data under the CDR Rules. However, if a data holder chooses to enable consumer or product data sharing before the compliance dates stated in the CDR Rules,[64] their obligation to report begins from that earlier date. This includes data sharing during any pilot phases that permit only limited groups of consumers (such as employees) to share their CDR data.

The reports must be in the approved format, and contain specific information.[65]

### 10.1.2. Submitting the reporting form

Data holders must submit rule 9.4 reports to the ACCC and the OAIC. To do this, they must complete an online web form they will find on the CDR Participant Portal. See section 10 of the CDR Participant Portal user guide for more details.

The approved reporting form template for data holders in the energy sector covers consumer data only (product data requests do not apply to energy retailers[66]).

Data holders that have multiple brands must submit a single report containing aggregated data that covers all their brands. The information in the report must be current as at the last day of the relevant reporting period.

The following sections give 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.

### 10.1.3. CDR complaint data summary

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

- the number of CDR consumer complaints received by the data holder
- the number of CDR consumer complaints received for each of the data holder's CDR consumer complaints categories, noting that 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 2 numbers to show 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

63 Under the CDR Rules, rule 9.4.

64 CDR Rules, Schedule 4, clause 8.6

65 See content under the heading 'Submitting the reporting form' at section 10.1.5 for more information.

66 See the CDR Rules, Schedule 4, clause 8.4.

- 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
- the number of CDR product data complaints received - that is, complaints made to the data holder about its required or voluntary product data for which a response or resolution could reasonably be expected.[67]

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

### 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[68]
- consumer data requests by accredited persons on behalf of consumers received during the relevant reporting period.[69]

Data holders are expected to report on both 'successful' CDR data requests (requests that resulted in the requested CDR data being shared) and 'unsuccessful' ones (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.

When requests do not reach the data holder's servers, the data holder may be unable to reasonably identify whether the request is a product data request or a consumer data request. The data holder is not expected to report on these. For example, it is not expected that a data holder will report on requests that are blocked by their global firewall (the firewall set up to protect their entire system) and that they cannot readily identify as a CDR-related request.

### 10.1.5. Refusals to disclose CDR data – total number and reasons

Normally a data holder must share required CDR data in response to a valid request that it receives. However, in some circumstances a data holder may refuse to disclose data in response to a request.[70]

A data holder must inform the requester, CDR consumer or accredited person if they are refusing a request.[71] They must use data standards error codes to indicate why CDR data has not been disclosed.

---

[67] The CDR Rules only stipulate internal dispute resolution requirements for handling complaints from CDR consumers, not CDR product data complaints (see CDR Rules, Schedule 3, clause 5.1(2)(a) and Schedule 4, clause 5.1(4)(a)), 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.

[68] 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.

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

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

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

Table 16 sets out the CDR Rules that permit a refusal to disclose CDR data. It also gives the corresponding HTTP error codes as set out in the Standards.

### Table 16 CDR rules on refusal to disclose data

| Circumstance | CDR Rule | HTTP error code |
|---|---|---|
| Requests received may cause physical, psychological, or financial harm or abuse | 3.5(1)(a),<br>4.7(1)(a) | 403 Forbidden |
| Requests received relate to an account that is blocked or suspended | 3.5(1)(aa),<br>4.7(1)(c) | 404 Not Found<br>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),<br>3.5(1)(b),<br>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),<br>3.5(1)(b),<br>4.7(1)(d) | 429 Too Many Requests |
| The consumer data request originated from a sanctioned country. | 2.5(1)<br>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. |

Return of a 403, 404, 422 and 429 HTTP error code in response to circumstances other than those set out in Table 14 does not constitute a refusal to disclose CDR data under the CDR Rules.

A data holder cannot provide CDR data if they have not received a request or the request is not valid. Therefore, they have not refused to disclose data and they do not need to report a refusal.[72]

For more information on refusals, see various articles on the CDR Support Portal, such as Refusals to disclose during outages and the Consumer Data Standards Guide on Outages. See also Table 17 below.

[72] CDR Rules, rule 9.4.

**Table 17 Refusals to disclose data**

| Valid | Received | Data holder obligation | HTTP code provided to requester |
|---|---|---|---|
| Yes | Yes | Must disclose required CDR data, except in circumstances set out above. | 200 OK<br>403 Forbidden<br>404 Not Found<br>422 Unprocessable Entity<br>429 Too Many Requests |
| No | Yes | Unable to disclose required data in response to an invalid request. | Bad Request<br>Unauthorized<br>405 Method Not Allowed 406 Not Acceptable<br>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<br>504 Gateway Timeout |

Data holders are not necessarily required to 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. Also, they do not have to report on requests they failed to respond to because of scheduled maintenance, an unexpected outage or a period of system instability.

Data holders are not required to record and report information where they have refused to ask for an authorisation (for example, to avoid harm or abuse or for the other reasons in the CDR Rules, rule 4.7).

## 10.2. Updating the register

*CDR Rules: see rule 5.25.*

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

## 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.

Data holders can find the Get Metrics API within the Admin APIs section of the Standards.

To collect the statistics, the CDR Register sends a request to data holders – for example, it calls the data holders' Get Metrics endpoints. In practice, this occurs at approximately 5 am 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 the Get Metrics API available to be called. The data provided in response must be complete and accurate in accordance with the Standards.[73]

### Table 18 Standards for Admin APIs

| Standards/ Guidelines | Section | Sub-section |
|---|---|---|
| Standards | Admin APIs | Get Metrics |

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.[74]

Data holders should 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 publishes the statistics it collects on the CDR.gov.au website. This gives transparency to consumers and other CDR participants about the performance and availability of data holder CDR solutions.

[73] The DSB is required to make related Standards as set out in rule 8.11(1)(f).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.

[74] If a person who is under an obligation to comply with a binding data standard made by the DSB fails to meet that obligation, an application to the Court may be made by the ACCC or a person aggrieved by the failure. See sections 56FA and 56FE of the *Competition and Consumer Act 2010*.