



Australian Government
Office of the Australian Information Commissioner



Consumer Data Right

Privacy Safeguard Guidelines

Version 5.0 November 2023

OAIC

Contents

A comprehensive contents page appears at the beginning of each Chapter.

General matters

Chapter A: Introductory matters

Chapter B: Key concepts

Chapter C: Consent – The basis for collecting, using and disclosing CDR data

Part 1 — Consideration of CDR data privacy

Chapter 1: Privacy Safeguard 1 — Open and transparent management of CDR data

Chapter 2: Privacy Safeguard 2 — Anonymity and pseudonymity

Part 2 — Collecting CDR data

Chapter 3: Privacy Safeguard 3 — Seeking to collect CDR data from CDR participants

Chapter 4: Privacy Safeguard 4 — Dealing with unsolicited CDR data from CDR participants

Chapter 5: Privacy Safeguard 5 — Notifying of the collection of CDR data

Part 3 — Dealing with CDR data

Chapter 6: Privacy Safeguard 6 — Use or disclosure of CDR data by accredited data recipients or designated gateways

Chapter 7: Privacy Safeguard 7 — Use or disclosure of CDR data for direct marketing by accredited data recipients or designated gateways

Chapter 8: Privacy Safeguard 8 — Overseas disclosure of CDR data by accredited data recipients

Chapter 9: Privacy Safeguard 9 — Adoption or disclosure of government related identifiers by accredited data recipients

Chapter 10: Privacy Safeguard 10 — Notifying of the disclosure of CDR data

Part 4 — Integrity of CDR data

Chapter 11: Privacy Safeguard 11 — Quality of CDR data

Chapter 12: Privacy Safeguard 12 — Security of CDR data and destruction of de-identification of redundant CDR data

Part 5 — Correction of CDR data

Chapter 13: Privacy Safeguard 13 — Correction of CDR data

Chapter A:

Introductory matters

Version 5.0, November 2023



Contents

Purpose	3
About the consumer data right	4
About the privacy safeguards	4
Who must comply with the privacy safeguards?	6
Additional roles for accredited persons	7
CDR system roles for unaccredited entities	8
Primary and secondary data holders for shared responsibility data (SR data)	9
Which privacy protections apply in the CDR context?	10
Do the privacy safeguards apply instead of the Privacy Act and the APPs?	11
Accredited persons and accredited data recipients	11
Data holders	12
Designated gateways	12
What happens if an entity breaches the privacy safeguards?	13
Where do I get more information?	13

Purpose

- A.1 The Australian Information Commissioner issues these Privacy Safeguard guidelines under paragraph 56EQ(1)(a) of the *Competition and Consumer Act 2010* (Competition and Consumer Act). These guidelines are not a legislative instrument.¹
- A.2 The Privacy Safeguard guidelines are made in order to guide entities on avoiding acts or practices that may breach the privacy safeguards, which are set out in Division 5 of Part IVD of the Competition and Consumer Act.
- A.3 Part IVD of the Competition and Consumer Act is the legislative base for the consumer data right (CDR) system.
- A.4 The Privacy Safeguard guidelines outline:
- the mandatory requirements in the privacy safeguards and related consumer data rules (CDR Rules) — generally indicated by ‘must’ or ‘is required to’
 - the Information Commissioner’s interpretation of the privacy safeguards and CDR Rules — generally indicated by ‘should’
 - examples that explain how the privacy safeguards and CDR Rules may apply to particular circumstances. Any examples given are not intended to be prescriptive or exhaustive of how an entity may comply with the requirements in the privacy safeguards; the particular circumstances of an entity will also be relevant, and
 - good privacy practice to supplement minimum compliance with the mandatory requirements in the privacy safeguards and CDR Rules — generally indicated by ‘could’.
- A.5 The Privacy Safeguard guidelines are not legally binding and do not constitute legal advice about how an entity should comply with the privacy safeguards and CDR Rules. An entity may wish to seek independent legal advice where appropriate.²
- A.6 In developing the Privacy Safeguard guidelines, the Information Commissioner has had regard to the objects of Part IVD of the Competition and Consumer Act, stated in section 56AA of the Competition and Consumer Act:
- to enable consumers in certain sectors of the Australian economy to require information relating to themselves in those sectors to be disclosed safely, efficiently and conveniently:
 - to themselves for use as they see fit, or
 - to accredited persons for use subject to privacy safeguards
 - to enable any person to efficiently and conveniently access information in those sectors that is about goods (such as products) or services and does not relate to any identifiable, or reasonably identifiable, consumers, and
 - to create more choice and competition, or to otherwise promote the public interest.

¹ Competition and Consumer Act, subsection 56EQ(5).

² Further, if there is an inconsistency between the Privacy Safeguard guidelines and the CDR Rules, the rules prevail over the guidelines to the extent of the inconsistency: Competition and Consumer Act, subsection 56EQ(4).

About the consumer data right

- A.7 The CDR aims to provide greater choice and control for Australians over how their data is used and disclosed. It allows consumers to direct a business to securely transfer particular data in a usable form to an accredited person or other permitted person under the CDR rules.
- A.8 Individual consumers and small, medium and large business consumers are able to exercise the CDR in relation to data that is covered by the CDR system.
- A.9 The CDR commenced in the banking sector in 2019 (known as ‘Open Banking’) and the energy sector in 2022 (with staged application to continue into 2024).³Next, CDR will be implemented in the non-bank lending sector, and will continue to be introduced across the broader economy as designated by the Minister.⁴

About the privacy safeguards

- A.10 The privacy safeguards are legally binding statutory provisions, which ensure the security and integrity of the CDR system. The specific requirements for certain privacy safeguards are set out in the CDR Rules.
- A.11 The privacy safeguards set out standards, rights and obligations in relation to collecting, using, disclosing and correcting CDR data for which there are one or more CDR consumers:
- Privacy Safeguard 1 – Open and transparent management of CDR data
 - Privacy Safeguard 2 – Anonymity and pseudonymity
 - Privacy Safeguard 3 – Soliciting CDR data from CDR participants
 - Privacy Safeguard 4 – Dealing with unsolicited CDR data from CDR participants
 - Privacy Safeguard 5 – Notifying of the collection of CDR data
 - Privacy Safeguard 6 – Use or disclosure of CDR data by accredited data recipients or designated gateways
 - Privacy Safeguard 7 – Use or disclosure of CDR data for direct marketing by accredited data recipients or designated gateways
 - Privacy Safeguard 8 – Overseas disclosure of CDR data by accredited data recipients
 - Privacy Safeguard 9 – Adoption or disclosure of government related identifiers by accredited data recipients
 - Privacy Safeguard 10 – Notifying of the disclosure of CDR data
 - Privacy Safeguard 11 – Quality of CDR data

³ For staged application of CDR Rules in the energy sector, see CDR Rules, Part 8 of Schedule 4. For further information about staged application of CDR Rules, see [Chapter B \(Key concepts\)](#).⁴ For more information about the rollout of the CDR, see <https://www.cdr.gov.au/rollout>.

⁴ For more information about the rollout of the CDR, see <https://www.cdr.gov.au/rollout>.

- Privacy Safeguard 12 – Security of CDR data, and destruction or de-identification of redundant CDR data
 - Privacy Safeguard 13 – Correction of CDR data
- A.12 The privacy safeguards only apply to CDR data for which there are one or more ‘CDR consumers’.⁵ A CDR consumer can be an individual or a business enterprise.⁶
- A.13 There are a number of factors that determine whether CDR data has a ‘CDR consumer’.⁷ In particular, for CDR data to have a CDR consumer, at least one person needs to be identifiable or reasonably identifiable from the CDR data or other information held by the relevant entity.⁸ See [Chapter B \(Key concepts\)](#) of the CDR Privacy Safeguard Guidelines for the full meaning of ‘CDR consumer’.
- A.14 The privacy safeguards do not apply where there is no CDR consumer⁹ because, for example, there is no person that is identifiable or reasonably identifiable from the data. Product data is an example of CDR data for which there is no CDR consumer.
- A.15 The privacy safeguards are structured to reflect the CDR data lifecycle. They are grouped into five subdivisions within Division 5 of Part IVD of the Competition and Consumer Act:
- Subdivision B – Consideration of CDR data privacy (Privacy Safeguards 1 and 2)
 - Subdivision C – Collecting CDR data (Privacy Safeguards 3, 4 and 5)
 - Subdivision D – Dealing with CDR data (Privacy Safeguards 6, 7, 8, 9 and 10)
 - Subdivision E – Integrity of CDR data (Privacy Safeguards 11 and 12)
 - Subdivision F – Correction of CDR data (Privacy Safeguard 13)
- A.16 The requirements in each of these privacy safeguards interact with and complement each other.
- A.17 The privacy safeguards extend to certain acts, omissions, matters and things outside Australia.¹⁰
- A.18 In respect of CDR data held within Australia, the privacy safeguards apply to all persons, including foreign persons.¹¹

⁵ Competition and Consumer Act, subsection 56EB(1).

⁶ Competition and Consumer Act, subsection 56AI(3); Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019, paragraphs 1.100 and 1.101. See also *Acts Interpretation Act 1901* (Cth), section 2C, which provides that in any Act (including the references to ‘person’ in the Competition and Consumer Act, subsection 56AI(3)), expressions used to denote persons generally include a body politic or corporate as well as an individual.

⁷ Competition and Consumer Act, subsection 56AI(3).

⁸ Competition and Consumer Act, paragraph 56AI(3)(c). The ‘relevant entity’ here is the data holder, accredited data recipient, or person holding data on their behalf: Competition and Consumer Act, subsection 56AI(3)(c)(ii) referencing subsection 56AI(3)(b).

⁹ Competition and Consumer Act, subsection 56AI(3)(c).

¹⁰ Competition and Consumer Act, subsection 56AO(1). In particular, the Privacy Safeguards apply for CDR data held inside Australia (subsection 56AO(2)), acts or omissions by (or on behalf of) an Australian person (paragraph 56AO(3)(a)), acts or omissions occurring wholly or partly in Australia or on board an Australian aircraft or ship (paragraph 56AO(3)(b)), or acts or omissions occurring wholly outside Australia if an Australian person suffers or is likely to suffer financial or other disadvantage as a result of the act or omission (paragraph 56AO(3)(c)).

¹¹ Competition and Consumer Act, subsection 56AO(2).

- A.19 In respect of an act or omission relating to CDR data held outside Australia, the privacy safeguards only apply if the act or omission:¹²
- is done by or on behalf of an Australian person
 - occurs wholly or partly in Australia, or wholly or partly on board an Australian aircraft or an Australian ship, or
 - occurs wholly outside Australia, and an Australian person suffers, or is likely to suffer, financial or other disadvantage as a result of the act or omission.

How to use these guidelines

- A.20 The structure of the Privacy Safeguard guidelines reflects the structure of the privacy safeguards: Privacy Safeguards 1 to 13 are each dealt with in separate chapters.
- A.21 The number of the chapter corresponds to the number of the privacy safeguard.
- A.22 Chapter B contains guidance on general matters, including an explanation of key concepts that are used throughout the privacy safeguards and the Privacy Safeguard guidelines.
- A.23 Chapter C contains guidance on consent, which is the primary basis for collecting, using and disclosing CDR data under the CDR system.
- A.24 These guidelines should be read together with the full text of Division 5 of Part IVD of the Competition and Consumer Act and the CDR Rules.

Who must comply with the privacy safeguards?

- A.25 The privacy safeguards apply to the following entities who are authorised or required under the CDR system to collect, use or disclose CDR data for which there is at least one CDR consumer:
- **accredited persons:** persons who have been granted accreditation (at either the unrestricted or sponsored level)¹³ by the Australian Competition and Consumer Commission (ACCC) to receive data through the CDR system¹⁴
 - **accredited data recipients:** accredited persons who have collected the CDR data from a data holder or another accredited data recipient¹⁵
 - **data holders:** persons who hold data specified in a designation instrument and meet relevant conditions in the Act, who may be required to disclose data under the CDR system (including primary and secondary data holders for shared responsibility data),¹⁶ and

¹² Competition and Consumer Act., subsection 56AO(3).

¹³ CDR Rules, rule 5.1A. Persons accredited at the sponsored level are known as ‘affiliates’.

¹⁴ For specific requirements, see Competition and Consumer Act, section 56CA.

¹⁵ For specific requirements, see Competition and Consumer Act, section 56AK.

¹⁶ At a high level, these conditions are that the person is also designated, that the person is a reciprocal data holder, or that the person meets certain conditions in the rules. For specific requirements, see Competition and Consumer Act, section 56AJ. For definitions of primary and secondary data holders, see CDR Rules, subrule 1.7(1).

- **designated gateways:** entities designated by the Minister as responsible for facilitating the transfer of information between data holders and accredited persons.¹⁷

A.26 Each of these types of entities are defined in the Competition and Consumer Act and discussed further in [Chapter B \(Key concepts\)](#).

A.27 Each privacy safeguard chapter specifies the type of entity to which it applies.

Additional roles for accredited persons

A.28 Some accredited persons perform specific roles in the CDR system. This includes some roles under a sponsorship arrangement, a CDR representative arrangement, or an outsourced service provider arrangement.

A.29 The sponsored accreditation model allows a person accredited to the ‘sponsored’ level (an ‘affiliate’) to provide goods or services directly to a consumer where the affiliate has a sponsorship arrangement with an unrestricted accredited person (a ‘sponsor’).¹⁸ The model is intended to provide an alternative to unrestricted accreditation and support a broader array of business arrangements in the CDR system.¹⁹ The two roles for accredited persons under this model are:

- **Affiliates:** persons who have entered into a written contract, known as a sponsorship arrangement, with another person with unrestricted accreditation (known as the sponsor).²⁰ Affiliates are accredited to the sponsored level, must comply with the privacy safeguards and are liable in their own right for their handling of CDR data.
- **Sponsors:** persons who have entered into a written contract, known as a sponsorship arrangement, with another person (known as the affiliate) under which the sponsor discloses CDR data they hold as an accredited data recipient to the affiliate.²¹ Sponsors are accredited to the unrestricted level and must continue to comply with the privacy safeguards when acting at their affiliate’s request.

Both sponsors and affiliate are required to comply with the privacy safeguards when handling CDR data.

A.30 The CDR representative model allows an unaccredited person (a ‘CDR representative’) to use or disclose CDR data to provide CDR goods or services directly to a consumer, where they have a CDR representative arrangement with an unrestricted accredited person (a ‘CDR representative principal’).²² As with sponsored accreditation, the CDR representative model is intended to facilitate the participation of a broader array of business models in the CDR system.²³ The role for accredited persons under this model is:

¹⁷ For specific requirements, see Competition and Consumer Act, subsection 56AL(2).

¹⁸ CDR Rules, rule 1.10D.

¹⁹ See [Chapter B \(Key concepts\)](#) for additional information about sponsorship arrangements, sponsors and affiliates.

²⁰ CDR Rules, rule 1.10D.

²¹ CDR Rules, rule 1.10D.

²² CDR Rules, rule 1.10AA.

²³ See [Chapter B \(Key concepts\)](#) for additional information about CDR representative arrangements, CDR representative principals and CDR representatives.

- **CDR representative principal:** persons who have entered into a CDR representative arrangement with a person without accreditation, known as ‘the CDR representative’. CDR representative principals are accredited to the unrestricted level, collect CDR data on behalf of their CDR representative and are liable for the actions of the CDR representative.²⁴

A.31 A CDR outsourcing arrangement allows an accredited or unaccredited outsourced service provider (an ‘OSP’) engaged by an accredited person (a ‘principal’) to do one or both of the following:

- collect CDR data from a CDR participant on behalf of the OSP chain principal
- provide goods or services to the principal using CDR data that the OSP collected on the principal’s behalf or that was disclosed to the OSP by that principal.²⁵

The two roles for accredited persons under this type of arrangement are:

- **Accredited outsourced service providers (OSPs):** accredited entities who collect CDR data on behalf of a principal, or provide goods or services to the principal under a CDR outsourcing arrangement.²⁶ All OSPs (whether accredited or unaccredited) must comply with the terms of their written contract with the principal that engaged them. An accredited OSP must also comply with the privacy safeguards.
- **Principals under a CDR outsourcing arrangement:** accredited entities who engage an OSP under a CDR outsourcing arrangement.²⁷ Principals who are ‘chain principals’²⁸ are liable for any collection, use or disclosure of service data by their OSP or their OSP’s subcontractors.²⁹

A.32 Each of these specific roles is discussed further in [Chapter B \(Key concepts\)](#).

CDR system roles for unaccredited entities

A.33 In specified circumstances, an entity who is not an accredited person, accredited data recipient, data holder or designated gateway can handle CDR data within the CDR system. These entities are not directly bound by the privacy safeguards set out in Division 5 of Part IVD of the Competition and Consumer Act. This includes entities performing the following roles:

- **CDR representative:** further to the discussion of the CDR representative model in paragraph A.30 above, a CDR representative is a person who has entered into a CDR representative arrangement with a CDR representative principal under which they can

²⁴ As unaccredited entities, ‘CDR representatives’ are discussed below under the ‘CDR system roles for unaccredited entities’ heading.

²⁵ CDR Rules, subrule 1.10(3)(a).

²⁶ While there is no requirement for an OSP to be accredited under the CDR system, some accredited persons may choose to enter a CDR outsourcing arrangement in a provider capacity.

²⁷ CDR Rules, rule 1.10.

²⁸ An ‘OSP chain principal’ is the initial OSP principal entity in a chain of CDR outsourcing arrangements – see ‘Outsourcing’ in Chapter B: Key concepts for more information.

²⁹ CDR Rules, rule 1.16. Principals who are not ‘chain principals’ do not carry this liability. For further discussion of subcontracting under a further outsourcing arrangement, see the discussion under ‘Outsourced service provider’ in [Chapter B \(Key concepts\)](#).

use or disclose CDR data to provide goods or services directly to a consumer. As unaccredited entities, CDR representatives are not directly bound by the privacy safeguards, but must comply with the terms of their written contract with their CDR representative principal. These contractual obligations apply in addition to other privacy obligations a CDR representative will have under the *Privacy Act 1988* (Privacy Act) if they are an APP entity.

- **Unaccredited outsourced service provider (OSP):** further to the discussion of CDR outsourcing arrangements in paragraph A.31, an unaccredited OSP is an unaccredited person who collects CDR data from a CDR participant on behalf of an OSP chain principal under a CDR outsourcing arrangement, and/or provides goods or services to an OSP principal under a CDR outsourcing arrangement using CDR data that it has collected on behalf of the OSP chain principal or that has been disclosed to it by the OSP principal. All OSPs (whether accredited or unaccredited) must comply with the terms of their written contract with the principal that engaged them. As unaccredited OSPs are not bound by the privacy safeguards, these contractual obligations apply in addition to other privacy obligations unaccredited OSPs will have under the Privacy Act if they are APP entities. Where an unaccredited OSP enters a further CDR outsourcing arrangement, that OSP will be the OSP principal under that further arrangement.

A.34 While CDR representatives and unaccredited OSPs are not directly bound by the Privacy Safeguards set out in Division 5 of Part IVD of the Competition and Consumer Act, they will be party to either a CDR representative arrangement³⁰ or a CDR outsourcing arrangement³¹ as required by the CDR Rules. In accordance with those rules, these written contracts will reflect many of the obligations in the privacy safeguards. This means that these Guidelines nevertheless contain useful guidance which will be applicable to CDR representatives and unaccredited OSPs in meeting their contractual obligations.

A.35 In specified circumstances, CDR data can be disclosed outside of the CDR system to unaccredited entities. This includes disclosures to ‘trusted advisers’, disclosures to any person under a business consumer disclosure consent, and disclosures of ‘CDR insights’ to any person. These recipients are not bound by the Privacy Safeguards. However, these CDR data recipients should consider any professional or other regulatory obligations they may have in relation to their handling of a consumer’s data (including privacy obligations under the Privacy Act if they are an APP entity) and handle data transparently and in the way a consumer would expect.

A.36 Further information on these roles is contained in [Chapter B \(Key concepts\)](#).

Primary and secondary data holders for shared responsibility data (SR data)

A.37 Where the CDR Rules specify CDR data as shared responsibility data (also called SR data in the CDR Rules),³² some data holders will perform special roles as a primary or secondary data holder for the SR data.

³⁰ CDR Rules, rule 1.10AA.

³¹ CDR Rules, rule 1.10.

³² See CDR Rules, rule 1.7, and [Chapter B \(Key concepts\)](#) for further information on SR data.

A.38 Primary and secondary data holders, and SR data, are discussed further in [Chapter B \(Key concepts\)](#).

Which privacy protections apply in the CDR context?

CDR entity	Privacy safeguards that apply in the CDR context	APPs that apply in the CDR context
Accredited person	Privacy safeguards 1–4³³	None. Privacy Safeguards 1–4 apply instead of the corresponding APPs³⁴
Accredited data recipient³⁵	Privacy safeguards 1, 2 and 5–13	None. The APPs do not apply to an accredited data recipient of a consumer’s CDR data in relation to that data
Data holder (other than the Australian Energy Market Operator Limited (AEMO))	Privacy safeguards 1, 10, 11 and 13	All APPs (1–13) APPs 10 and 13 are replaced by Privacy Safeguards 11 and 13 once the data holder is required or authorised to disclose the CDR data under the CDR Rules
Data holder (AEMO)	None. AEMO is exempt from the privacy safeguards that otherwise apply to data holders.³⁶	All APPs (1–13)

³³ See the Competition and Consumer Act, sections 56EC(4), 56ED, 56EE(1)(b), 56EF and 56EG.

³⁴ Note: If Privacy Safeguards 1 – 4 do not apply, the corresponding APPs may continue to apply to other handling of the individual’s personal information where the accredited person is an APP entity (see the Competition and Consumer Act, subsections 56EC(4) and (5)(aa)). Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See the Privacy Act, subsection 6E(1D).

³⁵ An accredited person becomes an accredited data recipient for CDR data when:

- CDR data is held by (or on behalf of) the person
- the CDR data, or any other CDR data from which it was directly or indirectly derived, was disclosed to the person under the consumer data rules, and
- the person is neither a data holder, nor a designated gateway, for the first mentioned CDR data. See the Competition and Consumer Act, section 56AK.

³⁶ In the energy sector, AEMO is exempt from privacy safeguards 1, 11 and 13, and is exempt from privacy safeguard 10 in relation to CDR data held by AEMO that AEMO discloses to an energy retailer as required or permitted by the Competition and Consumer Act: see the Competition and Consumer Regulations 2010 (Competition and Consumer Regulations), sub-

CDR entity	Privacy safeguards that apply in the CDR context	APPs that apply in the CDR context
Designated gateway	Privacy safeguards 1, 6, 7 and 12	APPs 1-5, 8-10 and 12-13

Do the privacy safeguards apply instead of the Privacy Act and the APPs?

- A.39 Subsection 56EC(4) of the Competition and Consumer Act sets out when a privacy safeguard applies instead of an Australian Privacy Principle (APP) under the *Privacy Act 1988* (Privacy Act).
- A.40 The privacy safeguards apply only to CDR data for which there are one or more CDR consumers.³⁷
- A.41 As set out in paragraph A.13 above, for there to be a CDR consumer, at least one person must be identifiable or reasonably identifiable from the CDR data or other information held by the relevant entity. As such, where the consumer is an individual, CDR data protected by the privacy safeguards will contain information about an identified or reasonably identifiable individual, and will therefore also be ‘personal information’ under the Privacy Act.
- A.42 To work out when the privacy safeguards apply, an entity needs to consider what capacity they are acting in – as a data holder, accredited person/accredited data recipient, or designated gateway.
- A.43 In each chapter in these guidelines, the interaction between the privacy safeguard and corresponding APP is discussed.

Accredited persons and accredited data recipients

- A.44 For an accredited person, or accredited data recipient of CDR data, the privacy safeguards apply instead of the APPs in relation to the handling of the CDR data within the CDR system.³⁸

regulation 28RA(2). Certain privacy safeguard obligations that would otherwise apply to the AEMO are instead applied to retailers who receive data from AEMO, with some modifications and exceptions: see Competition and Consumer Regulations, sub-regulation 28RA(3)-(4).

³⁷ Competition and Consumer Act, subsection 56EB(1).

³⁸ The APPs do not apply to an accredited data recipient of CDR data, in relation to that CDR data - Competition and Consumer Act, paragraph 56EC(4)(a). However, subsection 56EC(4) does not affect how the APPs apply to accredited persons and accredited data recipients who are APP entities, in relation to the handling of personal information outside the CDR system. (Note: Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See Privacy Act, subsection 6E(1D).) Subsection 56EC(4) also does not affect how the APPs apply to an accredited person who does not become an accredited data recipient of the CDR data (other than for Privacy Safeguards 1 – 4). See Competition and Consumer Act, paragraph 56EC(5)(aa)).

Data holders

- A.45 For data holders (other than AEMO), the APPs will apply to CDR data that is also personal information with the exception of APPs 10 (quality of personal information) and 13 (correction of personal information). These two APPs are replaced by Privacy Safeguards 11 (quality of CDR data) and 13 (correction of CDR data) once the data holder is required or authorised to disclose the CDR data under the CDR Rules. Privacy Safeguard 10 (notifying of the disclosure of CDR data) does not have an APP equivalent and applies to data holders in addition to all other privacy protections.
- A.46 Data holders (other than AEMO) must also comply with both APP 1 and Privacy Safeguard 1 which relate to open and transparent management of personal information and CDR data respectively. As explained above, these obligations apply concurrently and the obligations in Privacy Safeguard 1 do not displace the APP 1 obligations.
- A.47 AEMO is currently the only data holder who is exempt from the Privacy Safeguards that otherwise apply to data holders.³⁹ The APPs continue to apply to any CDR data held by AEMO that is also personal information.

Designated gateways

- A.48 The APPs will continue to apply to designated gateways for CDR data that is personal information except in relation to the use and disclosure of CDR data, including for direct marketing purposes, for which Privacy Safeguards 6 (use or disclosure of CDR data) and 7 (direct marketing) apply instead of APP 6 and APP 7, and the security of the CDR data, for which Privacy Safeguard 12 (security of CDR data) applies instead of APP 11.
- A.49 Further, designated gateways must comply with Privacy Safeguard 1 (open and transparent management of CDR data) in addition to APP 1. As explained above, these obligations apply concurrently and the obligations in Privacy Safeguard 1 do not displace the APP 1 obligations.

Note: *There are currently no designated gateways in the banking sector or energy sector.⁴⁰ See Chapter B (Key concepts) for the meaning of designated gateway.*

³⁹ At date of publication. See Competition and Consumer Regulations, regulation 28RA.

⁴⁰ For the banking sector, see the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019. For the energy sector, the energy designation specifies AEMO as a gateway for certain information: Consumer Data Right (Energy Sector) Designation 2020, subsection 6(4). However, at the time of publication, AEMO is not a designated gateway for any CDR data because under current CDR Rules, no CDR data is (or is to be) disclosed to AEMO because of the reasons in the Competition and Consumer Act, paragraph 56AL(2)(c).

There are also no designated gateways in the telecommunications sector (Consumer Data Right (Telecommunications Sector) Designation 2022) or non-bank lending sector (Consumer Data Right (Non-Bank Lenders) Designation 2022), although unlike the banking and energy sectors, at the date of publication of these guidelines, there are no rules allowing for the sharing of designated telecommunications data or non-bank lending data under the CDR system.

What happens if an entity breaches the privacy safeguards?

- A.50 The Information Commissioner has powers to investigate possible breaches of the privacy safeguards, either following a complaint by a consumer who is an individual or small business or on the Information Commissioner’s own initiative.
- A.51 Where a consumer makes a complaint, the Information Commissioner will generally attempt to conciliate the complaint.
- A.52 The Information Commissioner has a range of enforcement powers and other remedies available. These powers include those available under:
- Part V of the Privacy Act,⁴¹ for example the power to make a determination,⁴² and
 - Part IVD of the Competition and Consumer Act, for example the privacy safeguards attract a range of civil penalties enforceable by the Information Commissioner.⁴³
- A.53 Where a CDR representative or an OSP breaches their contractual obligations, their CDR representative principal or OSP chain principal (as applicable) would be liable and held to have breached the relevant privacy safeguard or related CDR Rule. Such conduct will trigger the Information Commissioner’s investigation and enforcement powers against the accredited party, either following a complaint by a consumer who is an individual or small business or on the Information Commissioner’s own initiative.
- A.54 The ACCC also has a strategic enforcement role where there are repeated or serious breaches. The Office of the Australian Information Commissioner (OAIC) and the ACCC have published a joint [Compliance and Enforcement Policy](#) for the CDR intended to help consumers and CDR entities understand the approach that the OAIC and ACCC will take to encourage compliance with the CDR Rules, legislation (including privacy safeguards and Consumer Data Standards) and how they will respond to breaches of the regulatory framework. The OAIC has also published a [CDR Regulatory Action Policy](#) which sets out the OAIC’s priorities, goals and principles in regulating the CDR, and complements the joint Compliance and Enforcement Policy.

Where do I get more information?

- A.55 The OAIC has further information about the CDR and its role on the OAIC website, see www.oaic.gov.au/consumer-data-right.

⁴¹ The Competition and Consumer Act, subsection 56ET(4), extends the application of Part V of the Privacy Act to a privacy safeguard breach relating to the CDR data of a consumer who is an individual or small business.

⁴² Privacy Act, section 52.

⁴³ Competition and Consumer Act, section 56EU. All privacy safeguards contain civil penalty provisions except for Privacy Safeguard 2.

Chapter B:

Key concepts

Version 5.0, November 2023



Contents

About this Chapter	5
Accredited data recipient	7
Accredited person	8
Unrestricted accreditation	8
Sponsored accreditation	9
Affiliate	9
Assurance report	10
Attestation statement	10
Australian Privacy Principles, APPs	10
Authorise, Authorisation	10
CDR data	11
Derived CDR data	11
SR or shared responsibility data	11
CDR insight	12
CDR participant	12
CDR policy	12
CDR receipt	13
CDR representative principal	13
CDR representative	14
CDR representative arrangement	15
CDR system	16
Collect	17
Consent	17
Collection consent	18
Use consent	18
AP disclosure consent	18
Direct marketing consent	18
TA disclosure consent	19
Insight disclosure consent	19
De-identification consent	19
Business consumer disclosure consent	20
Business consumer statement	20
Consumer, CDR consumer, ‘eligible’ CDR consumer and CDR business consumer	20
Reasonably identifiable	21
Relates to	22

Associate	23
Eligible CDR consumer	23
CDR business consumer	25
Consumer dashboard, or dashboard	25
Consumer data request	26
SR data request	27
Accredited person request service	27
Valid request	27
Competition and Consumer Regulations	28
CDR Rules	28
Current	29
Current consent	29
Current authorisation	30
Consumer Experience Guidelines	30
Data holder	31
Primary and secondary data holders	32
Earliest holding day	33
Data minimisation principle	33
Data standards	34
Consumer Experience Standards	34
Designated gateway	35
Designation instrument	35
Disclosure	36
Eligible	36
General research	37
Holds	37
Joint account	37
Outsourcing	38
OSPs, OSP principals and OSP chain principals	38
Service Data	39
CDR outsourcing arrangement	39
Purpose	41
Reasonable, Reasonably	42
Reasonable steps	42
Redundant data	43
Required consumer data	43
Required or authorised by an Australian law or by a court/tribunal order	43
Australian law	43
Court/tribunal order	44
Required	44

Authorised	44
Required or authorised to use or disclose CDR data under the CDR Rules	45
Required	45
Authorised	45
Required product data	46
Service data	46
Sponsor	46
Sponsorship Arrangement	47
Staged application	47
Trusted adviser	48
Use	49
Voluntary consumer data	50
Voluntary product data	50

About this Chapter

- B.1 This Chapter outlines some key words and phrases that are used in the privacy safeguards and consumer data rules (CDR Rules).
- B.2 The example below outlines a key information flow in the CDR system and demonstrates the operation of several key concepts in the CDR system. While it outlines a key information flow, it does not account for all CDR arrangements and sector specific nuances.
- B.3 Further information regarding the underlined terms can be found within this Chapter under the corresponding heading.

Key concepts in the CDR system explained



Accredited persons

Meadow Cost Comparison wants to receive CDR data to provide product comparison services to consumers under the CDR system, so it applies to the ACCC (the Data Recipient Accreditor)¹ to become accredited at the unrestricted level. (It is also possible to be accredited at the ‘sponsored’ level). The ACCC is satisfied that Meadow Cost Comparison meets the accreditation criteria under the CDR Rules and grants unrestricted accreditation. Meadow Cost Comparison is therefore an **accredited person** and is allowed to receive CDR data under the CDR system.



CDR data

Carly is a customer of Sunny Bank but is interested in what alternative credit card rates other banks could provide. Carly has an existing credit card, and provides Meadow Cost Comparison with a valid request (with her consent) to collect her account numbers, balances and features from Sunny Bank and use that information for the purposes of comparing credit card rates. Account numbers, balances, and features fall into a class of information set out in the designation instrument for the banking sector,² and are therefore **CDR data**.

¹ See paragraph B.7.

² Competition and Consumer Act, subsection 56AI(1). The Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019 sets out the classes of information in the banking sector that are subject to the CDR system, the persons who hold this information and will be required or authorised to transfer the information under the regime, and the earliest date that the information must have begun to be held to be subject to the CDR system.



Data holders

Sunny Bank is a **data holder**. This is because:

- Carly's CDR data is within a class of information specified in the designation instrument for the banking sector
- Carly's CDR data is held by Sunny Bank on or after the earliest holding day³
- Sunny Bank is not a designated gateway for the data, and
- Sunny Bank is an authorised deposit-taking institution (one of the categories specified in paragraph 56AJ(1)(d) of the Competition and Consumer Act).⁴



CDR consumers

Carly is a **CDR consumer for CDR data** because:

- the CDR data relates to Carly because it is about her credit card
- the CDR data is held by a data holder (Sunny Bank), being one of the entity types listed in paragraph 56AI(3)(b),⁵ and
- Carly is identifiable or reasonably identifiable from the CDR data.⁶

³ For the banking sector, 1 January 2017 is the 'earliest holding day' specified in the designation instrument: Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019, subsection 5(3). See paragraph B.167 for further information.

⁴ Sunny Bank is an authorised-deposit taking institution, which has been specified as a relevant class of persons in the designation instrument for the banking sector (the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019).

⁵ See paragraph B.162 for further information.

⁶ Competition and Consumer Act, subsection 56AI(3).



Accredited data recipients

Meadow Cost Comparison, as an unrestricted accredited person makes a consumer data request on Carly's behalf by asking Sunny Bank to disclose Carly's CDR data.⁷ Sunny Bank asks Carly to authorise the disclosure of her CDR data to Meadow Cost Comparison.

Upon receiving authorisation from Carly to do so, Sunny Bank discloses Carly's CDR data to Meadow Cost Comparison.

Following receipt of Carly's data from Sunny Bank, Meadow Cost Comparison is now an **accredited data recipient** of CDR data. This is because Meadow Cost Comparison:

- is an accredited person
- has been disclosed CDR data from a data holder (Sunny Bank) under the CDR Rules
- holds that CDR data, and
- does not hold that CDR data as a data holder or designated gateway.⁸



Consumer dashboards

Given that Meadow Cost Comparison has made a consumer data request on Carly's behalf, Meadow Cost Comparison provides Carly with a **consumer dashboard**.⁹ A consumer dashboard is an online service that allows Carly to manage and view details about her consent.

Upon receiving the consumer data request from Meadow Cost Comparison, Sunny Bank also provides Carly with a consumer dashboard that will allow Carly to manage and view details about her authorisation.¹⁰

Accredited data recipient

B.4 A person is an 'accredited data recipient' of a consumer's CDR data if the person:

- is an accredited person (see paragraphs B.7 to B.11 below)
- was disclosed CDR data from a CDR participant under the CDR Rules¹¹

⁷ Only entities with unrestricted accreditation can collect CDR data directly from a data holder. In this example, we have specified that Meadow Cost Comparison holds unrestricted accreditation which allows it to make a consumer data request directly to Sunny Bank for collection of Carly's CDR data.

⁸ Competition and Consumer Act, section 56AK.

⁹ CDR Rules, rule 1.14.

¹⁰ CDR Rules, rule 1.15.

¹¹ If an accredited person is disclosed CDR data otherwise than in accordance with the CDR Rules (for instance, outside the CDR system), they will not become an 'accredited data recipient' for that CDR data.

- holds that CDR data (or has another person hold that CDR data on their behalf), and
 - does not hold that CDR data as a data holder or designated gateway.¹²
- B.5 Accredited persons should be aware that where they are seeking consent from a consumer to collect, use or disclose CDR data, and the CDR data is yet to be collected, they are not yet an accredited data recipient of the CDR data.
- B.6 For an illustration of how and when an accredited person becomes an accredited data recipient of CDR data, see the example under paragraph B.3.

Accredited person

- B.7 An ‘accredited person’ is a person who has been granted accreditation by the Data Recipient Accreditor.¹³ The Data Recipient Accreditor is the Australian Competition and Consumer Commission (ACCC).¹⁴
- B.8 An example of an accredited person could be a bank, a fintech, a retailer such as an electricity retailer or financial comparison service or another business that wishes to provide a good or service using CDR data. This is demonstrated by the example under paragraph B.3.
- B.9 To be granted an accreditation, the person must satisfy the relevant accreditation criteria in Part 5 of the CDR Rules.
- B.10 A data holder may be accredited under the CDR system, and therefore be both a data holder and an accredited person.
- B.11 There are 2 levels of accreditation:
- unrestricted accreditation, and
 - sponsored accreditation.¹⁵

Unrestricted accreditation

- B.12 Entities with unrestricted accreditation can undertake the full range of functions permitted for accredited persons under the CDR Rules.
- B.13 A person with unrestricted accreditation is able to sponsor other accredited persons in the CDR system under sponsorship arrangements, and/or enter into CDR representative arrangements with unaccredited entities.¹⁶ See paragraphs B.49 to B.53 and B.251 to B.260 for more information.

In this situation, the *Privacy Act 1988* and the APPs would apply (to the extent the CDR data is personal information, and where the accredited person is an APP entity). Note: Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See s 6E(1D) of the Privacy Act.

¹² Competition and Consumer Act, section 56AK.

¹³ Competition and Consumer Act, subsection 56CA(1).

¹⁴ The ACCC has been appointed as the Data Recipient Accreditor by the Minister under section 56CG of the Competition and Consumer Act.

¹⁵ CDR Rules, rule 5.1A.

¹⁶ CDR Rules, rules 1.10D and 1.10AA.

Sponsored accreditation

- B.14 A person with ‘sponsored accreditation’ has or intends to have a sponsorship arrangement with an unrestricted accredited person who is willing to act as their sponsor in the CDR system. There are certain restrictions on participation in the CDR system for those entities with sponsored accreditation (see ‘Affiliate’ below).
- B.15 A person accredited to the sponsored level and in a sponsorship arrangement will be known as an ‘affiliate’ of its sponsor.

Affiliate

- B.16 An ‘affiliate’ is a person with sponsored accreditation who has entered into a written contract (a ‘sponsorship arrangement’), with another person with unrestricted accreditation (the ‘sponsor’) that meets certain requirements as set out in paragraphs B.258 to B.260.¹⁷
- B.17 The sponsored accreditation model allows a person who is accredited to the ‘sponsored’ level (rather than the unrestricted level) to provide goods or services directly to a consumer.
- B.18 An affiliate may directly collect CDR data from an accredited data recipient (via a consumer data request made under rule 4.7A) or request that their sponsor collect CDR data from a data holder, ADR or CDR representative on their behalf. They cannot collect data directly from a data holder or CDR representative.¹⁸
- B.19 An affiliate cannot engage an outsourced service provider (OSP) to collect CDR data from a CDR participant on their behalf¹⁹ and they cannot have a CDR representative.²⁰
- B.20 As a sponsor and their affiliate are both accredited persons, each entity will be liable in their own right for their handling of CDR data. In addition, where a sponsor collects a consumer’s CDR data at the affiliate’s request, that data is taken also to have been collected by the affiliate.²¹ This ensures that limitations on uses and disclosures apply to affiliates.
- B.21 The CDR Rules contain some specific obligations for affiliates, particularly in relation to consent, notification, dashboards and CDR policy content. For more information, see Chapter C (paragraphs C.15, C.30 – C.31, C.64, C.73, C.77, C.101, diagram after C.116), Chapter 1 (paragraph 1.55), Chapter 3 (paragraphs 3.26 – 3.27, 3.36 – 3.38, diagram after 3.41), Chapter 5 (paragraph 5.3, 5.10, 5.27, 5.40 – 5.42), Chapter 6 (paragraphs 6.25, 6.68), Chapter 10 (paragraph 10.56), Chapter 11 (paragraph 11.31) and the OAIC’s separate guidance for affiliates.²²
- B.22 An affiliate may have more than one sponsor at any time.

¹⁷ CDR Rules, rule 1.10D. The Note under this Rule states that ‘A person does not need to have sponsored accreditation to enter into a sponsorship arrangement as an affiliate, but will need it to make consumer data requests to the sponsor for information held by the sponsor as an accredited data recipient.’

¹⁸ CDR Rules, subrule 5.1B(3).

¹⁹ CDR Rules, subrule 5.1B(4).

²⁰ CDR Rules, subrule 5.1B(5).

²¹ CDR Rules, subrule 7.6(3).

²² For more information on the privacy obligations of affiliates, see: <https://www.oaic.gov.au/consumer-data-right/guidance-and-advice/sponsored-accreditation-model-privacy-obligations-of-affiliates>.

Assurance report

- B.23 An assurance report for a person with unrestricted accreditation means a report made in accordance with ASAE 3150 or an approved standard, report or framework.
- B.24 An assurance report for a person with sponsored accreditation is an assessment of its capacity to comply with Schedule 2 (Steps for privacy safeguard 12 – security of CDR data held by accredited data recipients) of the CDR Rules that is made in accordance with any approved requirements.²³
- B.25 This report does not include information that must be provided in an attestation statement.
- B.26 Assurance reports are discussed in [Chapter 12 \(Security of CDR data and destruction or de-identification of redundant data\)](#).

Attestation statement

- B.27 An attestation statement for a person with unrestricted accreditation means the responsible party's statement on controls and system description, made in accordance with ASAE 3150.
- B.28 An attestation statement for a person with sponsored accreditation is a statement about its compliance with Schedule 2 of the CDR Rules that is made in accordance with any approved requirements.²⁴
- B.29 Attestation statements are discussed in Chapter 12 of the privacy safeguard guidelines which relate to the security of CDR data.

Australian Privacy Principles, APPs

- B.30 The Australian Privacy Principles (APPs) are set out in Schedule 1 of the *Privacy Act 1988* (Cth) (Privacy Act). There are 13 APPs and they set out standards, rights and obligations in relation to a regulated entity's handling, holding, accessing and correcting of personal information.
- B.31 For information about which APPs apply to CDR entities in the CDR context, see Chapter A.

Authorise, Authorisation

- B.32 An authorisation is sought from or provided by a CDR consumer. It must meet the requirements set out in the CDR Rules, and be sought in accordance with the data standards.²⁵
- B.33 Data holders must ask the consumer to authorise the disclosure of their CDR data to an accredited person before disclosing CDR data to the relevant accredited person.²⁶

²³ See CDR Rules, subclause 2.1(1) of Schedule 1. For example, the Rules list the [CDR Accreditation Guidelines](#).

²⁴ See CDR Rules, subclause 2.1(1) of Schedule 1.

²⁵ CDR Rules, rule 4.5. See Division 4.4 of the CDR Rules for the requirements for asking a consumer to give or amend an authorisation.

²⁶ For SR (shared responsibility) data covered by a SR data request, the obligation to ask for authorisation applies to the primary data holder as if it were the data holder for the SR data: CDR Rules, subrule 1.23(3).

- B.34 For requests that relate to joint accounts, in some cases, the data holder might need to seek an ‘approval’ from the other joint account holder/s in addition to the authorisation provided by the requesting joint account holder.²⁷ Joint accounts are discussed further at paragraph B.193.
- B.35 For further information, see the [Guide to privacy for data holders](#). See also the example under paragraph B.3 to understand at which point a data holder must seek authorisation from the consumer to disclose CDR data.

CDR data

- B.36 ‘CDR data’ is information that is:
- within a class of information specified in the designation instrument for each sector;²⁸ or
 - derived from the above information (‘derived CDR data’).²⁹

Derived CDR data

- B.37 ‘Derived CDR data’ is data that has been wholly or partly derived from CDR data, or data derived from previously derived data (‘indirectly derived’ data).³⁰ This means data derived from ‘derived CDR data’ is also ‘derived CDR data’.
- B.38 ‘Derived’ takes its ordinary meaning. This is because ‘derived’ is not defined in the Competition and Consumer Act or the Privacy Act.

SR or shared responsibility data

- B.39 CDR data for which there is a CDR consumer may be specified as SR (shared responsibility) data where it is held by one data holder (the secondary data holder), but it would be more practical for consumer data requests for the data to be directed to a different data holder (the primary data holder).³¹
- B.40 Under current arrangements, only the energy sector has SR data (and by extension, primary and secondary data holders). For further information on data holders, see paragraphs B.162 to B.163. The meaning of SR data for the energy sector is set out in the Schedule 4 to the CDR Rules. In the energy sector, the Australian Energy Market Operator Limited (AEMO) is the secondary data holder,³² and SR data means AEMO data in relation to a CDR consumer.³³ AEMO data is NMI (national metering identifier) standing data, metering data and DER

²⁷ Depending on which ‘disclosure option’ (i.e. pre-approval or co-approval option) applies to the joint account: CDR Rules, rule 4A.5. Joint account holders can manage ‘disclosure options through the disclosure option management service: CDR Rules, rule 4A.6. See Subdivision 4A.3.2 of the CDR Rules, which sets out how consumer data requests to data holders that relate to joint accounts are handled in the CDR system.

²⁸ Competition and Consumer Act, subsection 56AI(1). For further information on designation instruments, see paragraphs B.180 to B.182.

²⁹ Competition and Consumer Act, subsection 56AI(1). For information on ‘materially enhanced information’ as derived CDR data, see paragraph B.276.

³⁰ Competition and Consumer Act, subsection 56AI(2).

³¹ Explanatory Statement, Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2021, page 5.

³² See CDR Rules, clause 4.3 of Schedule 4.

³³ See CDR Rules, clause 4.3 of Schedule 4. See definition of AEMO data at CDR Rules, clause 1.2 of Schedule 4.

(distributed energy resource) register data that relates to a relevant arrangement with the retailer.³⁴ The primary data holder for this data is the energy retailer, who has a direct relationship with the consumer.³⁵ The outcome of this is that consumer data requests involving AEMO data are to be directed to the retailer, rather than to AEMO.³⁶

B.41 For further guidance on primary and secondary data holders, see paragraphs B.164 to B.166.

CDR insight

B.42 A ‘CDR insight’ is an insight based on a consumer’s CDR data, which is subject to an insight disclosure consent.³⁷

B.43 CDR insights are CDR data.³⁸ The CDR insights model is intended to allow accredited data recipients³⁹ to disclose CDR data outside the CDR system to either confirm, deny, or provide simple information to a person selected by the CDR consumer, where this is for a limited, permitted purpose. ‘Insight disclosure consent’ is defined at B.85.

CDR participant

B.44 A ‘CDR participant’ is a data holder, or an accredited data recipient, of CDR data.⁴⁰

CDR policy

B.45 A ‘CDR policy’ is a document that provides information to consumers about how a CDR entity manages CDR data and how CDR consumers can make an inquiry or a complaint. The policy must be developed and maintained by entities in accordance with Privacy Safeguard 1 and CDR Rule 7.2.

B.46 The CDR policy must be a separate document to any of the entity’s privacy policies. For further information on the suggested process for developing a CDR policy and the minimum requirements for what must be included, see [Chapter 1 \(Privacy Safeguard 1\)](#) and the [Guide to developing a CDR policy](#).

³⁴ See CDR Rules, clause 1.2 of Schedule 4. The CDR Rules define NMI standing data, metering data and DER register data with reference to the definitions in the National Electricity Rules: see CDR Rules, clauses 1.2 and 1.3 of Schedule 4.

³⁵ See CDR Rules, clause 4.3 of Schedule 4 and Explanatory Statement, Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2021, page 20.

³⁶ CDR Rules, subrules 1.22(2) and 1.23(2).

³⁷ CDR Rules, rule 1.7.

³⁸ See CDR Rules, rules 1.7 and 1.10A(3).

³⁹ CDR representatives can also disclose CDR insights with the consumer’s consent.

⁴⁰ Competition and Consumer Act, subsection 56AL(1).

CDR receipt

- B.47 A 'CDR receipt' is a notice given by an accredited person⁴¹ to a CDR consumer who has provided, amended or withdrawn a consent.⁴²
- B.48 CDR receipts must be given in accordance with CDR Rule 4.18.

CDR representative principal

- B.49 A CDR representative principal is a person with unrestricted accreditation who has entered a written contract (a 'CDR representative arrangement'), with an unaccredited person (a 'CDR representative'). The CDR representative arrangement must meet the requirements in the CDR Rules (as discussed under 'CDR representative arrangement' below).⁴³
- B.50 Under a CDR representative arrangement, a CDR representative principal collects CDR data on behalf of their CDR representative and discloses it to the CDR representative (in accordance with a consumer's collection consent), so the CDR representative may provide goods or services to consumers by using or disclosing that data.
- B.51 While the CDR representative has the consumer-facing relationship, the CDR representative principal retains obligations in relation to the consumer for a range of matters, including providing the dashboard and notifications. Some of these obligations may be delegated to the CDR representative.
- B.52 The CDR representative principal is liable for the actions of their CDR representative, including breaches of the privacy safeguards.⁴⁴ In addition, a CDR representative principal must ensure that the CDR representative complies with the requirements of the CDR representative arrangement,⁴⁵ and the CDR representative principal is liable if the CDR representative:
- breaches any of the CDR representative arrangement provisions required by CDR subrules 1.10AA(1), (3) or (4)
 - engages in conduct referred to in subrule 1.10AA(2) where the CDR representative arrangement does not provide for the CDR representative to engage in that conduct.⁴⁶
- B.53 The CDR Rules contain some specific obligations for CDR representative principals, particularly in relation to the CDR representative arrangement, consent, notification,

⁴¹ Where the accredited person who is required to give a CDR receipt is a CDR representative principal, the receipt may be given through the CDR representative – CDR Rules, paragraph 4.3C(1)(l).

⁴² CDR Rules, subrule 4.18(1).

⁴³ CDR Rules, rule 1.10AA. These requirements are discussed in paragraphs B.58, B.61 - B.66.

⁴⁴ See CDR Rules, rules 1.16A(3) and (4) (Giving and amending consents), 7.3(2) (Rules relating to PS2 – anonymity and pseudonymity), 7.3A (Rule relating to PS4 – destruction of unsolicited data), 7.6(4) (Use or disclosure of CDR data), 7.8A (Rules relating to PSs 8 and 9), 7.9(5) (Rule relating to PS10 – notifying of the disclosure of CDR data), 7.10A (Rule relating to PS 11 – quality of data), 7.11(3) (Rule relating to PS 12 – security of CDR data), 7.12(3) (Rule relating to PS 12 – de-identification of redundant data) and 7.16 (Rule relating to PS 13 – correction of data).

⁴⁵ CDR Rules, subrule 1.16A(1).

⁴⁶ CDR Rules, subrules 1.16A(2) and (5). CDR Rules, subrule 1.10AA(2) states a CDR representative arrangement may provide for a CDR representative to seek any use or disclosure consent that the CDR representative principal could seek in the same circumstances, or to make certain permitted uses or disclosures referred to in rule 7.5.

dashboards and the CDR representative principal's CDR policy. For more information, see Chapter C (paragraphs C.9 – C.11, C.15, C.17 – C.19, C.22 – C.29, C.32, C.53, C.58-C.59, C.74, C.85, C.91, C.94 - C.97, C.101, C.106, C.108, diagram after C.115), Chapter 1 (paragraphs 1.8 – 1.9, 1.12, 1.21, 1.45, 1.55, 1.61), Chapter 2 (paragraph 2.6), Chapter 3 (paragraphs 3.2, 3.16 – 3.17, 3.23 – 3.24, 3.33, diagram after 3.41), Chapter 4 (paragraph 4.9 – 4.10), Chapter 5 (paragraphs 5.10, 5.16), Chapter 6 (paragraphs 6.8, 6.25, 6.27, 6.65, 6.71 – 6.72), Chapter 7 (paragraphs 7.9, 7.21, 7.42 – 7.43), Chapter 8 (paragraph 8.8 – 8.9, 8.45), Chapter 9 (paragraph 9.7 – 9.8), Chapter 10 (paragraph 10.8), Chapter 11 (paragraphs 11.11, 11.31), Chapter 12 (paragraphs 12.10, 12.41, 12.43, 12.58 – 12.61, 12.125 – 12.129), Chapter 13 (paragraph 13.12), and the OAIC's separate guidance for CDR representative principals.⁴⁷

CDR representative

- B.54 A CDR representative is an unaccredited person who has entered a written contract (a 'CDR representative arrangement') with a CDR representative principal. The CDR Rules outline the requirements for these arrangements (as discussed under 'CDR representative arrangement' below).⁴⁸ The CDR representative principal must be accredited at the unrestricted level.
- B.55 The CDR representative principal collects CDR data on behalf of the CDR representative. The CDR representative collects the CDR data from their CDR representative principal, and uses or discloses that CDR data to provide goods or services directly to the consumer (but not in their capacity as CDR business consumers).⁴⁹
- B.56 A CDR representative may collect CDR data only from their CDR representative principal. They are not permitted under the CDR Rules to collect CDR data from data holders or other accredited data recipients.
- B.57 As an unaccredited entity, a CDR representative is not directly bound by the privacy safeguards. However, under their CDR representative arrangement, they have contractual obligations to comply with Privacy Safeguards 2, 4, 6, 7, 8, 9, 11, 12 and 13.⁵⁰ They must also comply with the other terms of the CDR representative arrangement.⁵¹ As outlined in paragraph B.52 above, the CDR representative principal is liable for the actions of their CDR representative. A CDR representative's contractual obligations apply in addition to other privacy obligations they have under the Privacy Act if they are an APP entity. While they are not directly bound by the privacy safeguards, the following paragraphs are of particular relevance to CDR representatives: Chapter C (paragraphs C.9 – C.11, C.15, C.17 – C.19, C.22 – C.29, C.32, C.49 – C.51, C.54, C.58 – C.62, C.65 – C.69, C.74, C.85, C.91, C.94 - C.97, C.101, C.106, C.108, diagram after C.115), Chapter 1 (paragraphs 1.8, 1.12, 1.61), Chapter 2 (paragraph 2.6), Chapter 3 (paragraphs 3.2, 3.16 – 3.17, 3.23 – 3.24, 3.28, 3.33, diagram after 3.41), Chapter 4 (paragraph 4.9), Chapter 5 (paragraphs 5.10, 5.16), Chapter 6 (paragraphs 6.8, 6.25, 6.27, 6.71 – 6.72), Chapter 7 (paragraph 7.9, 7.42 – 7.43), Chapter 8 (paragraph 8.8), Chapter 9

⁴⁷ See <https://www.oaic.gov.au/consumer-data-right/guidance-and-advice/CDR-representative-model-Privacy-obligations-of-CDR-principals>.

⁴⁸ CDR Rules, subrules 1.10AA(1), (3) and (4). These requirements are discussed in paragraphs B.58, B.61 - B.66.

⁴⁹ CDR Rules, paragraphs 1.10AA(1)(a) and (b).

⁵⁰ CDR Rules, paragraphs 1.10AA(4)(a) and (g).

⁵¹ For more information on the privacy obligations of CDR representatives, see: <https://www.oaic.gov.au/consumer-data-right/guidance-and-advice/cdr-representative-model-privacy-obligations-of-cdr-representatives>.

(paragraph 9.7), Chapter 10 (paragraph 10.8), Chapter 11 (paragraph 11.11), Chapter 12 (paragraph 12.10), Chapter 13 (paragraphs 13.12).

- B.58 A CDR representative can only have one CDR representative principal.⁵²
- B.59 A CDR representative cannot engage an outsourced service provider (OSP) for the collection of CDR data, but may otherwise engage OSPs as provided in their CDR representative arrangement.⁵³

CDR representative arrangement

- B.60 A CDR representative arrangement is a written contract between a CDR representative (an unaccredited person) and their CDR representative principal. The CDR Rules outline requirements for these arrangements in CDR Rules, rule 1.10AA.
- B.61 Under the arrangement:
- the CDR representative principal will make consumer data requests on behalf of the CDR representative (where the consumer has given the representative a collection and use consent), and disclose the relevant CDR data to the CDR representative
 - the CDR representative will use or disclose the CDR data to provide the relevant goods or services to CDR consumers (but not in their capacity as CDR business consumers).⁵⁴
- B.62 A person intending to be a CDR representative must not seek consent from a consumer, or collect, use, disclose or otherwise handle CDR data unless they have a CDR representative arrangement in place with their CDR representative principal, and their details have been entered onto the Register of Accredited Persons.⁵⁵
- B.63 The purpose of a CDR representative arrangement is to regulate the CDR representative's handling of 'service data', being CDR data that was collected by the CDR representative principal on the CDR representative's behalf (and subsequently disclosed by the CDR representative principal to the CDR representative), and any information directly or indirectly derived from such CDR data.⁵⁶
- B.64 A CDR representative arrangement requires a CDR representative to comply with the following privacy safeguards in relation to service data as if they were the CDR representative principal:⁵⁷
- [Privacy Safeguard 2](#) (giving the CDR consumer the option of using a pseudonym, or not identifying themselves)
 - [Privacy Safeguard 4](#) (destroying unsolicited CDR data)
 - Privacy Safeguard 6 (use or disclosure of CDR data)

⁵² CDR Rules, paragraph 1.10AA(3)(a).

⁵³ CDR Rules, paragraph 1.10AA(3)(b).

⁵⁴ CDR Rules, paragraphs 1.10AA(1)(a) and (b). See also [Chapter C \(Consent — The basis for collecting and using CDR data\)](#) for more information about obtaining consent from a CDR consumer under a CDR representative arrangement.

⁵⁵ CDR Rules, paragraph 1.10AA(1)(c).

⁵⁶ CDR Rules, subrule 1.10AA(5).

⁵⁷ CDR Rules, paragraph 1.10AA(4)(a).

- Privacy Safeguard 7 (use or disclosure of CDR data for direct marketing)
- [Privacy Safeguard 11](#) (ensuring the quality of CDR data), other than subsection (1)⁵⁸
- [Privacy Safeguard 12](#) (security of CDR data and destruction or de-identification of redundant CDR data), and
- [Privacy Safeguard 13](#) (correction of CDR data), other than subsection (1).⁵⁹

B.65 Further, a CDR representative arrangement requires a CDR representative to comply with the following privacy safeguards as if they were an accredited data recipient:

- [Privacy Safeguard 8](#) (overseas disclosure of CDR data)
- [Privacy Safeguard 9](#) (adoption or disclosure of government-related identifiers).⁶⁰

B.66 In addition, CDR representatives have further obligations under a CDR representative arrangement, including requirements to:

- adopt and comply with the CDR representative principal's CDR policy in relation to service data⁶¹
- take the steps in Schedule 2 to the CDR Rules to protect the service data as if it were the CDR representative principal⁶²
- not use or disclose the service data other than in accordance with the CDR representative arrangement with the CDR representative principal⁶³
- not use or disclose the service data unless the use or disclosure would be permitted under specified paragraphs in CDR Rule 7.5⁶⁴
- when directed by the CDR representative principal, delete any service data that it holds in accordance with the CDR data deletion process, provide to the principal records of any deletion that are required to be made under the CDR data deletion process and require any of their direct or indirect outsourced service providers (OSPs) to do the same.⁶⁵

CDR system

B.67 The 'CDR system' was enacted by the *Treasury Laws Amendment (Consumer Data Right) Act 2019* to insert a new Part IVD into the *Competition and Consumer Act 2010* (Competition and Consumer Act).

B.68 The CDR system includes the CDR Rules, privacy safeguards, data standards, designation instruments, and any regulations made in respect of the provisions in the Competition and Consumer Act.

⁵⁸ Competition and Consumer Act, subsection 56EN(1).

⁵⁹ Competition and Consumer Act, subsection 56EP(1).

⁶⁰ CDR Rules, subrule 1.10AA(4)(g).

⁶¹ CDR Rules, paragraph 1.10AA(4)(f). See [Chapter 1 \(Privacy Safeguard 1 – Open and transparent management of CDR data\)](#) of these guidelines for more information on CDR policies.

⁶² CDR Rules, paragraph 1.10AA(4)(b).

⁶³ CDR Rules, paragraph 1.10AA(4)(c).

⁶⁴ CDR Rules, paragraph 1.10AA(4)(d).

⁶⁵ CDR Rules, paragraph 1.10AA(4)(e).

Collect

- B.69 'Collect' is not defined in the Competition and Consumer Act or the Privacy Act.
- B.70 Under the CDR system 'collect' has its ordinary, broad meaning (as it does under the Privacy Act). The concept of 'collection' applies broadly, and includes gathering, acquiring or obtaining CDR data by any means including from individuals and other entities.
- B.71 Subsection 4(1) of the Competition and Consumer Act, provides that a person 'collects' information only if the person collects the information for inclusion in:
- a record (within the meaning of the Privacy Act), or
 - a generally available publication (within the meaning of the Privacy Act).⁶⁶

Consent

- B.72 Consent is the:
- only basis on which an accredited person may collect CDR data through the CDR,⁶⁷ and
 - primary basis on which an accredited data recipient of particular CDR data, or a CDR representative, may use and disclose CDR data.⁶⁸
- B.73 Consent means a collection consent, a use consent or a disclosure consent (including a consent that has been amended by a consumer under the CDR Rules).⁶⁹ The CDR system sets out specific categories of consents that may be sought from a CDR consumer.⁷⁰ These are set out in CDR Rule 1.10A and outlined below in paragraphs B.76 to B.89.
- B.74 Consent must meet the requirements set out in the CDR Rules.⁷¹
- B.75 For further information, including the requirements which must be complied with when asking a CDR consumer to give or amend a consent, see [Chapter C \(Consent\)](#).

⁶⁶ 'Record' is defined in subsection 6(1) of the Privacy Act to include a document or an electronic or other device, with certain exclusions. 'Generally available publication' is defined in subsection 6(1) of the Privacy Act to include certain publications that are, or will be, generally available to members of the public whether or not published in print, electronically or any other form and whether or not available on the payment of a fee.

⁶⁷ See [Chapter 3 \(Privacy Safeguard 3\)](#) for information on seeking to collect CDR data.

⁶⁸ See [Chapter 6 \(Privacy Safeguard 6\)](#), [Chapter 7 \(Privacy Safeguard 7\)](#), [Chapter 8 \(Privacy Safeguard 8\)](#) and [Chapter 9 \(Privacy Safeguard 9\)](#) for information regarding use or disclosure of CDR data.

⁶⁹ CDR Rules, rule 1.7.

⁷⁰ An accredited person or CDR representative cannot ask for a consent that is not in a category of consents - CDR Rules, paragraphs 4.12(3)(a) and 4.20F(3)(a).

⁷¹ The requirements that an accredited person must comply with when asking for consent are contained in Division 4.3 of the CDR Rules (while those relating to CDR representatives seeking consent are in Division 4.3A). The specific requirements differ depending on which type of consent is being sought.

Collection consent

- B.76 A collection consent is a consent given by a CDR consumer for an accredited person to collect particular CDR data from a data holder or, accredited data recipient of that CDR data.⁷²

Use consent

- B.77 A use consent is a consent given by a CDR consumer for an accredited data recipient of particular CDR data, or a CDR representative that holds the CDR data as service data, to use that CDR data in a particular way, for example to provide goods or services requested by the consumer.⁷³
- B.78 Types of use consents include a direct marketing consent for an accredited data recipient to use CDR data for the purposes of direct marketing, and a de-identification consent (as outlined in paragraphs B.80 to B.82 and B.88 to B.89 below).

AP disclosure consent

- B.79 An AP disclosure consent is a consent given by a consumer for an accredited data recipient of particular CDR data, or a CDR representative, to disclose that CDR data to an accredited person in response to a consumer data request.⁷⁴

Direct marketing consent

- B.80 A direct marketing consent is a consent given by a CDR consumer for an accredited data recipient of particular CDR data, or a CDR representative, to use or disclose CDR data for the purposes of direct marketing.⁷⁵
- B.81 A direct marketing consent for an accredited data recipient or CDR representative to use CDR data for the purposes of direct marketing is a form of ‘use consent’.
- B.82 A direct marketing consent for an accredited data recipient or CDR representative to disclose CDR data to an accredited person for the purposes of direct marketing is a form of ‘disclosure consent’.

⁷² CDR Rules, paragraphs 1.10A(1)(a) and 1.10A(2)(a). ‘Collection consent’ also includes consent given by a consumer to a CDR representative for a CDR representative principal to collect CDR data from a data holder or accredited data recipient and disclose it to the CDR representative – CDR Rules, subrule 1.10A(8).

⁷³ CDR Rules, rule 1.7 (‘consent’ definition), paragraphs 1.10A(1)(b) and 1.10A(2)(b), and paragraph 4.3A(2)(b).

⁷⁴ CDR Rules, paragraphs 1.10A(1)(c)(i) and 1.10A(2)(e). Disclosures under an AP disclosure consent have been permitted since 1 July 2021. See CDR Rules, paragraphs 1.10AA(1)(b) and subrule 1.10AA(2) in relation to CDR representatives.

⁷⁵ CDR Rules, paragraphs 1.10A(1)(d) and 1.10A(2)(c). See CDR Rules, paragraph 1.10AA(1)(b) and (2) in relation to CDR representatives.

TA disclosure consent

- B.83 A TA disclosure consent is a consent given by a CDR consumer for an accredited data recipient of particular CDR data, or a CDR representative, to disclose that CDR data to a trusted adviser⁷⁶ of the consumer.⁷⁷
- B.84 A TA disclosure consent is a form of ‘disclosure consent’.

Insight disclosure consent

- B.85 An insight disclosure consent is a consent given by a CDR consumer for an accredited data recipient, or a CDR representative, to disclose their CDR data to a specified person for one or more of the following purposes:
- verifying the consumer’s identity
 - verifying the consumer’s account balance, or
 - verifying the details of credits to, or debits from, the consumer’s accounts.⁷⁸
- B.86 Where the CDR data relates to more than one transaction, an insight disclosure consent does not authorise the accredited data recipient or CDR representative to disclose the amount or date in relation to any individual transaction.⁷⁹
- B.87 An insight disclosure consent is a form of ‘disclosure consent’.

De-identification consent

- B.88 A de-identification consent⁸⁰ is a consent given by a CDR consumer for an accredited data recipient of particular CDR data, or a CDR representative, to de-identify some or all of that CDR data in accordance with the CDR data de-identification process⁸¹ and:
- use the de-identified data for ‘general research’ (see paragraph B.190), and/or
 - disclose (including by selling) the de-identified data.⁸²
- B.89 A de-identification consent is a form of ‘use consent’.

⁷⁶ See B.253 for more information on trusted advisers.

⁷⁷ CDR Rules, paragraphs 1.10A(1)(c)(iii) and 1.10A(2)(f). See CDR Rules, paragraph 1.10AA(1)(b) and (2) in relation to CDR representatives.

⁷⁸ CDR Rules, paragraphs 1.10A(1)(c)(iv), 1.10A(2)(g) and 1.10A(3)(a)(i)-(iii). See CDR Rules, paragraphs 1.10AA(1)(b) and (2) in relation to CDR representatives.

⁷⁹ CDR Rules, paragraph 1.10A(3)(b).

⁸⁰ CDR Rules, definition of consent under rule 1.7 and paragraphs 1.10A(1)(e) and 1.10A(2)(d).

⁸¹ See CDR Rules, rule 1.17 and [Chapter 12 \(Privacy Safeguard 12\)](#) for further information on the CDR data de-identification process. See CDR Rules, paragraph 1.10AA(1)(b) and (2) in relation to CDR representatives.

⁸² CDR Rules, paragraphs 1.10A(1)(e) and 1.10A(2)(d).

Business consumer disclosure consent

- B.90 A business consumer disclosure consent is a disclosure consent given by a CDR business consumer for an accredited data recipient to disclose their CDR data to a specified person. A business consumer disclosure consent must include a business consumer statement.⁸³
- B.91 A business consumer disclosure consent cannot be given to or sought by a CDR representative.⁸⁴
- B.92 An accredited person must not deal with a person in their capacity as a CDR business consumer until the earlier of 1 December 2023 or the day the Data Standards chair makes related data standards.⁸⁵

Business consumer statement

- B.93 A ‘business consumer statement’ is a statement made by a CDR business consumer, given in relation to certain consents, that certifies that the consent is given for the purpose of enabling the accredited person⁸⁶ to provide goods or services to the CDR business consumer in its capacity as a business (and not as an individual).⁸⁷
- B.94 The categories of consent in relation to which a business consumer statement can be given are use consents relating to the goods or services requested by the CDR business consumer, TA disclosure consents, insight disclosure consents and business consumer disclosure consents. Business consumer disclosure consents must include a business consumer statement.
- B.95 Making a business consumer statement allows a CDR business consumer to give a use, TA disclosure, insight disclosure or business consumer disclosure consent for a duration of up to 7 years.⁸⁸
- B.96 An accredited person must not deal with a person in their capacity as a CDR business consumer until the earlier of 1 December 2023 or the day the Data Standards chair makes related data standards.⁸⁹

Consumer, CDR consumer, ‘eligible’ CDR consumer and CDR business consumer

- B.97 The ‘CDR consumer’ is the person who has the right to:
- access the CDR data held by a data holder, and

⁸³ CDR Rules, subparagraph 1.10A(1)(c)(v), paragraph 1.10A(2)(h) and subrule 1.10A(11). ‘Business consumer statement’ is outlined at paragraph B.93.

⁸⁴ CDR Rules, subparagraph 1.10A(1)(c)(v) and paragraph 1.10AA(1)(a).

⁸⁵ CDR rules, 1.10A(14) and 7.5A(5).

⁸⁶ But not CDR representatives, as they are not permitted to deal with persons in their CDR business consumer capacity – CDR Rules, notes to rule 1.10AA and paragraph 1.10A(10)(b).

⁸⁷ CDR Rules, subrule 1.10A(10).

⁸⁸ CDR rules, subrule 4.12(1A), 4.14(2),

⁸⁹ CDR rules, 1.10A(14) and 7.5A(5).

- direct that the CDR data be disclosed to an accredited person.⁹⁰

B.98 A person is a ‘CDR consumer’ for CDR data if each of the following four conditions are met:⁹¹

- the CDR data ‘relates to’⁹² the person because of the supply of a good or service to the person or an associate⁹³ of the person⁹⁴
- the CDR data is held by another person who is:
 - a data holder of the CDR data
 - an accredited data recipient of the CDR data, or
 - holding⁹⁵ the data on behalf of a data holder or accredited data recipient of the CDR data⁹⁶
- the person is identifiable, or reasonably identifiable,⁹⁷ from the CDR data or other information held by the other person (the data holder, accredited data recipient, or person holding data on their behalf),⁹⁸ and
- none of the conditions (if any) prescribed by the regulations apply to the person in relation to the CDR data.⁹⁹

B.99 A CDR consumer can be an individual or a business enterprise.¹⁰⁰

B.100 Section 4B of the Competition and Consumer Act does not apply for the purposes of determining whether a person is a ‘CDR consumer’.¹⁰¹ This section explains when a person is taken to have acquired particular goods or services as a consumer, outside of the CDR system.

B.101 These guidelines use the term ‘consumer’ and ‘CDR consumer’ interchangeably.

Reasonably identifiable

B.102 As outlined in paragraph B.98, for a person to be a ‘CDR consumer’ that person must be identifiable, or ‘reasonably identifiable’, from the CDR data or other information held by the

⁹⁰ Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019, paragraph 1.100.

⁹¹ Competition and Consumer Act, subsection 56AI(3).

⁹² See paragraphs B.106 to B.112 for the meaning of ‘relates to’.

⁹³ See paragraphs B.113 to B.118 for the meaning of ‘associate’.

⁹⁴ Competition and Consumer Act, paragraph 56AI(3)(a). Note that paragraph 56AI(3)(a)(ii) allows for regulations to be made to prescribe circumstances in which CDR data may relate to a person.

⁹⁵ See paragraphs B.191 to B.192 for the meaning of ‘holds’.

⁹⁶ Competition and Consumer Act, subsection 56AI(3)(b).

⁹⁷ See paragraphs B.102 to B.105 for the meaning of ‘reasonably identifiable’.

⁹⁸ Competition and Consumer Act, paragraph 56AI(3)(c).

⁹⁹ At the time of publication, there are no conditions prescribed by the regulations.

¹⁰⁰ Competition and Consumer Act, subsection 56AI(3); Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019, paragraphs 1.100 and 1.101. See also section 2C of the *Acts Interpretation Act 1901* (Cth), which provides that in any Act (including the references to ‘person’ in subsection 56AI(3) of the Competition and Consumer Act), expressions used to denote persons generally include a body politic or corporate as well as an individual.

¹⁰¹ Competition and Consumer Act, subsection 56AI(4).

relevant entity (i.e. the data holder, accredited data recipient, or person holding data on their behalf).¹⁰²

B.103 For the purpose of determining whether a person is a ‘CDR consumer’ for CDR data, ‘reasonably identifiable’ is an objective test that has practical regard to the relevant context. This can include consideration of:

- the nature and amount of information
- other information held by the entity (see paragraphs B.191 to B.192 for a discussion on the meaning of ‘held’), and
- whether it is practicable to use that information to identify the person.

B.104 Where it is unclear whether a person is ‘reasonably identifiable’, an entity should err on the side of caution and act as though the person is ‘reasonably identifiable’ from the CDR data or other information held by the entity. In practice, this generally means treating the person as a ‘CDR consumer’ – the entity would need to handle CDR data which relates to the consumer in accordance with the privacy safeguards.

B.105 See paragraphs B.217 to B.220 for a discussion on the meaning of ‘reasonably’.

Relates to

B.106 As outlined in paragraph B.98, for a person to be a ‘CDR consumer’ the CDR data must ‘relate to’ that person.¹⁰³

B.107 In this context, the concept of ‘relates to’ is broad. It applies where there is some ‘association’ between the CDR data and the person which is ‘relevant’ or ‘appropriate’ depending on the statutory context.¹⁰⁴ The relevant context in the CDR system is the Competition and Consumer Act and the Privacy Act.

B.108 The Competition and Consumer Act states that the CDR data must ‘relate to’ the person because of the supply of a good or service to them or an associate of theirs, or because of circumstances of a kind prescribed by the CDR Rules.¹⁰⁵

B.109 CDR data will not ‘relate to’ a person unless the data itself is somehow relevant or appropriate for that person to use as a consumer under the CDR system.

B.110 An association between a person and certain CDR data will not be relevant or appropriate merely because, for instance, a sibling or other relative of the person has been supplied goods or services which the data concerns (see the discussion of ‘associate’ at B.106 to B.111 below).

B.111 Where information is primarily about a good or service but reveals information about a person’s use of that good or service, it ‘relates to’ the person.¹⁰⁶

¹⁰² Competition and Consumer Act, paragraph 56AI(3)(c).

¹⁰³ Competition and Consumer Act, paragraph 56AI(3)(a).

¹⁰⁴ *PMT Partners Pty Ltd (in liq) v Australian National Parks and Wildlife Service* (1995) 184 CLR 301, 331 (Toohey and Gummow JJ).

¹⁰⁵ Competition and Consumer Act, paragraph 56AI(3)(a).

¹⁰⁶ Explanatory Memorandum, *Treasury Laws Amendment (Consumer Data Right) Bill 2019*, section 1.108.

B.112 By using the broad phrase ‘relates to’, the CDR system captures meta-data.¹⁰⁷

Associate

B.113 As outlined in paragraph B.98, for a person to be a CDR consumer the CDR data must relate to that person because of the supply of a good or service to the person or one or more of that person’s ‘associates’.¹⁰⁸

B.114 This means a person can be a ‘CDR consumer’ for CDR data relevant to goods or services used by one of their associates, such as a partner, family member or related body corporate.¹⁰⁹

B.115 In this context, ‘associate’ has the same meaning as in the *Income Tax Assessment Act 1936* (ITA Act).¹¹⁰ Section 318 of the ITA Act defines ‘associates’ with respect to natural persons, companies, trustees and partnerships.¹¹¹

B.116 For natural persons, an associate includes:

- a relative
- a partner
- a trustee of a trust under which the person or another associate benefits, or
- certain companies able to be sufficiently influenced by the person or their associates.

B.117 The ITA Act offers further guidance on when a person is an ‘associate’ of a natural person, trustee of a trust or a company.

B.118 The ITA Act does not define ‘associate’ with respect to a government entity. This means that a government entity that is not a company cannot be a CDR consumer if the CDR data relates to the entity because of the supply of a good or service to one or more of the entity’s ‘associates’, because the entity does not have any ‘associates’ as defined in the ITA Act.

Eligible CDR consumer

B.119 While ‘CDR consumer’ is defined in the Competition and Consumer Act, only ‘eligible’ CDR consumers may make consumer data requests to access or transfer their CDR data under the CDR Rules.

B.120 A consumer is ‘eligible’ if, at that time all of the following are met:¹¹²

¹⁰⁷ This includes meta-data of the type found not to be ‘about’ an individual for the purpose of the Privacy Act in *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFA 4: Explanatory Memorandum, *Treasury Laws Amendment (Consumer Data Right) Bill 2019*, section 1.106.

¹⁰⁸ Competition and Consumer Act, paragraph 56AI(3)(a).

¹⁰⁹ Examples of this include where CDR data relates to a joint account or where a CDR consumer purchases goods or services used by a household.

¹¹⁰ Competition and Consumer Act, subsection 56AI(3).

¹¹¹ For the purposes of the CDR system, associates of partnerships are not directly relevant, as a partnership is not a ‘person’.

¹¹² CDR Rules, rule 1.10B.

- for any consumer – the consumer is an account holder or a secondary user¹¹³ for an account with the data holder that is open
- for a consumer that is an individual – the consumer is 18 years or older
- for a consumer that is a partner in a partnership for which there is partnership account¹¹⁴ with the data holder – the partnership account is open,¹¹⁵ and
- the additional criteria in the relevant sector schedule to the CDR Rules are met.¹¹⁶

B.121 Schedule 3 to the CDR Rules provides that banking consumers are only ‘eligible’ if the consumer’s account is set up in such a way that it can be accessed online, or where relevant, if the partnership account is set up in such a way that it can be accessed online (together, ‘online consumers’).¹¹⁷

B.122 Schedule 4 to the CDR Rules provides that energy consumers are only ‘eligible’ if the consumer is a customer of the retailer in relation to an eligible arrangement, the account relates to the arrangement, and certain consumption requirements are met.¹¹⁸ Unlike the banking sector, energy sector consumers will be eligible even if they do not have online access to their account with their energy retailer (‘offline consumers’). These Guidelines provide advice with respect to how particular rules should be applied in the context of both online and offline consumers.

B.123 For SR data, if a CDR consumer is eligible to make or initiate a consumer data request to a primary data holder, the CDR consumer is not eligible to make or initiate a consumer data request for that data to the secondary data holder.¹¹⁹ For further information on primary data holders, see paragraph B.165. For further information on SR data, see paragraphs B.39 to B.40.

B.124 For guidance regarding ‘consumers’ and ‘CDR consumers’, see paragraphs B.97 to B.101.

¹¹³ A person is a ‘secondary user’ for an account with a data holder if the person is an individual who is 18 years or older, the person has ‘account privileges’ in relation to the account, and the account holder has given the data holder an instruction to treat the person as a secondary user for the purposes of the CDR Rules: rule 1.7. ‘Account privileges’ is defined in the relevant sector schedule to the CDR Rules: see clause 2.2 of Schedule 3 (banking) and clause 2.2 of Schedule 4 (energy). For the staged application of the CDR Rules in relation to secondary users, see the relevant sector schedule to the CDR Rules. For general information on the staged application of CDR Rules, see paragraphs B.261 to B.263.

¹¹⁴ A ‘partnership account’ means an account with a data holder that is held by or on behalf of the partnership or the partners in a partnership: CDR Rules, rule 1.7.

¹¹⁵ For the staged application of the CDR Rules in relation to partnerships, see the relevant sector schedule to the CDR Rules. For general information on the staged application of CDR Rules, see paragraphs B.261 to B.263.

¹¹⁶ For the banking sector, see CDR Rules, clause 2.1 to Schedule 3. For the energy sector, see CDR Rules, clause 2.1 of Schedule 4.

¹¹⁷ See CDR Rules, clause 2.1 to Schedule 3.

¹¹⁸ See CDR Rules, subclause 2.1(1) of Schedule 4. An arrangement will be an ‘eligible arrangement’ if it relates to one or more connection points or child connection points for which there is a financially responsible market participant in the National Electricity Market: CDR Rules, subclause 2.1(2) of Schedule 4.

¹¹⁹ CDR Rules, rule 1.19.

CDR business consumer

B.125 A CDR consumer is taken to be a ‘CDR business consumer’ in relation to a consumer data request to be made by an accredited person if the accredited person has taken reasonable steps to confirm that either:

- the CDR consumer is not an individual, or
- the CDR consumer has an active ABN.¹²⁰

B.126 Only accredited persons can deal with a person in their capacity as a CDR business consumer. CDR representatives are not permitted to deal with CDR business consumers.¹²¹

Consumer dashboard, or dashboard

B.127 Each accredited person and each data holder must offer (and in most circumstances must provide) a ‘consumer dashboard’ for CDR consumers.¹²²

B.128 Where a CDR representative principal makes a consumer data request at the request of a CDR representative, it may arrange for a CDR representative to provide the consumer dashboard on its behalf.¹²³

B.129 An accredited person’s consumer dashboard is an online service that can be used by CDR consumers to manage consumer data requests and associated consents they have given to the accredited person or CDR representative (for example, to withdraw such consents). The service must also provide the CDR consumer with certain details of each consent. Each dashboard is visible only to the accredited person (or CDR representative where the CDR representative provides the dashboard) and the relevant CDR consumer.

B.130 The requirements for an accredited person’s consumer dashboard are set out in CDR Rule 1.14.¹²⁴ For more information, see [Chapter C \(Consent\)](#).

B.131 A data holder’s consumer dashboard is an online service that can be used by each CDR consumer to manage authorisations to disclose CDR data in response to consumer data requests (for example, to withdraw such authorisations). The service must also notify the CDR consumer of information related to CDR data disclosed pursuant to an authorisation.

B.132 A data holder must provide a consumer dashboard to a CDR consumer in the circumstances specified in the relevant sector schedule to the CDR Rules.¹²⁵ In the banking sector, a data holder must provide a consumer dashboard whenever it receives a consumer data request

¹²⁰ CDR Rules, rule 1.10A(9).

¹²¹ CDR Rules, note to subrule 1.10(10) and note to paragraph 1.10AA(1)(a).

¹²² Energy consumers may be eligible CDR consumers even if they do not have an online account with their retailer: see paragraph B.122. For eligible energy consumers without an online account, the retailer must offer the CDR consumer a dashboard and provide it if the CDR consumer accepts: CDR Rules, clause 2.3 of Schedule 4. For other CDR consumers, each accredited person and data holder must provide a consumer dashboard: CDR Rules, rules 1.14 and 1.15.

¹²³ CDR Rules, subrule 1.14(5).

¹²⁴ Additional requirements for updating dashboards in relation to collections and disclosures are set out in CDR Rules, rules 7.4 and 7.9.

¹²⁵ For the banking sector, see CDR Rules, clause 2.3 of Schedule 3. For the energy sector, see CDR Rules, clause 2.3 of Schedule 4.

from an accredited person on behalf of an eligible CDR consumer.¹²⁶ In the energy sector, an offline consumer may choose not to have a consumer dashboard provided by their energy retailer.¹²⁷ The requirements for a data holder's consumer dashboard are set out in CDR Rule 1.15.¹²⁸ For more information, see the [Guide to privacy for data holders](#).

B.133 If a consumer data request relates to a joint account where either the co-approval or pre-approval option applies, the data holder must provide each relevant account holder with a consumer dashboard.¹²⁹ Where this is the case, the dashboards must have the functionality set out in CDR Rule 4A.13, which includes:

- allowing relevant account holders to manage approvals in relation to authorisations
- allowing for the withdrawal of approvals.

B.134 These guidelines use the term 'dashboard' and 'consumer dashboard' interchangeably.

Consumer data request

B.135 A 'consumer data request' is a request made by an accredited person to a data holder,¹³⁰ accredited data recipient¹³¹ or CDR representative¹³² on behalf of a CDR consumer, in response to the consumer's valid request for the accredited person to seek to collect the consumer's CDR data.¹³³

B.136 A request from an accredited person to a data holder must be made through the data holder's accredited person request service¹³⁴

¹²⁶ CDR rules, clause 2.3 of Schedule 3.

¹²⁷ Energy retailers must offer offline CDR consumers a dashboard and provide it if the CDR consumer accepts: CDR Rules, clause 2.3 of Schedule 4. For further information on offline consumers in the energy sector, see paragraph B.122.

¹²⁸ If the request is a SR data request, the primary data holder must comply with CDR Rule 1.15 and provide a consumer dashboard as if it were the data holder for that data: CDR Rules, rule 1.21.

¹²⁹ CDR Rule, rules 4A.13. Where a co-approval option or pre-approval option applies to a joint account and consumer data request, the data holder must provide each account holder with a consumer dashboard. This includes the requirements set out in CDR Rules, rules 1.15 and 4A.13.

¹³⁰ CDR Rules, rule 4.4.

¹³¹ CDR Rules, rule 4.7A.

¹³² CDR Rules, rule 4.3B.

¹³³ The CDR Rules also make provision for consumer data requests to be made directly by a CDR consumer to a data holder: CDR Rules, Part 3. A request directly from a CDR consumer must be made using a data holder's 'direct request service': CDR Rules, subrule 3.3(1). A data holder's 'direct request service' is an online service, that must comply with the data standards, that allows eligible CDR consumers to make consumer data requests under Part 3 of the CDR Rules directly to the data holder in a timely and efficient manner and allows consumers to receive the requested data in human-readable form: CDR Rules, subrule 1.13(2). However:

- for the banking sector, there is currently no compliance date for a data holder's obligations under Part 3 of the CDR Rules: CDR Rules, clause 6.6 of Schedule 3.
- for the energy sector, Part 3 of the CDR Rules does not apply in relation to energy sector data: CDR Rules, clause 8.5 of Schedule 4.

¹³⁴ CDR Rules, subrule 4.4(3). There are no equivalent requirements under CDR Rule 4.7A or 4.3B for how an accredited person makes a consumer data request to an accredited data recipient or CDR representative.

B.137 A request from an accredited person to a data holder, accredited data recipient or CDR representative must comply with the data minimisation principle.¹³⁵

B.138 Refer to [Chapter 3 \(Privacy Safeguard 3\)](#) and [Chapter C \(Consent\)](#) for further information.

SR data request

B.139 An SR data request (or shared responsibility data request) is a consumer data request for a CDR consumer's CDR data where that data is or includes SR data.¹³⁶ Like other consumer data requests, SR data requests will be made by an accredited person on a consumer's behalf.¹³⁷ SR data requests must be made to the primary data holder for the CDR data.¹³⁸

B.140 For further information on primary and secondary data holders, see paragraphs B.165 to B.166. For further information on SR data, see paragraphs B.39 to B.40.

Accredited person request service

B.141 A data holder's 'accredited person request service' is an online service allowing accredited persons to make consumer data requests to the data holder on behalf of eligible CDR consumers.¹³⁹

B.142 It also allows accredited persons to receive requested data in machine-readable form.

B.143 This service must conform with the data standards.

B.144 If an accredited person proposes to make a SR data request on behalf of a CDR consumer, the accredited person must make the request using the primary data holder's direct request service.¹⁴⁰

Valid request

B.145 A 'valid' request is defined in the CDR Rules in Part 4 (Consumer data requests made by accredited persons).¹⁴¹

B.146 Under Part 4 of the CDR Rules, a request is 'valid' if:

¹³⁵CDR Rules, paragraphs 4.4(1)(d), 4.7A(1)(d) for requests to data holders and accredited data recipients respectively; subparagraph 4.7A(1)(d) as modified by rule 4.3B for requests to CDR representatives.

¹³⁶ CDR Rules, rule 1.7.

¹³⁷ The CDR Rules also make provision for SR data request to be made directly by a CDR consumer to a primary data holder using the primary data holder's 'direct request service': CDR Rules, subrule 1.22(2). Currently, the energy sector is the only CDR sector with SR data. Part 3 of the CDR Rules (Consumer data requests made by eligible CDR consumers) does not apply to energy sector data: CDR Rules, clause 8.5 of Schedule 4. This means that currently, no CDR consumers will be able to directly make an SR data request.

¹³⁸ CDR Rules, subrules 1.22(2) and 1.23(2).

¹³⁹ CDR Rules, subrule 1.13(3).

¹⁴⁰ CDR Rules, subrule 1.23(2).

¹⁴¹ It is also defined in Part 3 (Consumer data requests made by eligible CDR consumers). However, for the banking sector, there is currently no compliance date for a data holder's obligations under Part 3 of the CDR Rules: CDR Rules, clause 6.6 of Schedule 3. For the energy sector, Part 3 of the CDR Rules does not apply in relation to energy sector data: CDR Rules, clause 8.5 of Schedule 4.

- the CDR consumer has requested the accredited person to provide goods or services to themselves or another person and the accredited person needs to collect the CDR data and use it in order to provide those goods or services
- the accredited person has asked the CDR consumer to give their consent for the person to collect their CDR data from a CDR participant and use that CDR data in order to provide those goods or services, and
- the CDR consumer has given a collection consent and a use consent in response to the accredited person's request (and that consent has not been withdrawn).¹⁴²

B.147 Refer to [Chapter 3 \(Privacy Safeguard 3\)](#) for further information regarding valid requests, and [Chapter C \(Consent\)](#) for information regarding collection and use consents.

Competition and Consumer Regulations

B.148 The 'Competition and Consumer Regulations' refer to the *Competition and Consumer Regulations 2010*.

B.149 The Governor-General may make regulations prescribing matters required or permitted by the Competition and Consumer Act to be prescribed, or necessary or convenient to be prescribed for carrying out or giving effect to that Act.¹⁴³ This includes regulations that exempt a person or class of persons from CDR provisions in relation to particular CDR data or one or more classes of CDR data.¹⁴⁴ It also includes regulations that modify the operation of CDR obligations for a person or class of persons.¹⁴⁵

B.150 Currently, the Competition and Consumer Regulations exempt AEMO from certain privacy safeguard obligations, modify how the privacy safeguards apply to retailers in the energy sector, and modify certain provisions for parts of the banking sector.¹⁴⁶

CDR Rules

B.151 The consumer data rules (CDR Rules) refer to the Competition and Consumer (Consumer Data Right) Rules 2020.

B.152 The Minister has the power to make rules to determine how the CDR system functions in each sector.¹⁴⁷ CDR Rules may be made on aspects of the CDR system (as provided in Part IVD of the Competition and Consumer Act) including the privacy safeguards,¹⁴⁸ accreditation of

¹⁴² CDR Rules, rule 4.3.

¹⁴³ Competition and Consumer Act, subsection 172(1).

¹⁴⁴ Competition and Consumer Act, paragraphs 56GE(2)(a)-(b). See also Explanatory Statement, Competition and Consumer Amendment (Consumer Data Right) Regulations 2021, page 1.

¹⁴⁵ Competition and Consumer Act, paragraph 56GE(2)(c). See also Explanatory Statement, Competition and Consumer Amendment (Consumer Data Right) Regulations 2021, page 1.

¹⁴⁶ Competition and Consumer Regulations, Part 2BA.

¹⁴⁷ Competition and Consumer Act, subsection 56BA(1).

¹⁴⁸ Competition and Consumer Act, Part IVD, Division V.

data recipients and the disclosure, collection, use, accuracy, storage, security or deletion of CDR data for which there are one or more CDR consumers.¹⁴⁹

Current

Current consent

B.153 A consent is ‘current’ if it has not expired under CDR Rule 4.14.¹⁵⁰

B.154 CDR Rule 4.14 provides that a consent expires when one of the following occurs:

- if it is withdrawn, in accordance with CDR Rule 4.13(1)(a) or (b)
- at the end of the period the CDR consumer consented to, in accordance with CDR Rule 4.11
- 12 months have passed after consent was given or last amended, or 7 years for consents given by CDR business consumers that include a business consumer statement¹⁵¹
- for a collection consent:
 - when the accredited person is notified by the data holder of the withdrawal of authorisation¹⁵²
 - when the accredited person with a collection consent to collect CDR data from a particular accredited data recipient is notified by the accredited data recipient of the expiry of the AP disclosure consent to disclose that CDR data¹⁵³
- for an AP disclosure consent to disclose CDR data to a particular accredited person, when the accredited data recipient is notified by the accredited person of the expiry of the collection consent to collect that CDR data¹⁵⁴
- if the accredited person’s accreditation is revoked or surrendered, when this revocation or surrender takes effect¹⁵⁵
- upon an accredited person becoming a data holder of particular CDR data (in this situation, each of the accredited person’s consents that relate to the CDR data would expire),¹⁵⁶ or
- if another CDR Rule provides that consent expires.

B.155 For further information on when a consent expires, see [Chapter C \(Consent\)](#).

¹⁴⁹ Competition and Consumer Act, section 56BB.

¹⁵⁰ CDR Rules, subrule 1.7(1) (Definitions).

¹⁵¹ CDR Rules, paragraph 4.14(1)(c). However, note that an accredited person may not deal with a person in their capacity as a CDR business consumer until the earlier of 1 December 2023 or the day the Data Standards chair makes related data standards (see subrule 1.10A(14)).

¹⁵² CDR Rules, subrule 4.14(3).

¹⁵³ CDR Rules, subrule 4.14(4).

¹⁵⁴ Ibid.

¹⁵⁵ CDR Rules, subrule 4.14(6).

¹⁵⁶ CDR Rules, subrule 4.14(5).

Current authorisation

B.156 Authorisation to disclose particular CDR data to an accredited person is ‘current’ if it has not expired under CDR Rule 4.26.¹⁵⁷

B.157 CDR Rule 4.26 provides that authorisation expires when one of the following occurs:

- if it is withdrawn
- if the CDR consumer ceases to be eligible
- when the data holder is notified by the accredited person of the withdrawal of consent to collect the CDR data
- if the authorisation was for disclosure of CDR data over a specified period, at the end of that period or the period as last amended
- if the authorisation was for disclosure of CDR data on a single occasion, once the disclosure has occurred
- once 12 months have passed after authorisation was given
- if the accreditation of the accredited person to whom the data holder is authorised to disclose is revoked or surrendered, when the data holder is notified of that revocation or surrender, or
- if another CDR Rule provides that authorisation expires.¹⁵⁸

B.158 For further information on when an authorisation expires, see the [Guide to privacy for data holders](#).

Consumer Experience Guidelines

B.159 The Consumer Experience Guidelines set out guidelines for best practice design patterns to be used by entities seeking consent and/or authorisation from consumers under the CDR system.¹⁵⁹

B.160 The Consumer Experience Guidelines are made by the Data Standards Body and cover matters including:

- the process and decision points for a CDR consumer when consenting to share their data
- what (and how) information should be presented to CDR consumers to support informed decision making, and
- language that should be used (where appropriate) to ensure a consistent experience for CDR consumers across the broader CDR ecosystem.

B.161 The Consumer Experience Guidelines contain examples illustrating how a range of key CDR Rules can be implemented.

¹⁵⁷ CDR Rules, rule 1.7.

¹⁵⁸ See CDR Rules, subclause 7.2(3) of Schedule 3 and subclause 9.2(3) of Schedule 4.

¹⁵⁹ The Consumer Experience Guidelines are available at <https://cx.cds.gov.au/>. For more information on the Data Standards Body, see consumerdatastandards.gov.au.

Data holder

B.162 A person is a data holder of CDR data if:¹⁶⁰

- the CDR data falls within a class of information specified in the designation instrument for the relevant sector¹⁶¹
- the CDR data is held by (or on behalf of) the person on or after the earliest holding day¹⁶²
- the CDR data began to be held by (or on behalf of) the person before that earliest holding day, is of continuing use and relevance (e.g. a current account number),¹⁶³ and is not about the provision of a product or service by (or on behalf of) the person before the earliest holding day¹⁶⁴ (e.g. a transaction on an account)¹⁶⁵
- the person is not a designated gateway for the CDR data, and
- any of the three cases below apply:
 - **First case – person is also specified in the designation instrument:** the person is specified or belongs to a class of persons specified in a designation instrument and neither the CDR data, nor any other CDR data from which the CDR data was directly or indirectly derived, was disclosed to the person under the CDR Rules.¹⁶⁶
 - **Second case – reciprocity arising from the person being disclosed other CDR data under the CDR Rules:** neither the CDR data, nor any other CDR data from which the CDR data was directly or indirectly derived, was disclosed to the person under the CDR Rules, and the person is an accredited data recipient of other CDR data.¹⁶⁷
 - **Third case – conditions in the CDR Rules are met:** the CDR data or any other CDR data from which the CDR data was directly or indirectly derived was disclosed to the person under the CDR Rules, the person is an accredited person and the conditions specified in the CDR Rules are met.¹⁶⁸

¹⁶⁰ Competition and Consumer Act, section 56AJ.

¹⁶¹ For further information on designation instruments, which state the persons who are data holders in each sector, see paragraphs B.180 to B.182. See also Competition and Consumer Act, paragraph 56AC(2)(a).

¹⁶² Being the earliest holding date specified in the designation instrument for the relevant sector. The earliest holding day for each CDR sector is set out in the table at paragraph B.167.

¹⁶³ Explanatory Memorandum, Treasury Laws Amendment (2020 Measures No. 6) Bill 2020, [2.35].

¹⁶⁴ For a product or service that the person began providing before the earliest holding day and continued providing after that day, the person will:

- not be the data holder of CDR data about the person's provision of the product or service before that day, but
- be the data holder of CDR data about the person's provision of the product or service on or after the earliest holding day (provided all the other criteria in s 56AJ of the Competition and Consumer Act, as discussed at paragraphs B.162 are met by the entity): see Competition and Consumer Act, Note 2 to section 56AJ.

¹⁶⁵ Explanatory Memorandum, Treasury Laws Amendment (2020 Measures No. 6) Bill 2020, [2.35].

¹⁶⁶ For example, the person is an accredited data recipient of that CDR data or is an OSP to whom the CDR data was disclosed under CDR Rules, rule 1.10.

¹⁶⁷ Competition and Consumer Act, subsection 56AJ(3). This means that the person is an accredited person who is an accredited data recipient in respect of data other than the CDR data in question.

¹⁶⁸ The conditions for each sector are outlined in the sector specific schedule to the CDR Rules. For the banking sector, see CDR Rules, clause 7.2 of Schedule 3. For the energy sector, see CDR Rules, clause 9.2 of Schedule 4.

B.163 For further information on the privacy obligations for data holder, see the [Guide to privacy for data holders](#).

Primary and secondary data holders

B.164 In the current CDR system, only the energy sector has ‘primary’ and ‘secondary’ data holders. For the energy sector, ‘primary data holder’ and ‘secondary data holder’ are defined in Schedule 4 to the CDR Rules.¹⁶⁹ Primary and secondary data holders share responsibility for responding to requests for CDR data that is or includes SR data (SR data requests).¹⁷⁰ Data holders will only be ‘primary’ or ‘secondary’ data holders for SR data.

B.165 For the energy sector, the primary data holder is the retailer that has a direct relationship with the CDR consumer.¹⁷¹ Under the energy sector designation instrument, the retailer is not a specified data holder for the SR data identified in Schedule 4 to the CDR Rules.¹⁷² Despite this, from the point of view of the CDR consumer, the primary data holder is treated as if it were the data holder for the consumer’s SR data. This means a consumer or accredited person will make the SR data request to the primary data holder. The primary data holder will then seek the consumer’s authorisation to disclose SR data, will offer (and in most circumstances provide) the consumer dashboard, and will disclose (or refuse to disclose) the requested SR data.¹⁷³

B.166 For the energy sector, the secondary data holder is AEMO. The primary data holder must request relevant SR data from AEMO as secondary data holder where it needs this information to respond to the SR data request.¹⁷⁴ The secondary data holder is then authorised to disclose the CDR data directly to the primary data holder that has received the relevant consumer data request.¹⁷⁵ If the secondary data holder chooses not to disclose the requested SR data, it must notify the primary data holder of its refusal.¹⁷⁶ While AEMO is a data holder, in some cases it is treated differently to primary data holders in the energy sector. Certain chapters in these guidelines therefore specify that references to data holders do not include AEMO.¹⁷⁷

¹⁶⁹ CDR Rules, rule 1.7. See also CDR Rules, clause 4.3 of Schedule 4.

¹⁷⁰ For further information on SR data, see paragraphs B.39 to B.40.

¹⁷¹ CDR Rules, subclause 4.3(b) of Schedule 4 and Explanatory Statement, Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2021, page 3–6.

¹⁷² See Consumer Data Right (Energy Sector) Designation 2020, subsections 8(2) and 12(2); CDR Rules, clauses 4.3 and 1.2 of Schedule 4.

¹⁷³ See CDR Rules, subrules 1.22(2), 1.23(2), 1.21 and 1.22(6). See also Explanatory Statement, Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2021, pages 3–4.

¹⁷⁴ CDR Rules, subrule 1.22(5). The primary data holder will request this information when it has received a SR data request that includes information held by the secondary data holder, the consumer has authorised the disclosure of that data, and the primary data holder has not refused the SR data request under CDR Rules, rule 4.7: See CDR Rules, subrule 1.23(9) and Explanatory Statement, Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2021, page 4. The secondary data holder is required to have an online service to receive and respond to requests from primary data holders for CDR data it holds: CDR Rules, subrule 1.20(2).

¹⁷⁵ See Explanatory Statement, Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2021, page 3.

¹⁷⁶ CDR Rules, subrule 1.22(5).

¹⁷⁷ See [Chapter 1 \(Privacy Safeguard 1\)](#), [Chapter 10 \(Privacy Safeguard 10\)](#), [Chapter 11 \(Privacy Safeguard 11\)](#) and [Chapter 13 \(Privacy Safeguard 13\)](#).

Earliest holding day

B.167 A designation instrument must specify the ‘earliest holding day’ for a particular sector. This is the earliest day applicable to the sector for holding the designated information.¹⁷⁸ The earliest holding day for each designated CDR sector is outlined in the table below.

CDR sector ¹⁷⁹	Earliest holding day
Banking	1 January 2017 ¹⁸⁰
Energy	1 July 2018 ¹⁸¹
Non-bank Lending	1 January 2020 ¹⁸²

Data minimisation principle

B.168 The data minimisation principle limits the scope and amount of CDR data an accredited person may collect and use.

B.169 An accredited person collects CDR data in compliance with the data minimisation principle if, when making a consumer data request on behalf of a CDR consumer, the person does not seek to collect:

- more CDR data than is reasonably needed, or
- CDR data that relates to a longer time period than is reasonably needed

in order for it (or a relevant CDR representative) to provide the goods or services requested by the CDR consumer.¹⁸³

B.170 The use of CDR data by an accredited person or a CDR representative complies with the data minimisation principle if they do not use the collected data or derived data beyond what is reasonably needed in order to provide the requested goods or services or to fulfill any other purpose consented to by the CDR consumer.¹⁸⁴

¹⁷⁸ Competition and Consumer Act, paragraph 56AC(2)(c). Notwithstanding the earliest holding day, a person may be a data holder of CDR data that it held (or was held on its behalf) before the earliest holding day if the data is of continuing use and relevance, and is not about the provision of a product or service by (or on behalf of) the person before the earliest holding day: Competition and Consumer Act, paragraph 56AJ(1)(ba).

¹⁷⁹ A designation instrument has also been made in relation to telecommunications (Consumer Data Right (Telecommunications Sector) Designation 2022), and an earliest holding date of 1 January 2022. However, as at the date of publication of this document, there are no rules allowing for the sharing of designated telecommunications data pursuant to the CDR, and expansion to the telecommunications sector has been paused.

¹⁸⁰ Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019, subsection 5(3).

¹⁸¹ Consumer Data Right (Energy Sector) Designation 2020, subsection 6(3).

¹⁸² Consumer Data Right (Non-Bank Lenders) Designation 2022, subsection 6(3).

¹⁸³ CDR Rules, subrule 1.8(1).

¹⁸⁴ CDR Rules, subrule 1.8(2).

Data standards

B.171 A 'data standard' is a standard made by the Data Standards Chair of the Data Standards Body under section 56FA of the Competition and Consumer Act.

B.172 Data standards are about:

- the format and description of CDR data
- the disclosure of CDR data
- the collection, use, accuracy, storage, security and deletion of CDR data
- de-identifying CDR data, or
- other matters prescribed by regulations.¹⁸⁵

B.173 The current data standards are available on Consumer Data Standards website, consumerdatastandards.gov.au and include the following:

- API Standards
- Shared Responsibility Standards
- Information Security Standards
- Register Standards, and
- Consumer Experience Standards.

Consumer Experience Standards

B.174 The 'Consumer Experience Standards' are data standards¹⁸⁶ regarding:

- the obtaining of authorisations and consents and withdrawal of authorisations and consents
- the collection and use of CDR data, including requirements to be met by CDR participants in relation to seeking consent from CDR consumers.
- the authentication of CDR consumers, and
- the types of CDR data and descriptions of those types to be used by CDR participants in making and responding to requests ('Data Language Standards').

B.175 The Consumer Experience Standards are available on Consumer Data Standards website, consumerdatastandards.gov.au.

Data Language Standards

B.176 The 'Data Language Standards' are data standards¹⁸⁷ regarding the types of CDR data and descriptions of those types to be used by CDR participants in making and responding to requests.

¹⁸⁵ Competition and Consumer Act, section 56FA and CDR Rules, rule 8.11.

¹⁸⁶ Competition and Consumer Act, section 56FA and CDR Rules, rule 8.11.

¹⁸⁷ Competition and Consumer Act, section 56FA and CDR Rules, rule 8.11.

B.177 The Data Language Standards form part of the Consumer Experience Standards and are available on the Consumer Data Standards website, consumerdatastandards.gov.au.

Designated gateway

B.178 A ‘designated gateway’ is a person specified as a gateway in a legislative instrument made under subsection 56AC(2) of the Competition and Consumer Act, to whom CDR data is (or is to be) disclosed under the CDR Rules because of the reasons in paragraph 56AL(2)(c) of the Competition and Consumer Act.¹⁸⁸

B.179 There are currently no designated gateways in the banking sector or energy sector.¹⁸⁹ There are also no designated gateways in the non-bank lending sector, although unlike the banking and energy sectors, at the date of publication of these guidelines, there are no rules allowing for the sharing of designated non-bank lending data under the CDR system.^{190,191}

Designation instrument

B.180 A ‘designation instrument’ is a legislative instrument made by the Minister under subsection 56AC(2) of the Competition and Consumer Act.

B.181 A designation instrument designates a sector of the Australian economy for the purposes of the CDR system by specifying classes of information that can be shared under the CDR, among other things. A designation instrument has the effect of enlivening the ability to make rules allowing for the sharing of designated data pursuant to the CDR.¹⁹²

B.182 Existing CDR designation instruments are listed in the table below. The designation instrument for each CDR sector is also available on the [Federal Register of Legislation](#).

CDR sector	Designation Instrument
Banking	Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019
Energy	Consumer Data Right (Energy Sector) Designation 2020

¹⁸⁸ See section 56AL of the Competition and Consumer Act for the definition of ‘designated gateway’.

¹⁸⁹ For the banking sector, see the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019. For the energy sector, the energy designation specifies AEMO as a gateway for certain information: subsection 6(4) of the Consumer Data Right (Energy Sector) Designation 2020. However, at the time of publication, AEMO is not a designated gateway for any CDR data because under current CDR Rules, no CDR data is (or is to be) disclosed to AEMO because of the reasons in subsection 56AL(2)(c) of the Competition and Consumer Act.

¹⁹⁰ For further information on the effect of designation instruments, see paragraph B.181.

¹⁹¹ There are also no designated gateways in the designation instrument for the telecommunications sector; however, as at the date of publication of these guidelines, there are no rules allowing for the sharing of designated telecommunications data under the CDR system.

¹⁹² See Competition and Consumer Act, Division 2 of Part IVD.

Telecommunications	Consumer Data Right (Telecommunications Sector) Designation 2022 ¹⁹³
Non-bank lending	Consumer Data Right (Non-Bank Lenders) Designation 2022 ¹⁹⁴

Disclosure

B.183 ‘Disclosure’ is not defined in the Competition and Consumer Act or the Privacy Act.

B.184 Under the CDR system ‘disclose’ takes its ordinary, broad meaning.

B.185 An entity discloses CDR data when it makes the data accessible or visible to others outside the entity.¹⁹⁵ This interpretation focuses on the act done by the disclosing party, and not on the actions or knowledge of the recipient. Disclosure, in the context of the CDR system, can occur even where the data is already held by the recipient.¹⁹⁶

B.186 For example, an entity discloses CDR data when it transfers a copy of the data in machine-readable form to another entity.

B.187 Where an accredited data recipient engages a third party to perform services on its behalf, the provision of CDR data to that third party will in most circumstances be a disclosure (see paragraphs B.270 to B.273 for the limited circumstances where it will be a ‘use’).

B.188 ‘Disclosure’ is a separate concept from:

- ‘Unauthorised access’ which is addressed in [Chapter 12 \(Privacy Safeguard 12\)](#). An entity is not taken to have disclosed CDR data where a third party intentionally exploits the entity’s security measures and gains unauthorised access to the information. Examples include unauthorised access following a cyber-attack or a theft, including where the third party then makes that data available to others outside the entity.
- ‘Use’ which is discussed in paragraphs B.270 to B.273 below. ‘Use’ encompasses information handling and management activities occurring within an entity’s effective control, for example, when staff of an entity access, read, exchange or make decisions based on CDR data the entity holds.

Eligible

B.189 ‘Eligible’ CDR consumers are discussed at paragraphs B.119 to B.124.

¹⁹³ At the date of publication of these guidelines, there are no rules allowing for the sharing of designated telecommunications data under the CDR system, and expansion to the sector has been paused.

¹⁹⁴ At the date of publication of these guidelines, there are no rules allowing for the sharing of designated non-bank lending data under the CDR system.

¹⁹⁵ Information will be ‘disclosed’ under the CDR system regardless of whether an entity retains effective control over the data.

¹⁹⁶ For a similar approach to interpreting ‘disclosure’, see *Pratt Consolidated Holdings Pty Ltd v Commissioner of Taxation* [2011] AATA 907, [112]–[119].

General research

B.190 ‘General research’ is defined in CDR Rule 1.7 to mean research undertaken by an accredited data recipient with CDR data de-identified in accordance with the CDR Rules that does not relate to the provision of goods or services to any particular CDR consumer. An example is product or business development.¹⁹⁷

Holds

B.191 Subsection 4(1) of the Competition and Consumer Act provides that a person ‘holds’ information if they have possession or control of a record (within the meaning of the Privacy Act)¹⁹⁸ that contains the information.¹⁹⁹ This definition is comparable to the definition of ‘holds’ in the Privacy Act.²⁰⁰

B.192 The term ‘holds’ extends beyond physical possession of a record to include a record that a CDR entity has the right or power to deal with. Whether a CDR entity ‘holds’ a particular item of CDR data may therefore depend on the particular data collection, management and storage arrangements it has adopted. For example, a CDR entity ‘holds’ CDR data where:

- it physically possesses a record containing the CDR data and can access that data physically or by use of an electronic device (such as decryption software), or
- it has the right or power to deal with the CDR data, even if it does not physically possess or own the medium on which the CDR data is stored. For example, the entity has outsourced the storage of CDR data to a third party but it retains the right to deal with it, including to access and amend that data.

Joint account

B.193 A joint account is an account with a data holder for which there are 2 or more account holders. Each account holder must be:

- an individual
- so far as the data holder is aware, acting in their own capacity and not on behalf of another person, and
- an ‘eligible CDR consumer’.²⁰¹

A ‘partnership account’ is not a joint account.²⁰²

B.194 For the purposes of the CDR system, one of three disclosure options applies to a joint account.²⁰³

¹⁹⁷ Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020*, [21].

¹⁹⁸ ‘Record’ is defined in subsection 6(1) of the Privacy Act.

¹⁹⁹ Competition and Consumer Act, subsection 4(1).

²⁰⁰ Privacy Act, subsection 6(1).

²⁰¹ See paragraphs B.119 to B.124 for further information about ‘an eligible CDR consumer’.

²⁰² CDR Rules, subrule 1.7(1) (Definitions).

²⁰³ CDR Rules, rule 4A.5.

- **pre-approval option:** joint account data may be disclosed in response to a valid CDR consumer data request on the authorisation of the requester, without the approval of the relevant account holders. This option applies to a joint account by default.²⁰⁴
- **co-approval option:** joint account data may be disclosed in response to a valid CDR consumer data request only after the requester has authorised the disclosure, and each of the relevant joint account holders has approved the disclosure
- **non-disclosure option:** means that joint account data may not be disclosed even in response to a valid CDR consumer data request.

B.195 A data holder must provide the pre-approval and non-disclosure options, but may choose whether to make the co-approval option available.²⁰⁵

B.196 Part 4A of the CDR Rules sets out the rules that apply to CDR consumer data requests for the disclosure of CDR data that relates to a joint account.²⁰⁶

Outsourcing

B.197 The CDR Rules permit the use of ‘outsourced service providers’ (OSPs) by accredited persons, CDR representatives and other OSPs. A ‘CDR outsourcing arrangement’ meeting the requirements of CDR Rule 1.10 must be in place between the principal and each OSP.

OSPs, OSP principals and OSP chain principals

B.198 Where a person enters into a CDR outsourcing arrangement with an OSP, the person is the ‘OSP principal’ of the OSP, and the OSP is a ‘direct OSP’ of that person.

B.199 Where that OSP enters into a further CDR outsourcing arrangement with another OSP, the other OSP is an ‘indirect OSP’ of the first person. Any OSP subsequently engaged by that other OSP will also be an indirect OSP of the first person.

B.200 In a chain of OSPs, the accredited person or CDR representative who was the initial ‘OSP principal’ at the top of the chain is the ‘OSP chain principal’.²⁰⁷

B.201 For example, if A is an accredited person who engages B as an OSP under a CDR outsourcing arrangement, B engages C as an OSP under a further CDR outsourcing arrangement, and C engages D as an OSP under another further CDR outsourcing arrangement, then:

- A is the OSP chain principal for this set of arrangements
- A is the OSP principal of B, B is a direct OSP of A, and C and D are indirect OSPs of A
- B is the OSP principal of C, C is a direct OSP of B and D is an indirect OSP of B
- C is the OSP principal of D, D is a direct OSP of C.

²⁰⁴ CDR Rules, subrule 4A.5(5).

²⁰⁵ CDR Rules, subrules 4A.5(2) and (3).

²⁰⁶ For more information, see ‘Authorisation’ in [Chapter C \(Consent\)](#), and the OAIC’s [Guide to privacy for data holders](#).

²⁰⁷ CDR Rules, subrules 1.10(1) and (2).

Service Data

B.202 Service data, in relation to a person who is a direct or indirect OSP of an OSP chain principal, means any CDR data of a CDR consumer of the OSP chain principal held by the OSP that:

- was disclosed to the OSP by the OSP chain principal for the purposes of the relevant CDR outsourcing arrangement
- was collected from a CDR participant by the OSP on behalf of the OSP chain principal in accordance with the relevant CDR outsourcing arrangement
- was disclosed to the OSP by another direct or indirect OSP of the OSP chain principal in accordance with the relevant CDR outsourcing arrangement for the other direct or indirect OSP, or
- is directly or indirectly derived from such CDR data.²⁰⁸

CDR outsourcing arrangement

B.203 A CDR outsourcing arrangement is a written contract between an OSP principal and an OSP that meets the minimum requirements listed in CDR Rules, rule 1.10(3).

B.204 Under the arrangement, the OSP will:

- collect CDR data from a CDR participant on behalf of the OSP chain principal, and/or
- provide goods or service to the OSP principal by using or disclosing CDR data that it has collected on behalf of the principal or that has been disclosed to it by the principal.²⁰⁹

B.205 Where the OSP is providing goods or services, the provision of those goods or services must be:

- where the OSP principal is also the OSP chain principal, for the purposes of the OSP chain principal providing goods and services to a CDR consumer for the service data
- otherwise, for the purposes of enabling the OSP principal to provide the goods and services it must provide under its CDR outsourcing arrangement.²¹⁰

Content of CDR outsourcing arrangements

B.206 A CDR outsourcing arrangement must include the matters referred to in paragraphs B.207 - B.208. It must also address the nature of the services to be provided, as outlined in paragraph B.204. Together, these are known as 'required provisions'.²¹¹

B.207 A CDR outsourcing arrangement must require an OSP, when holding, using or disclosing service data, to comply with the following as if it were the OSP principal:²¹²

²⁰⁸ CDR Rules, subrule 1.10(6).

²⁰⁹ CDR Rules, paragraph 1.10(3)(a).

²¹⁰ CDR Rules, subrule 1.10(4).

²¹¹ CDR Rules, subrule 1.16(6).

²¹² CDR Rules, subrule 1.10(3)(b)(i)

- the OSP principal's CDR policy in relation to the deletion and de-identification of CDR data and the treatment of redundant or de-identified data
- Privacy Safeguard 4 (destroying unsolicited CDR data)
- Privacy Safeguard 6 (use or disclosure of CDR data)
- Privacy Safeguard 7 (use or disclosure of CDR data for direct marketing)
- Privacy Safeguard 8 (overseas disclosure of CDR data), and
- Privacy Safeguard 9 (adoption or disclosure of government-related identifiers).

B.208 In addition, a CDR outsourcing arrangement must include requirements for the OSP to:

- take the steps in Schedule 2 to protect service data as if it were an accredited data recipient
- not disclose service data other than:
 - to another direct or indirect OSP of the OSP chain principal
 - to the OSP chain principal
 - in circumstances where the disclosure of the service data by the OSP chain principal would be permitted under the rules
- not use or disclose service data other than in accordance with the CDR outsourcing arrangement
- if directed by the OSP principal or OSP chain principal:
 - provide the OSP principal or OSP chain principal with access to any service data that it holds
 - delete (in accordance with the CDR data deletion process) any service data that it holds and make the required records
 - provide the required records to the OSP principal or OSP chain principal
 - direct any other person to which it has disclosed the service data under a further CDR outsourcing arrangement to take corresponding steps
- if directed by the CDR representative principal of the OSP chain principal (where the OSP chain principal is a CDR representative):
 - delete (in accordance with the CDR data deletion process) any service data that it holds and make the required records
 - provide the required records to the OSP principal or OSP chain principal
 - direct any other person to which it has disclosed the service data under a further CDR outsourcing arrangement to take corresponding steps
- ensure its own direct OSPs comply with their respective CDR outsourcing arrangements, including in relation to service data disclosed to them by the OSP chain principal or another direct or indirect OSP of the OSP chain principal.

Compliance and liability

- B.209 An accredited person who is an OSP chain principal must ensure its direct and indirect OSPs comply with their requirements under their respective CDR outsourcing arrangements.²¹³
- B.210 Similarly, where a CDR representative principal permits a CDR representative to engage OSPs, the CDR representative principal must ensure the CDR representative's direct and indirect OSPs comply with their requirements under their respective CDR outsourcing arrangements.²¹⁴
- B.211 An accredited person is liable for any collection, use or disclosure of service data by its direct or indirect OSPs or the direct or indirect OSPs of its CDR representatives, whether or not the collection, use or disclosure was made in accordance with a relevant CDR outsourcing arrangement.²¹⁵

Limitations

- B.212 An affiliate must not engage an OSP to collect data on their behalf, but may engage a provider to provide goods or services using CDR data disclosed to it by the affiliate.²¹⁶
- B.213 A CDR representative must not engage an OSP to collect CDR data on its behalf, but may otherwise engage an OSP in accordance with their CDR representative arrangement.²¹⁷

Purpose

- B.214 A person is deemed to engage in conduct for a particular 'purpose' if they engage in the conduct for purposes which include that purpose, and where that purpose is a substantial purpose.²¹⁸
- B.215 The purpose of an act is the reason or object for which it is done.
- B.216 There may be multiple purposes. If one of those purposes is a substantial purpose, a person is deemed to engage in conduct for that particular purpose.²¹⁹ This means that:
- all substantial purposes for which a person holds CDR data are deemed to be a 'purpose' for which the person holds the data, and
 - if one purpose for a use of CDR data is direct marketing, and that purpose is a substantial purpose, the use is deemed to be for the purpose of direct marketing for the purposes of Privacy Safeguard 6.

²¹³ CDR Rules, subrules 1.16(1) and (2).

²¹⁴ CDR Rules, subrules 1.16(3) and (4).

²¹⁵ CDR Rules, rule 1.16 and subrules 7.6(2) and (5).

²¹⁶ CDR Rules, subrule 1.10(3)(a)(i) and 5.1B(4).

²¹⁷ CDR Rules, subrules 1.10(3)(a)(i) and 1.10AA(3)(b).

²¹⁸ Competition and Consumer Act, paragraph 4F(1)(b).

²¹⁹ Competition and Consumer Act, section 4F.

Reasonable, Reasonably

- B.217 ‘Reasonable’ and ‘reasonably’ are used in the privacy safeguards and CDR Rules to qualify a test or obligation. For example, for CDR data to have a ‘CDR consumer’, at least one person must be identifiable or ‘reasonably’ identifiable from the CDR data or other information held by the relevant entity.²²⁰
- B.218 ‘Reasonable’ and ‘reasonably’ are not defined in the Competition and Consumer Act or the Privacy Act. The terms bear their ordinary meaning, as being based upon or according to reason and capable of sound explanation.
- B.219 What is reasonable is a question of fact in each individual case. It is an objective test that has regard to how a reasonable person, who is properly informed, would be expected to act in the circumstances. What is reasonable can be influenced by current standards and practices.²²¹
- B.220 An entity must be able to justify its conduct as ‘reasonable’. The High Court has observed that whether there are ‘reasonable grounds’ to support a course of action ‘requires the existence of facts which are sufficient to [persuade] a reasonable person’,²²² and ‘involves an evaluation of the known facts, circumstances and considerations which may bear rationally upon the issue in question’.²²³ There may be a conflicting range of objective circumstances to be considered, and the factors in support of a conclusion should outweigh those against.

Reasonable steps

- B.221 References to ‘reasonable steps’ are used in the privacy safeguards and CDR Rules. Examples include:
- Privacy Safeguard 11, which includes a requirement for data holders and accredited data recipients to take reasonable steps to ensure the quality of disclosed CDR data.²²⁴
 - CDR Rule 1.10C, where a person is taken to be a trusted adviser if the accredited data recipient has taken reasonable steps to confirm that the person was, and remains, a member of a specified class²²⁵
 - CDR subrule 1.10A(9), where a CDR consumer is taken to be a CDR business consumer if the accredited person has taken reasonable steps to confirm that the CDR consumer is not an individual, or that the CDR consumer has an active ABN.²²⁶

²²⁰ Competition and Consumer Act, paragraph 56AI(3)(c).

²²¹ For example, *Jones v Bartlett* [2000] HCA 56, [57]–[58] (Gleeson CJ); *Bankstown Foundry Pty Ltd v Braistina* [1986] HCA 20, [12] (Mason, Wilson and Dawson JJ).

²²² *George v Rockett* (1990) 170 CLR 104, 112.

²²³ *McKinnon v Secretary, Department of Treasury* (2006) 228 CLR 423, 430 (Gleeson CJ & Kirby J).

²²⁴ See [Chapter 11 \(Privacy Safeguard 11\)](#) for information about the obligations under Privacy Safeguard 11 (section 56EN of the Competition and Consumer Act).

²²⁵ See [Chapter 6 \(Privacy Safeguard 6\)](#) for information about disclosures by accredited data recipients to trusted advisers.

²²⁶ Subrule 1.10A(9).

B.222 The ‘reasonable steps’ test is an objective test and is to be applied in the same manner as ‘reasonable’ and ‘reasonably’.

B.223 An entity must be able to justify that reasonable steps were taken.

Redundant data

B.224 CDR data is ‘redundant data’ if the data is collected by an accredited data recipient under the CDR system and the entity no longer needs any of the data for a purpose permitted under the CDR Rules or for a purpose for which the entity may use or disclose it under Division 5, Part IVD of the Competition and Consumer Act.²²⁷

B.225 For further information on redundant data, including how to meet the obligation under Privacy Safeguard 12 to delete or de-identify redundant data, see [Chapter 12 \(Privacy Safeguard 12\)](#).

Required consumer data

B.226 ‘Required consumer data’ for each CDR sector is defined in the relevant sector schedule to the CDR Rules.²²⁸

B.227 Required consumer data must be disclosed by a data holder in response to a consumer data request under CDR Rules, subrule 4.6(4) (subject to any exceptions under rules 4.6A or 4.7).

Required or authorised by an Australian law or by a court/tribunal order

B.228 A number of the privacy safeguards and CDR Rules provide an exception if a CDR entity is ‘required or authorised by or under an Australian law or a court/tribunal order’ to act differently. For example, Privacy Safeguard 6 which prohibits the use or disclosure of CDR data by an accredited data recipient unless, for example, the use or disclosure is required or authorised by or under another Australian law or a court/tribunal order.²²⁹

Australian law

B.229 ‘Australian law’ has the meaning given to it in the Privacy Act.²³⁰ It means:

- an Act of the Commonwealth, or of a State or Territory
- regulations or any other instrument made under such an Act

²²⁷ Competition and Consumer Act, subsection 56EO(2). Note that this section also applies to designated gateways. For information on designated gateways, see paragraphs B.178 to B.179.

²²⁸ For the banking sector, see CDR Rules, clause 3.2 of Schedule 3. For the energy sector, see CDR Rules, clause 3.2 of Schedule 4.

²²⁹ And the accredited data recipient makes a written note of the use or disclosure. Competition and Consumer Act, paragraph 56EI(1)(c). See [Chapter 6 \(Privacy Safeguard 6\)](#) for further information.

²³⁰ Competition and Consumer Act, subsection 4(1).

- any other law in force in the Jervis Bay Territory or an external Territory, or
- a rule of common law or equity.²³¹

Court/tribunal order

B.230 ‘Court/tribunal order’ has the meaning given to it in the Privacy Act. It means an order, direction or other instrument made by a court, a tribunal, a judge, a magistrate, a person acting as a judge or magistrate, a judge or magistrate acting in a personal capacity, or a member or an officer of a tribunal.²³²

B.231 The definition applies to orders and the like issued by Commonwealth, State and Territory courts, tribunals and members, and officers. The definition includes an order, direction or other instrument that is of an interim or interlocutory nature.

B.232 The reference to a judge or a magistrate acting in a personal capacity means that the definition applies to an order or direction issued by a judge or magistrate who has been appointed by government to an office or inquiry that involves the exercise of administrative or executive functions, including functions that are quasi-judicial in nature. An example is a judge who is appointed by Government to conduct a royal commission.

Required

B.233 A person who is ‘required’ by an Australian law or a court/tribunal order to handle data in a particular way has a legal obligation to do so and cannot choose to act differently.

B.234 The obligation will usually be indicated by words such as ‘must’ or ‘shall’ and may be accompanied by a sanction for non-compliance.

Authorised

B.235 A person who is ‘authorised’ under an Australian law or a court/tribunal order has discretion as to whether they will handle data in a particular way. The person is permitted to take the action but is not required to do so. The authorisation may be indicated by a word such as ‘may’ but may also be implied rather than expressed in the law or order.

B.236 A person may be impliedly authorised by law or order to handle data in a particular way where a law or order requires or authorises a function or activity, and this directly entails the data handling practice.

B.237 For example, a statute that requires a person to bring information to the attention of a government authority where they know or believe a serious offence has been committed²³³ may implicitly authorise a person to use CDR data to confirm whether or not the offence has been committed, and then may require the person to disclose the data to the authority.

B.238 An act or practice is not ‘authorised’ solely because there is no law or court/tribunal order prohibiting it. The purpose of the privacy safeguards is to protect the privacy of consumers

²³¹ Privacy Act, subsection 6(1).

²³² Privacy Act, subsection 6(1).

²³³ For example, subsection 316(1) of the *Crimes Act 1900* (NSW).

by imposing obligations on persons in their handling of CDR data. A law will not authorise an exception to those protections unless it does so by clear and direct language.²³⁴

Required or authorised to use or disclose CDR data under the CDR Rules

B.239 For data holders, certain regulatory provisions refer to situations where the data holder is or was ‘required or authorised’ to disclose the CDR data under the CDR Rules. For example, the requirement in Privacy Safeguard 13 to respond to a correction request applies where the data holder was ‘earlier required or authorised under the CDR Rules’ to disclose the CDR data.²³⁵

B.240 For accredited data recipients, certain regulatory provisions refer to situations where the accredited data recipient is ‘required or authorised’ under the CDR Rules to use or disclose CDR data. For example, Privacy Safeguard 6 provides that an accredited data recipient must not use or disclose CDR data unless, for example, the use or disclosure is required or authorised under the CDR Rules.²³⁶

Required

B.241 A data holder is ‘required’ to disclose required consumer data²³⁷ under the CDR Rules:

- in response to a valid consumer data request under CDR Rules subrule 3.4(3), subject to rule 3.5, and
- in response to a consumer data request from an accredited person on behalf of a CDR consumer under subrule 4.6(4) of the CDR Rules, subject to rules 4.6A and 4.7, where the data holder has a current authorisation to disclose the data from the CDR consumer.

B.242 A primary data holder will be ‘required’ to disclose any SR data covered by a SR data request under the CDR Rules as if the primary data holder were the data holder for that data.²³⁸

B.243 An accredited data recipient is never ‘required’ to use or disclose CDR data under the CDR Rules.

Authorised

B.244 A data holder may be ‘authorised’ to disclose a consumer’s CDR data to an accredited person by the relevant CDR consumer.²³⁹ Such an authorisation must be in accordance with Division 4.4 of the CDR Rules.

²³⁴ See *Coco v The Queen* (1994) 179 CLR 427.

²³⁵ Competition and Consumer Act, paragraph 56EP(1)(c). See [Chapter 13 \(Privacy Safeguard 13\)](#) for further information.

²³⁶ Competition and Consumer Act, paragraph 56EI(1)(b). See [Chapter 6 \(Privacy Safeguard 6\)](#) for further information.

²³⁷ See paragraphs B.226 to B.227 for further information about ‘required consumer data’.

²³⁸ CDR Rules, subrules 1.22(6) and 1.23(7).

²³⁹ CDR Rules, rule 4.5.

B.245 A secondary data holder will be ‘authorised’ to disclose the SR data that it holds to the primary data holder when requested.²⁴⁰

B.246 An accredited data recipient is ‘authorised’ to use or disclose CDR data under the CDR Rules in the circumstances outlined in CDR Rule 7.5. For information on the permitted uses or disclosures that do not relate to direct marketing, see [Chapter 6 \(Privacy Safeguard 6\)](#). For information on the permitted uses or disclosures that relate to direct marketing, see [Chapter 7 \(Privacy Safeguard 7\)](#).

Required product data

B.247 The privacy safeguards do not apply to required product data.²⁴¹

B.248 ‘Required product data’ for each CDR sector is defined in the relevant sector schedule to the CDR Rules.²⁴²

Service data

B.249 For information on the meaning of ‘service data’ in relation to a CDR outsourcing arrangement, see paragraph B.202 above.

B.250 For information on the meaning of ‘service data’ in relation to a CDR representative arrangement, see paragraph B.63 above.

Sponsor

B.251 A sponsor is a person with unrestricted accreditation who has entered into a written contract (‘a sponsorship arrangement’) with another person (known as the ‘affiliate’) that meets certain requirements.²⁴³

B.252 The role of the sponsor is to disclose CDR data to their affiliate so that the affiliate may use that data to provide goods or services directly to a CDR consumer. The sponsor may also collect CDR data on behalf of their affiliate, and use or disclose CDR data at the request of their affiliate.

B.253 As a sponsor and their affiliate are both accredited persons, each entity will be liable in their own right for their handling of CDR data. For example, where a sponsor makes a consumer data request, or uses or discloses CDR data at their affiliate’s request, the sponsor remains liable for their own conduct and must ensure they comply with the relevant privacy obligations.

B.254 The CDR Rules do contain some specific obligations for sponsors, particularly in relation to disclosure, notification and CDR policy. For more information, see Chapter C (paragraphs C.15, C.30, C.73, C.101, diagram after C.116), Chapter 1 (paragraph 1.55), Chapter 3

²⁴⁰ Explanatory Statement, Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2021, page 4.

²⁴¹ Competition and Consumer Act, subsection 56EB(1).

²⁴² For the banking sector, see CDR Rules, clause 3.1 of Schedule 3. For the energy sector, see CDR Rules, clause 3.1 of Schedule 4.

²⁴³ CDR Rules, rule 1.10D.

(paragraphs 3.26 – 3.27, diagram after 3.41), Chapter 5 (paragraph 5.3, 5.10, 5.27, 5.40 – 5.42), Chapter 6 (paragraphs 6.25, 6.68), Chapter 10 (paragraph 10.56), Chapter 11 (paragraph 11.31), Chapter 12 (paragraphs 12.22, 12.76 – 12.79), and the OAIC’s separate guidance for sponsors.²⁴⁴

B.255 The CDR Rules also impose some additional obligations on sponsors in relation to accreditation and the sponsorship arrangement.²⁴⁵ For example, a sponsor has obligations relating to an affiliate’s information security capabilities and related compliance matters.²⁴⁶ A sponsor must also notify the Data Recipient Accreditor as soon as practicable after becoming a sponsor of an affiliate, or when a sponsorship arrangement is suspended, expires or is terminated.²⁴⁷

B.256 A sponsor may enter into multiple sponsorship arrangements.

Sponsorship Arrangement

B.257 A ‘sponsorship arrangement’ is a written contract between a ‘sponsor’ and an ‘affiliate’ which meets the minimum requirements in CDR Rule 1.10D(1).

B.258 The sponsorship arrangement must provide for the sponsor to disclose CDR data that it holds as an accredited data recipient to their affiliate, in response to a consumer data request from the affiliate.

B.259 The arrangement must also require the affiliate to provide the sponsor with appropriate information and access to their operations as needed for the sponsor to fulfil their obligations as a sponsor (see paragraph B.255).

B.260 The arrangement may also provide for the sponsor to make consumer data requests, or to use or disclose CDR data, at their affiliate’s request.

Staged application

B.261 The relevant sector schedule to the CDR Rules may provide for the ‘staged application’ of CDR Rules in that sector. Staged application means that the CDR Rules will apply to a broader range of data holders or a broader range of CDR data within that sector over time. The result of staged application is that data holders may be required to comply with particular CDR data sharing obligations from different dates.

B.262 Part 6 of Schedule 3 to the CDR Rules provides for staged application of the CDR Rules in the banking sector. Under Part 6, the CDR Rules apply to a progressively broader range of

²⁴⁴ See <https://www.oaic.gov.au/consumer-data-right/guidance-and-advice/sponsored-accreditation-model-privacy-obligations-of-sponsors>.

²⁴⁵ Sponsors should also refer to the ‘sponsored accreditation’ section of the ACCC’s CDR Accreditation Guidelines: <https://www.cdr.gov.au/sites/default/files/2022-02/CDR-Accreditation-guidelines-version-3-published-16-February-2022.pdf>.

²⁴⁶ CDR Rules, clause 2.2 of Schedule 1.

²⁴⁷ CDR Rules, subrule 5.14(2).

banking sector data holders and a progressively broader range of banking products.²⁴⁸ The staged application of consumer data sharing obligations for certain banking sector data holders and banking products commenced on 1 July 2020.²⁴⁹

B.263 Part 8 of Schedule 4 to the CDR Rules provides for staged application of the CDR Rules in the energy sector. Under Part 8, the CDR Rules apply to a progressively broader range of energy sector data holders.²⁵⁰ The staged application of consumer data sharing obligations for energy sector data holders commenced on 15 November 2022.²⁵¹

Trusted adviser

B.264 ‘Trusted advisers’ are defined in the CDR Rules.²⁵² Consumers can nominate certain people to be their ‘trusted adviser’ and provide consent for an accredited data recipient to share data with that adviser, in order to receive advice or a service.²⁵³

B.265 A trusted adviser must belong to one of the following specified classes:

- qualified accountants within the meaning of the *Corporations Act 2001*²⁵⁴
- people admitted to the legal profession that hold a current practising certificate
- registered tax agents, BAS agents and tax (financial) advisers within the meaning of the *Tax Agent Services Act 2009*
- financial counselling agencies within the meaning of the *ASIC Corporations (Financial Counselling Agencies) Instrument 2017/792*
- financial advisers that are relevant providers under the *Corporations Act 2001*, other than provisional and limited-service time-share advisers, and
- mortgage brokers within the meaning of the *National Consumer Credit Protection Act 2009*.

B.266 A person is taken to be a member of a trusted adviser class for the purposes of rule 1.10C of the CDR Rules if the accredited data recipient has taken reasonable steps to confirm that the person was, and remains, a member of the class.

B.267 Trusted advisers are not CDR participants and are therefore not subject to the privacy safeguards or other obligations that apply under the CDR system. They should, however, be

²⁴⁸ For further detail regarding the staged application of the CDR Rules in the banking sector, see Part 6 of Schedule 3 to the CDR Rules. For general information about the rollout of the CDR, see the CDR website: <https://www.cdr.gov.au/rollout>.

²⁴⁹ See CDR Rules, clause 6.6 of Schedule 3.

²⁵⁰ For further detail regarding the staged application of the CDR Rules in the energy sector, see Part 8 of Schedule 4 to the CDR Rules. For general information about the rollout of the CDR, see the CDR website: <https://www.cdr.gov.au/rollout>.

²⁵¹ See CDR Rules, clause 8.6 of Schedule 4.

²⁵² See CDR Rules, subrule 1.10C(2).

²⁵³ CDR representatives can also disclose data to a trusted adviser with a consumer’s consent.

²⁵⁴ Section 88B of the *Corporations Act 2001* states that ASIC may declare in writing persons who are qualified accountants for the purposes of that Act. ASIC’s qualified accountant declaration instrument can be accessed here: <https://asic.gov.au/regulatory-resources/financial-services/financial-product-disclosure/certificates-issued-by-a-qualified-accountant/>.

aware of their professional obligations that relate to their handling of a consumer's data, and privacy obligations under the Privacy Act if they are an APP entity.

B.268 Generally, an accredited data recipient must not make any of the following a condition for the supply of the goods or services:

- the consumer nominating a trusted adviser
- the consumer nominating a particular person as a trusted adviser, or
- the consumer giving consent to disclosure of data to a trusted adviser.²⁵⁵

B.269 However, this prohibition on making the nomination of a trusted adviser, or the giving of a TA disclosure consent, a condition for the supply of goods or services does not apply where the only good or service being requested by the CDR consumer is for the accredited data recipient to collect CDR data from a data holder and provide it to a trusted adviser.²⁵⁶

Use

B.270 'Use' is not defined in the Competition and Consumer Act or the Privacy Act. 'Use' is a separate concept from disclosure, which is discussed at paragraphs B.183– B.188

B.271 Generally, an entity 'uses' CDR data when it handles and manages that data within its effective control. Examples include the entity:

- accessing and reading the data
- searching records for the data
- making a decision based on the data
- passing the data from one part of the entity to another
- de-identifying data, and
- deriving data from the data.

B.272 In limited circumstances, providing CDR data to a third party (such as a cloud service provider) for limited purposes may be a use of data, rather than a disclosure (see paragraphs B.183– B.188). However, such a provision of data will constitute a 'use' only if the data remains encrypted at all times, and the third party does not hold or have access to the decryption keys (on the basis that the third party would be technically unable to view or access the data at all times, and there would therefore be no disclosure).

B.273 Whether the provision of CDR data constitutes a use or a disclosure needs to be considered carefully on a case-by-case basis, and depends on the specific technical arrangements in place with the third party. If the third party could access or view unencrypted data, for example, to maintain or provide its service, then the provision of data to that third party would constitute a disclosure, and a CDR outsourcing arrangement would be required (see paragraphs B.203 to B.1).

²⁵⁵ CDR Rules, subrule 1.10C(4).

²⁵⁶ CDR Rules, rule 1.10C(5).

Voluntary consumer data

B.274 'Voluntary consumer data' is CDR data a data holder may disclose to a CDR consumer under CDR Rule 3.4(2) or to an accredited person under subrule 4.6(2) of the CDR Rules.

B.275 'Voluntary consumer data' for each CDR sector is defined in the relevant sector schedule to the CDR Rules.²⁵⁷

B.276 An example of voluntary consumer data is 'materially enhanced information', which is excluded from certain specified classes of information in the designation instruments for the banking and energy sectors,²⁵⁸ but may nonetheless be CDR data (as it is data derived from a specified class of information in the relevant designation instrument).²⁵⁹

Voluntary product data

B.277 The privacy safeguards do not apply to voluntary product data.²⁶⁰

B.278 'Voluntary product data' for each CDR sector is defined in the relevant sector schedule to the CDR Rules.²⁶¹

B.279 An example of voluntary product data in the banking sector is information about the availability or performance of a particular savings account product, where that information is not publicly available.²⁶²

²⁵⁷ For the banking sector, see CDR Rules, clause 3.2 of Schedule 3. For the energy sector, see CDR Rules, clause 3.2 of Schedule 4.

²⁵⁸ See section 10 of the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019 and section 11 of the Consumer Data Right (Energy Sector) Designation 2020. See also section 7 of the Consumer Data Right (Telecommunications Sector) Designation 2022 and 8 of the Consumer Data Right (Non-Bank Lenders) Designation 2022. However, unlike the banking and energy sectors at the date of publication of these guidelines there are no rules allowing for the sharing of designated telecommunications and non-bank lenders data under the CDR system, and expansion to the telecommunications sector has been paused. For further information on designation instruments, see paragraphs B.180 to B.182.

²⁵⁹ Competition and Consumer Act, subsection 56AI(1).

²⁶⁰ Competition and Consumer Act, subsection 56EB(1).

²⁶¹ For the banking sector, see CDR Rules, clause 3.1 of Schedule 3. For the energy sector, see CDR Rules, clause 3.1 of Schedule 4.

²⁶² See CDR Rules, clause 3.1(1)-(2) of Schedule 3.

Chapter C:

Consent —

The basis for collecting, using and disclosing CDR data

Version 5.0, November 2023

Contents

Key points	3
Why is it important?	3
How is consent in the CDR system different to the Privacy Act?	3
How does consent fit into the CDR system?	4
What are the different categories of consents in the CDR system?	9
How must consent be sought?	11
CDR representative arrangements	12
Sponsorship arrangements	13
Can consents be amended?	13
Requirements for asking a consumer to give or amend a consent	15
General processes	15
Fees for disclosure	17
Name and accreditation number	17
Data minimisation principle	18
Insight disclosure consent	19
Outsourced service providers (OSPs)	19
Withdrawal of consent	20
Treatment of redundant data	20
Collection by a sponsor at an affiliate's request	21
De-identification consents	21
Amendment of consent	22
Restrictions on seeking consents	23
How consents must be managed	24
Consumer dashboards	24
Consumers may withdraw consent	28
Effect of withdrawing consent	29
When a consent expires	30
Notification requirements	33
Authorisation	35

Key points

- An accredited person may only collect, use and disclose CDR data with the consent of the CDR consumer.
- The CDR system sets out specific categories of consents that an accredited person may seek from a CDR consumer. It prohibits an accredited person from seeking a consent which does not fit into these categories.
- The consumer data rules (CDR Rules) seek to ensure that a consumer's consent is voluntary, express, informed, specific as to purpose, time limited and easily withdrawn. An accredited person must ask a CDR consumer to give or amend a consent in accordance with the CDR Rules.
- A CDR representative is responsible for seeking a CDR consumer's consent when CDR data is being collected by a CDR representative principal under a CDR representative arrangement. However, the CDR representative principal is liable if the CDR representative does not obtain consent in accordance with the CDR Rules.¹
- In giving consent to the collection and use of their CDR data, a CDR consumer provides the accredited person with a 'valid request' to seek to collect the relevant CDR data.
- An accredited person's processes for asking a CDR consumer to give or amend a consent must be compliant with the data standards and have regard to the Consumer Experience Guidelines.
- An accredited person must comply with the data minimisation principle when collecting or using CDR data.
- A data holder may disclose CDR data only with the authorisation of the relevant CDR consumers.

Why is it important?

- C.1 The CDR system places the control of consumer data in the hands of the consumer. This is achieved by requiring the consumer's consent for the collection, use and disclosure of their CDR data.
- C.2 Consumer consent is the bedrock of the CDR system. Consent enables CDR consumers to be the decision makers in the CDR system, ensuring that they can direct where their data goes in order to obtain the most value from it.

How is consent in the CDR system different to the Privacy Act?

- C.3 It is important to understand how consent in the CDR system differs from consent under the *Privacy Act 1988* (the Privacy Act).

¹ CDR Rules, subrules 1.16A(3) and (4).

C.4 Under the CDR system:

- express consent from consumers is required for the collection, use and disclosure of their CDR data by accredited persons.² Without express consent, the accredited person is not able to collect, use, or disclose CDR data
- consent must meet the requirements set out in the CDR Rules
- consent is time limited – a CDR consumer can only give consent for a maximum period of 12 months (or 7 years for certain consents given by CDR business consumers).

C.5 However, under the Privacy Act:

- consent is not the primary basis upon which an entity may collect, use or disclose personal information³
- consent can be either express or implied⁴
- there is no maximum period for which a consumer can give consent, although consent given at a particular time in particular circumstances cannot be assumed to endure indefinitely.⁵

C.6 The CDR Rules contain specific requirements for an accredited person’s processes for seeking consent in the CDR system, as well as for information that must be presented to a CDR consumer when they are being asked to consent.⁶

C.7 The requirements by which an accredited person must seek consent from a CDR consumer are discussed in this Chapter.

How does consent fit into the CDR system?

C.8 Consent is the primary basis on which an accredited person may collect, use and disclose CDR data for which there are one or more consumers.⁷

² Consent is the only basis on which an accredited person may collect CDR data through the CDR. See [Chapter 3 \(Privacy Safeguard 3\)](#) for information on seeking to collect CDR data.

Consent is the primary basis on which an accredited data recipient of CDR data may use and disclose that data. For example, under Privacy Safeguard 6 an accredited data recipient may use or disclose CDR data where in accordance with the CDR Rules (which requires consent), unless a use or disclosure is required or authorised by law: *Competition and Consumer Act 2010* (Competition and Consumer Act), paragraph 56EI(1)(c). For information regarding use or disclosure of CDR data, see [Chapter 6 \(Privacy Safeguard 6\)](#), [Chapter 7 \(Privacy Safeguard 7\)](#), [Chapter 8 \(Privacy Safeguard 8\)](#) and [Chapter 9 \(Privacy Safeguard 9\)](#).

³ For example, an APP entity can collect personal information (other than sensitive information) if the information is reasonably necessary for one or more of the entity’s functions or activities. See APP Guidelines, [Chapter 3 \(APP 3\)](#) and [Chapter B \(Key concepts\)](#).

⁴ See subsection 6(1) of the Privacy Act and APP Guidelines, [Chapter B \(Key concepts\)](#).

⁵ See B.49, APP Guidelines, [Chapter B \(Key concepts\)](#).

⁶ CDR Rules, rules 4.10 and 4.11.

⁷ An accredited person may make a product data request without the involvement of a consumer, in which case consent is not required because it is not CDR data for which there are one or more consumers. For CDR data for which there are

C.9 Where an accredited person:

- offers a good or service through the CDR system, and
- needs to collect a consumer's CDR data from a data holder or accredited data recipient ('CDR participant'), or a CDR representative, in order to use it to provide such goods or services, the accredited person may ask for the consumer's consent to the collection and use of their CDR data to provide the good or service.⁸ Under a CDR representative arrangement, the CDR representative asks the consumer for these consents.⁹

C.10 In giving the above consents, the CDR consumer provides the accredited person with a 'valid request' to seek to collect the relevant CDR data.¹⁰ An accredited person can only collect the CDR data if it has obtained this consent.

C.11 Upon obtaining a 'valid request' from the consumer, the accredited person¹¹ may seek to collect the consumer's CDR data from the relevant CDR participant, or CDR representative, of the CDR data. The accredited person collects this CDR data by making a 'consumer data request' to the relevant CDR participant/s or CDR representative/s.¹²

C.12 Privacy Safeguard 3 prohibits an accredited person from seeking to collect data under the CDR system unless it is in response to a 'valid request' from the consumer.

C.13 Consent also underpins how an accredited person may use or disclose CDR data under Privacy Safeguard 6 and Privacy Safeguard 7. An accredited person can only use or disclose CDR data if it has obtained a use or disclosure consent.

C.14 The flow charts below paragraph C.15 demonstrate how consent fits in the key information flow between a consumer, accredited person, data holder and (for the energy sector) AEMO as secondary data holder, in relation to CDR data.

C.15 The following charts demonstrate the points at which a valid request is given by the consumer and a consumer data request is made on behalf of the consumer by the accredited person.

one or more consumers, while consent is the only basis on which an accredited person may collect such CDR data, consent is a primary basis on which an accredited person may use and disclose such CDR data. See [Chapter 6 \(Privacy Safeguard 6\)](#), [Chapter 7 \(Privacy Safeguard 7\)](#), [Chapter 8 \(Privacy Safeguard 8\)](#) and [Chapter 9 \(Privacy Safeguard 9\)](#) for further information regarding use and disclosure of CDR data.

⁸ CDR Rules, rules 4.3 and 4.3B.

⁹ CDR Rules, subrule 4.3A(2). See 'CDR representative arrangement' and 'CDR representative' in [Chapter B \(Key Concepts\)](#).

¹⁰ CDR Rules, subrules 4.3(3) and 4.3A(4). Where a consumer has given a CDR representative consent for a CDR representative principal to collect their CDR data and disclose it to the CDR representative, the CDR consumer provides the CDR representative principal (an accredited person) with a valid request.

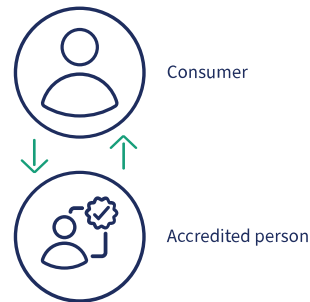
¹¹ The accredited person is the CDR representative principal where the CDR consumer has given the CDR representative principal a valid request.

¹² CDR Rules, rules 4.4 and 4.7A. For information regarding 'valid requests' and 'consumer data requests', see [Chapter 3 \(Privacy Safeguard 3\)](#). See also the flow chart underneath paragraph C.15 which demonstrates the points at which a valid request is given by the consumer and consumer data request is made on behalf of the consumer by the accredited person.

Consent and collection process for accredited persons

Obtaining consumer consent for the collection and use of CDR data

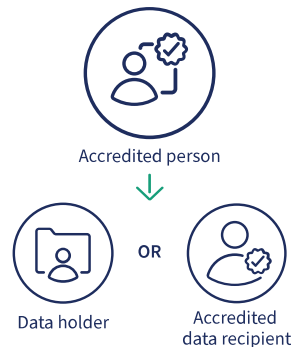
- Accredited person offers a good or service which requires CDR data
- Consumer wishes to be provided the good or service
- Accredited person asks the consumer to consent to the collection and use of their CDR data for this purpose
- Consumer provides their express consent to the collection and use of their CDR data



The consumer has given the accredited person a valid request ✓

Making a consumer data request on behalf of the consumer

- Consumer gives accredited person a valid request
- Accredited person asks the CDR participant ^[1] to disclose the consumer's CDR data
- Where the request is to a data holder, the accredited person makes the request using the data holder's 'accredited person request service', in accordance with the data standards ^[2]



The CDR participant obtains:

- the consumer's authorisation (in the case of a data holder)
- the consumer's AP disclosure consent (in the case of an accredited data recipient)

Where the CDR data is or includes SR data, the primary data holder obtains the consumer's authorisation. The primary data holder then requests any SR data it needs from the secondary data holder, using the secondary data holder's relevant online service. The secondary data holder discloses the SR data to the primary data holder (if it chooses)

The CDR participant sends the consumer's CDR data to the accredited person^[3]



The accredited person becomes an accredited data recipient for the consumer's CDR data

[1] This may be a data holder or accredited data recipient. However, an affiliate may only make a consumer data request directly to another accredited person

[2] Note: there are no equivalent requirements for how an accredited person makes a request to an accredited data recipient. Where the CDR data is or includes SR (shared responsibility) data, the request is made to the primary data holder.

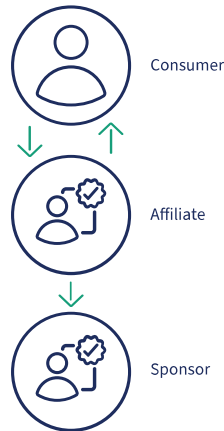
[3] Where the CDR participant is a primary data holder and the secondary data holder chooses not to disclose SR data to it, the primary data holder will not be able to send that SR data to the accredited person

[4] Note: For SR data requests, this will be the primary data holder

Consent and collection process for collection by sponsor

Obtaining consumer consent for the collection and use of CDR data

- Accredited person with sponsored accreditation (affiliate) offers a good or service which requires CDR data
- Consumer wishes to be provided the good or service
- A sponsor will collect the CDR data at the affiliate's request
- The affiliate asks the consumer to consent to the collection and use of their CDR data for this purpose
- Consumer provides their express consent to the collection and use of their CDR data
- The consumer's consent is taken to be consent for the sponsor to collect



The consumer has given the sponsor a valid request ✓

Making a consumer data request on behalf of the consumer

- Consumer gives sponsor a valid request
- Sponsor asks the CDR participant ^[1] to disclose the consumer's CDR data
- Where the request is to a data holder, the sponsor makes the request using the data holder's 'accredited person request service', in accordance with the data standards ^[2]

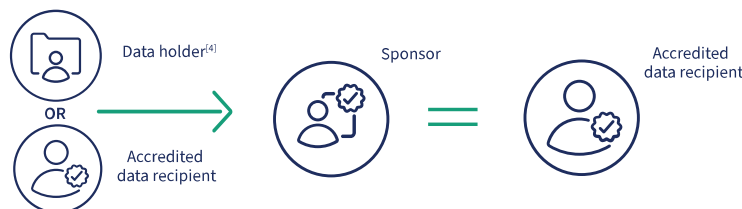


The CDR participant obtains:

- the consumer's authorisation (in the case of a data holder)
- the consumer's AP disclosure consent (in the case of an accredited data recipient)

Where the CDR data is or includes SR data, the primary data holder obtains the consumer's authorisation. The primary data holder then requests any SR data it needs from the secondary data holder, using the secondary data holder's relevant online service. The secondary data holder discloses the SR data to the primary data holder (if it chooses)

The CDR participant sends the consumer's CDR data to the sponsor^[3]



The sponsor becomes an accredited data recipient for the consumer's CDR data and discloses the data under the sponsorship arrangement to the affiliate (who also becomes an accredited data recipient)

[1] This may be a data holder or accredited data recipient.

[2] Note: there are no equivalent requirements for how an accredited person makes a request to an accredited data recipient. Where the CDR data is or includes SR (shared responsibility) data, the request is made to the primary data holder.

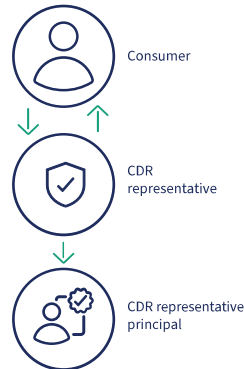
[3] Where the CDR participant is a primary data holder and the secondary data holder chooses not to disclose SR data to it, the primary data holder will not be able to send that SR data to the sponsor

[4] Note: For SR data requests, this will be the primary data holder

Consent and collection process for CDR representative arrangements

Obtaining consumer consent for the collection and use of CDR data

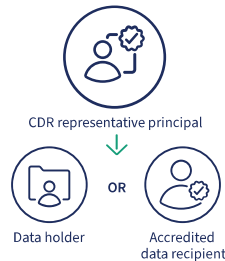
- CDR representative offers a good or service which requires CDR data
- Consumer wishes to be provided the good or service
- The CDR representative asks the consumer to consent to the collection and use of their CDR data for this purpose
- Consumer provides their express consent to the CDR representative principal collecting their CDR data, and disclosing it to the CDR representative for use



The consumer has given the CDR representative principal a valid request ✓

Making a consumer data request on behalf of the consumer

- Consumer gives CDR representative principal a valid request
- CDR representative principal asks the CDR participant^[1] to disclose the consumer's CDR data
- Where the request is to a data holder, the CDR representative principal makes the request using the data holder's 'accredited person request service', in accordance with the data standards^[2]

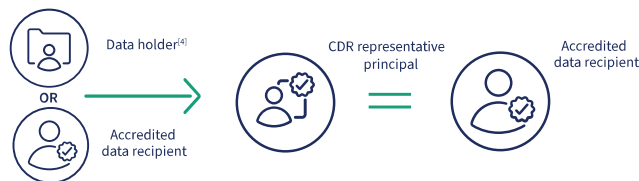


The CDR participant obtains:

- the consumer's authorisation (in the case of a data holder)
- the consumer's AP disclosure consent (in the case of an accredited data recipient)

Where the CDR data is or includes SR data, the primary data holder obtains the consumer's authorisation. The primary data holder then requests any SR data it needs from the secondary data holder, using the secondary data holder's relevant online service. The secondary data holder discloses the SR data to the primary data holder (if it chooses)

The CDR participant sends the consumer's CDR data to the CDR representative principal^[3]



The CDR representative principal becomes an accredited data recipient for the consumer's CDR data

CDR representative principal (accredited data recipient) discloses the consumer's CDR data to the CDR representative in accordance with the earlier consent from the consumer



The CDR representative has obtained the consumer's CDR data, and must comply with the terms of its CDR representative arrangement in handling the data

[1] This may be a data holder or accredited data recipient.

[2] Note: there are no equivalent requirements for how an accredited person makes a request to an accredited data recipient. Where the CDR data is or includes SR (shared responsibility) data, the request is made to the primary data holder

[3] Where the CDR participant is a primary data holder and the secondary data holder chooses not to disclose SR data to it, the primary data holder will not be able to send that SR data to the CDR representative principal

[4] Note: For SR data requests, this will be the primary data holder

What are the different categories of consents in the CDR system?

- C.16 The CDR system requires an accredited person to obtain different categories of consents from a consumer depending on what data-handling activity they propose to undertake.
- C.17 Consent means a collection consent, a use consent or a disclosure consent (including a consent that has been amended by a consumer under the CDR Rules).¹³ The categories of consents that may be given by a consumer to an accredited person in the CDR system are as follows:¹⁴
- **Collection consent:** a consent for an accredited person to collect particular CDR data from a data holder or accredited data recipient of that CDR data.¹⁵
 - **Use consent** – a consent for an accredited data recipient of particular CDR data, or a CDR representative that holds the CDR data as service data, to use that CDR data in a particular way, for example to provide goods or services requested by the consumer.¹⁶ Types of use consents include a direct marketing consent for an accredited data recipient to use CDR data for the purposes of direct marketing, and a de-identification consent (as outlined below).¹⁷
 - **AP disclosure consent:** a consent for an accredited data recipient of particular CDR data to disclose that CDR data to another accredited person in response to a consumer data request.¹⁸
 - **Direct marketing consent:** a consent for an accredited data recipient of particular CDR data to use or disclose that CDR data for the purposes of direct marketing.¹⁹

¹³ CDR Rules, rule 1.7.

¹⁴ Note: Each category of consent (except a ‘collection consent’) refers to an ‘accredited data recipient of particular CDR data’, rather than an ‘accredited person’. This is because, while the entity will be an ‘accredited person’ when seeking this category of consents, the entity would become an ‘accredited data recipient of particular CDR data’ in relation to that consumer upon collecting the relevant CDR data. See [Chapter B \(Key concepts\)](#) which outlines some key words and phrases that are used in the privacy safeguards and CDR Rules, including in relation to consent.

¹⁵ CDR Rules, paragraphs 1.10A(1)(a) and 1.10A(2)(a). If, in response to a collection consent, an accredited person proposes to make an SR data request to a data holder, the request must be made to the primary data holder and not the secondary data holder: CDR Rules, subrules 1.23(1)-(2). If the CDR consumer authorises the primary data holder to disclose the requested data, the primary data holder will then request any SR data it needs to respond to the request from the secondary data holder: CDR Rules, subrule 1.23(4). Under current arrangements, this is only relevant to the energy sector as the only sector with SR data and a secondary data holder (AEMO). For more information on SR data, see [Chapter B \(Key Concepts\)](#).

¹⁶ CDR Rules, paragraphs 1.10A(1)(b), 1.10A(2)(b) and 4.3A(2)(b).

¹⁷ CDR Rules, rule 1.7 defines a consent as ‘a collection consent, a use consent or a disclosure consent; or such a consent as amended in accordance with these rules’.

¹⁸ CDR Rules, paragraphs 1.10A(1)(c)(i) and 1.10A(2)(e).

Currently the CDR system only requires a consumer’s consent for disclosures to accredited persons. Consent is not required for disclosures to OSPs, however before doing so an accredited person must comply with other requirements in the CDR Rules. See [Chapter 6 \(Privacy Safeguard 6\)](#), [Chapter 7 \(Privacy Safeguard 7\)](#) and ‘outsourced service provider’ in [Chapter B \(Key Concepts\)](#).

¹⁹ CDR Rules, paragraphs 1.10A(1)(d) and 1.10A(2)(c).

- A direct marketing consent for an accredited data recipient to use CDR data for the purposes of direct marketing is a form of ‘use consent’.
- A direct marketing consent for an accredited data recipient to disclose CDR data to another accredited person for the purposes of direct marketing is a form of ‘disclosure consent’.²⁰
- **TA disclosure consent:** a consent for an accredited data recipient of particular CDR data, or a CDR representative, to disclose that CDR data to a trusted adviser of the CDR consumer, who belongs to one of the classes of ‘trusted advisers’ prescribed by CDR Rule 1.10C(2).²¹

An accredited data recipient or CDR representative must not make any of the following a condition for the supply of the goods or services:

- the consumer nominating a trusted adviser
- the consumer nominating a particular person as a trusted adviser, or
- the consumer giving consent to disclosure of data to a trusted adviser.²²
- **Insight disclosure consent:** a consent for an accredited data recipient or CDR representative to disclose certain insights based on their CDR data to a specified person for a permitted purpose.²³ These limited permitted purposes are:
 - to verify the CDR consumer’s identity
 - to verify the CDR consumer’s account balance, or
 - to verify the details of credits to, or debits from the consumer’s accounts.²⁴

However, where the CDR data relates to more than one transaction, the insight disclosure consent cannot authorise the accredited data recipient or CDR representative to disclose an amount or date in relation to any individual transaction.²⁵

- **De-identification consent:** a form of ‘use consent’ for an accredited data recipient of particular CDR data, or a CDR representative, to de-identify some or all of that CDR data in accordance with the CDR data de-identification process²⁶ and:
 - use the de-identified data for general research,²⁷ and/or

²⁰ CDR Rules, paragraph 1.10A(1)(c)(ii). A ‘disclosure consent’ includes an AP disclosure consent, as well as a consent for an accredited data recipient to disclose CDR data to an accredited person for the purposes of direct marketing.

²¹ CDR Rules, paragraph 1.10A(1)(c)(iii).

²² CDR Rules, subrule 1.10C(4). For the definition of a trusted adviser, including the classes of professions that are listed as trusted advisers, see [Chapter B \(Key concepts\)](#).

²³ CDR Rules, paragraph 1.10A(1)(c)(iv).

²⁴ CDR Rules, paragraph 1.10A(3)(a)(i)-(iii).

²⁵ CDR Rules, paragraph 1.10A(3)(b).

²⁶ See CDR Rules, rule 1.17 and [Chapter 12 \(Privacy Safeguard 12\)](#) for further information on the CDR data de-identification process.

²⁷ ‘General research’ is defined in CDR Rules, rule 1.7 to mean research undertaken by an accredited data recipient with CDR data de-identified in accordance with the CDR Rules that does not relate to the provision of goods or services to any particular consumer.

- disclose (including by selling) the de-identified data.
 - **Business consumer disclosure consent:** a consent for an accredited data recipient of particular CDR data to disclose that CDR data to a specified person,²⁸ where the CDR consumer providing consent is a CDR business consumer²⁹ who has given a business consumer statement.³⁰
- C.18 With the exception of business consumer disclosure consents, a CDR representative is also able to seek and obtain these use and disclosure consents in relation to CDR data it holds as service data.³¹
- C.19 An accredited person (or CDR representative) is prohibited from seeking a consent that is not in the list above.³²
- C.20 Each category of consent operates independently of each other. This means that an accredited person can ask for more than one category of consent, and that a CDR consumer must be enabled by an accredited person to independently manage each category of consent.³³ For example, an accredited person may ask a consumer for a collection consent and use consent, and the consumer can (in future) choose to withdraw only the collection consent, if they wish.³⁴
- C.21 The categories of consent are based off the ‘types’ of consents set out in the CDR Rules.³⁵

How must consent be sought?

- C.22 An accredited person must ask the consumer to give consent in accordance with Division 4.3 of the CDR Rules.³⁶ Division 4.3 sets out the specific requirements for each consent outlined in the section above.³⁷

²⁸ CDR Rules, paragraph 1.10A(1)(c)(v).

²⁹ CDR Rules, subrule 1.10A(9).

³⁰ CDR Rules, subrule 1.10A(10)-(11).

³¹ CDR Rules, paragraphs 1.10A(1)(b)-(e). See C.29 for more information.

³² CDR Rules, paragraph 4.12(3)(a) (and paragraph 4.20F(3)(a) in relation to CDR representatives).

³³ See the Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020* at [7].

³⁴ For example, where the consumer wishes to allow the accredited data recipient to keep using their CDR data so they may continue to receive the relevant good or service. Where a consumer withdraws both their collection consent and use consent, it is likely the CDR data would become redundant data that must be deleted or de-identified under Privacy Safeguard 12, unless an exception applies. For further information, see paragraphs C.90 to C.98 (‘Effect of withdrawing consent’).

³⁵ The ‘categories’ of consent are listed at CDR Rules, subrule 1.10A(2) and defined by reference to the ‘types’ of consents listed at CDR Rules, subrule 1.10A(1).

³⁶ CDR representatives must seek consent in accordance with Division 4.3A of the CDR Rules.

³⁷ Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020*, 13, which provides that an accredited person must ask for consent in accordance with Division 4.3 of the CDR Rules which now encompass provisions relating to all types and categories of consent. See also CDR Rules, subrule 4.3(2). Where a CDR representative is seeking consent from the consumer for their CDR representative principal to collect CDR data, the CDR representative must ask for consent in accordance with Division 4.3A of the CDR Rules.

- C.23 The requirements in Division 4.3 are outlined below under the headings ‘Requirements for asking a consumer to give or amend a consent’, ‘Restrictions on seeking consents’ and ‘How consents must be managed’.
- C.24 The object of Division 4.3 of the CDR Rules is to ensure that consent given by a consumer is voluntary, express, informed, specific as to purpose, time limited and easily withdrawn.³⁸
- C.25 In obtaining consent from a consumer, an accredited person must comply with requirements relating to:
- an accredited person’s processes for asking for consent³⁹
 - information to be presented to the consumer when asking for consent,⁴⁰ and
 - restrictions on seeking consent.⁴¹
- C.26 Where a consumer is not an individual and wishes to use the accredited person’s good or service through the CDR system, the accredited person should ensure the consent is given by a person who is duly authorised to provide the consent on the entity’s behalf.⁴²

CDR representative arrangements

- C.27 Under a CDR representative arrangement, the CDR representative seeks the relevant consents from the consumer, including consent for the CDR representative principal to collect the consumer’s CDR data.⁴³ See [Chapter B \(Key concepts\)](#) for more information on ‘CDR representative arrangement’, ‘CDR representative’ and ‘CDR representative principal’.
- C.28 The unaccredited CDR representative must ask for consent in accordance with Division 4.3A of the CDR Rules (which contains requirements which largely correspond to those for accredited persons in Division 4.3). The CDR representative principal must ensure its CDR representative complies with Division 4.3A and is liable for any breach of that division by its CDR representative.⁴⁴
- C.29 A CDR representative can seek certain specific consents from the consumer as follows:⁴⁵
- a collection consent for the CDR representative principal to collect the CDR consumer’s CDR data from the CDR participant and disclose it to the CDR representative

³⁸ CDR Rules, rule 4.9. (The same object is outlined in CDR Rules, rule 4.20C in relation to consent given by a consumer to a CDR representative). The Explanatory Statement to the CDR Rules, together with the Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020*, provides that the CDR Rules are intended to ensure that all consents sought in the CDR system are transparent and that consumers understand the potential consequences of what they are consenting to.

³⁹ CDR Rules, rule 4.10 (CDR Rules, rule 4.20D for the corresponding obligations for CDR representatives).

⁴⁰ CDR Rules, rule 4.11 (CDR Rules, rule 4.20E for the corresponding obligations for CDR representatives).

⁴¹ CDR Rules, rule 4.12 (CDR Rules, rule 4.20F for the corresponding obligations for CDR representatives).

⁴² A person is entitled, under section 128 of the *Corporations Act 2001*, to make the assumptions set out in section 129 of that Act when dealing with corporations, including that persons held out by the company as directors, officers and agents are duly appointed and have authority to exercise customary powers.

⁴³ CDR Rules, rule 4.3A.

⁴⁴ CDR Rules, subrules 1.16A(3) and (4).

⁴⁵ CDR Rules, subrule 4.3A(2).

- a use consent for the CDR representative to use the data to provide those goods or services. Once a collection consent has been given, a CDR representative may also ask the consumer to provide a disclosure consent in relation to the CDR data.⁴⁶

Sponsorship arrangements

- C.30 Under a sponsorship arrangement, an affiliate is responsible for seeking consents from the consumer. This is regardless of whether the affiliate intends to collect the CDR data themselves (which they are permitted to do from an accredited data recipient) or request their sponsors to do so on their behalf.⁴⁷
- C.31 Like all accredited persons, an affiliate must ask for consents in accordance with Division 4.3 of the CDR Rules.

Can consents be amended?

- C.32 An accredited person may invite a consumer to amend an existing consent.⁴⁸ This includes allowing a consumer to change:
- the types of CDR data that can be collected and/or disclosed
 - what the CDR data can be used for
 - what accounts or data holders CDR data is to be collected from, and/or
 - the duration of the consent.⁴⁹
- C.33 An invitation to amend a consent may be issued only where the amendment would:⁵⁰
- better enable the accredited person to provide the goods or services requested by the consumer under the existing consent,⁵¹ or
 - be consequential to an agreement between the accredited person and consumer to modify those goods or services, and enable the accredited person to provide the modified goods or services.

⁴⁶ CDR Rules, paragraph 1.10A(1)(c) (with the exception of business consumer disclosure consents) and subrule 4.3A(3).

⁴⁷ See CDR Rules, rule 5.1B. In particular, where CDR data is to be collected from a data holder, the affiliate must ask their sponsor to collect it as an affiliate cannot collect directly from a data holder: CDR Rules, subrule 5.1B(3).

⁴⁸ A CDR representative may also invite a consumer to amend an existing consent – see CDR Rules, rules 4.20G-4.20I.

⁴⁹ See the Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020* at [6].

⁵⁰ CDR Rules, subrule 4.12B(3).

⁵¹ That is, the goods or services requested by the consumer as part of their valid request in CDR Rules, paragraph 4.3(1)(a).

- C.34 An invitation to amend an existing consent may be given via the consumer dashboard (if applicable)⁵² or in writing to the CDR consumer.⁵³ An invitation can only be given where the consent is current (i.e. has not expired).⁵⁴
- C.35 Where an accredited person wishes to invite a CDR consumer to amend the duration of their consent, the invitation must not be given:
- any earlier than a reasonable period before the existing consent expires, and
 - more than a reasonable number of times within this period.⁵⁵

Example: A CDR consumer has given a consent to an accredited data recipient in relation to CDR data for a period of 3 months. In the 3 weeks prior to expiry, the accredited person invites the consumer on 2 occasions to extend the duration of their existing consent. The accredited data recipient has decided, based on their circumstances, that they have provided the invitation within a reasonable period before the existing consent expires, and a reasonable number of times within that period.⁵⁶

- C.36 Where an accredited person wishes to invite a CDR consumer to extend the duration of their consent, it should first consider whether the invitation would constitute an offer to renew existing goods or services under paragraph 7.5(3)(a)(ii) of the CDR Rules (in which case a direct marketing consent would be required).⁵⁷
- C.37 An accredited person cannot ask a CDR consumer to extend the duration of an existing consent for longer than 12 months,⁵⁸ unless the CDR consumer is a CDR business consumer and provides a business consumer statement. In this case, the accredited person cannot ask the CDR business consumer to extend the duration of an existing consent for longer than 7 years.⁵⁹
- C.38 An accredited person must ask the CDR consumer to give any amendments to their existing consent in the same manner that it asked the consumer to provide the existing consent (this

⁵² It is optional for accredited persons to offer a consent amendment functionality in the consumer dashboard: see CDR Rules, paragraphs 4.12B(2)(a) and 1.14(2A).

⁵³ CDR Rules, subrule 4.12B(2).

⁵⁴ CDR Rules, subrule 4.12B(3). See paragraphs C.99 to C.105 and CDR Rule 4.14 for information on when consent expires.

⁵⁵ CDR Rules, subrule 4.12B(4).

⁵⁶ Example adapted from the Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020*, 15.

⁵⁷ Sending the consumer an offer to renew existing goods or services when they expire is direct marketing, and is only permitted if the accredited person has obtained a direct marketing consent from the consumer to send them information for these purposes. See Competition and Consumer Act, subsection 56EJ(1) and CDR Rules, paragraph 7.5(3)(a)(ii). For further information on this requirement, see [Chapter 7 \(Privacy Safeguard 7\)](#).

⁵⁸ This is as a result of CDR Rules, subrule 4.12(1) and paragraph 4.14(1)(c), which provides that the duration of a consent cannot exceed 12 months.

⁵⁹ This is as a result of CDR Rules, subrule 4.12(1A) and paragraph 4.14(1)(c), which provide that the duration of a consent cannot exceed 7 years for a CDR business consumer who has given a business consumer statement. However, an accredited person may not deal with a person in their capacity as a CDR business consumer until the earlier of 1 December 2023 or the day the Data Standards chair makes related data standards (CDR rules, subrule 1.10A(14)).

includes compliance with Division 4.3 of the CDR Rules).⁶⁰ There are some exceptions, as outlined in the following section ('Requirements for asking a consumer to give or amend a consent').⁶¹

- C.39 Where a consumer data request made on behalf of a CDR consumer has not been completely resolved and the CDR consumer amends the corresponding collection consent, the accredited person must notify the relevant CDR participant/s that the consent has been amended.⁶²
- where the CDR data is being collected from a data holder, in accordance with the data standards, and/or
 - where the CDR data is being collected from an accredited data recipient, as soon as practicable. This notice should contain sufficient detail to enable the accredited data recipient to understand the types of CDR data to which the amended collection consent now applies.
- C.40 An accredited person must also provide a CDR consumer with certain notifications upon the amendment of a consent. These are outlined under 'Notification requirements' in paragraph C.106.
- C.41 An amendment of a consent takes effect when the CDR consumer amends the consent.⁶³

Requirements for asking a consumer to give or amend a consent

General processes

- C.42 An accredited person's processes for asking a CDR consumer to give or amend a consent must:
- accord with any consumer experience data standards,⁶⁴ and
 - be as easy to understand as practicable, including by using concise language and, where appropriate, visual aids.⁶⁵

⁶⁰ CDR Rules, subrule 4.12C(1).

⁶¹ The exceptions are contained in subrule 4.12C(2) of the CDR Rules and allow certain details of the existing consent to be presented as pre-selected options (namely, the details covered by CDR Rules, paragraphs 4.11(1)(a), (b),(ba) and (e)). They also require additional information to be presented to the consumer to explain: the consequences of amending consent; and that the accredited person would be able to continue to use CDR data already disclosed to it to the extent allowed by the amended consent.

⁶² CDR Rules, rule 4.18C.

⁶³ CDR Rules, rule 4.12A. As per the note to this CDR Rule, it is not possible for the consumer to specify a different date or time.

⁶⁴ CDR Rules, rule 4.10. The consumer experience standards are data standards regarding the obtaining and withdrawal of consents, the collection and use of CDR data, and the types of CDR data and description of those types to be used by CDR participants when making requests. Further information is available in [Chapter B \(Key concepts\)](#).

⁶⁵ CDR Rules, rule 4.10.

- C.43 In ensuring processes are easy to understand, an accredited person must also have regard to the Consumer Experience Guidelines.⁶⁶
- C.44 An accredited person must not:
- include or refer to the accredited person’s CDR policy or other documents in a way that would reduce consumer comprehension when seeking consent, or
 - bundle consents with other directions, agreements, consents or permissions.⁶⁷ This practice has the potential to undermine the voluntary nature of the consent.
- C.45 However, an accredited person may refer to its CDR policy when seeking consent, so long as doing so would not be likely to reduce consumer comprehension.⁶⁸
- C.46 Each time an accredited person seeks a CDR consumer’s consent, it must allow the consumer to actively select or clearly indicate:
- for collection and disclosure consents,⁶⁹ the particular types of CDR data to which the consent will apply⁷⁰
 - for all consents, whether the data will be:
 - collected and, if applicable, disclosed on a single occasion and used over a specified period of time (not exceeding 12 months, or in the case of a consent given by a CDR business consumer that includes a business consumer statement, 7 years), or
 - collected and, if applicable, disclosed on an ongoing basis and used over a specified period of time (not exceeding 12 months, or in the case of a consent given by a CDR business consumer that includes a business consumer statement, 7 years)⁷¹
 - for a use consent,⁷² the specific uses of that CDR data,⁷³ and

⁶⁶ CDR Rules, rule 4.10. The ‘Consumer Experience Guidelines’ provide best practice interpretations of several CDR Rules relating to consent and are discussed in [Chapter B \(Key concepts\)](#). They are available here: cx.cds.gov.au.

⁶⁷ CDR Rules, rule 4.10. Bundled consent refers to the ‘bundling’ together of multiple requests for a consumer’s consent to a wide range of collections, uses and/or disclosures of CDR data, without giving the consumer the opportunity to choose which collections, uses or disclosures they agree to and which they do not.

⁶⁸ Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020*, 14. Indeed, accredited persons are required to provide links to their CDR policy at certain points in the consent-seeking process, for example when providing information about OSPs (CDR Rules, paragraphs 4.11(3)(f)(i) and (ii)) and general research (CDR Rules, subrule 4.15(c)).

⁶⁹ Including both an AP disclosure consent (as defined in CDR Rule 1.10A) and a direct marketing consent for an accredited data recipient of particular CDR data to disclose that CDR data to another accredited person for the purposes of direct marketing: CDR Rules, paragraph 1.10A(1)(c)(ii).

⁷⁰ CDR Rules, paragraphs 4.11(1)(a)(i) and 4.11(1)(c) and subrule 4.11(2).

⁷¹ CDR Rules, paragraphs 4.11(1)(b) and 4.11(1)(c), and subrules 4.11(2), 4.12(1) and 4.12(1)(A).

⁷² Including a de-identification consent (as defined in CDR Rule 1.10A) and a direct marketing consent for an accredited data recipient of particular CDR data to use that CDR data for the purposes of direct marketing (as per CDR Rules, rule 1.10A).

⁷³ CDR Rules, paragraphs 4.11(1)(a)(ii) and 4.11(1)(c) and subrule 4.11(2).

- for a disclosure consent,⁷⁴ the person to whom the CDR data may be disclosed.⁷⁵

C.47 Each time an accredited person seeks a CDR consumer's consent, it must also:

- ask for the consumer's express consent for the selections in paragraph C.46 above,⁷⁶ and
- not pre-select these options,⁷⁷ except where the accredited person is asking the consumer to amend an existing consent.⁷⁸ In this situation, the accredited person may pre-select the above options to reflect what the consumer has selected in the past.⁷⁹

Fees for disclosure

C.48 An accredited person may charge the CDR consumer a fee for the disclosure of CDR data, or pass on to the consumer a fee charged by the data holder or accredited data recipient for the disclosure of CDR data.⁸⁰ This must be made clear to the consumer.

C.49 To do this, the accredited person must:

- clearly distinguish between the CDR data for which a fee will, and will not, be charged or passed on⁸¹
- inform the consumer of the amount of the fee, and the consequences if the consumer does not consent to the collection or disclosure, as appropriate, of the CDR data for which a fee will be charged or passed on,⁸² and
- allow the consumer to actively select or otherwise clearly indicate whether they consent to the collection or disclosure, as appropriate, of the CDR data for which a fee will be charged or passed on.⁸³

Name and accreditation number

C.50 The accredited person must ensure that its name is clearly displayed in the consent request.⁸⁴

⁷⁴ Including both an AP disclosure consent (as defined in CDR Rule 1.10A) and a direct marketing consent for an accredited data recipient of particular CDR data to disclose that CDR data to another accredited person for the purposes of direct marketing: CDR Rules, paragraph 1.10A(1)(c)(ii).

⁷⁵ CDR Rules, paragraph 4.11(1)(ba) and subrule 4.11(2).

⁷⁶ CDR Rule, paragraph 4.11(1)(c).

⁷⁷ CDR Rules, subrule 4.11(2).

⁷⁸ CDR Rules, paragraph 4.12C(2)(a).

⁷⁹ For example, where this would assist the consumer to make an informed decision as to how they would like to amend their consent.

⁸⁰ For example, where the consumer's request covers voluntary consumer data, the data holder may decide to charge the accredited person a fee. For information regarding 'required consumer data' and 'voluntary consumer data', see [Chapter B \(Key concepts\)](#).

⁸¹ CDR Rules, paragraph 4.11(1)(d) (CDR Rules, paragraph 4.20E(1)(e) where a CDR representative is seeking consent).

⁸² CDR Rules, paragraph 4.11(3)(d) (CDR Rules, paragraph 4.20E(3)(h) where a CDR representative is seeking consent).

⁸³ CDR Rules, paragraph 4.11(1)(d) (CDR Rules, paragraph 4.20E(1)(e) where a CDR representative is seeking consent).

⁸⁴ CDR Rules, paragraph 4.11(3)(a).

- C.51 The accredited person's accreditation number must also be included in the consent request.⁸⁵ This number is assigned to the accredited person by the Data Recipient Accreditor.
- C.52 For more information on the Data Recipient Accreditor and the accreditation process and conditions, see the ACCC's Accreditation Guidelines.

Data minimisation principle

- C.53 Collection and use of CDR data is limited by the data minimisation principle,⁸⁶ which provides that an accredited person:
- must not collect more data than is reasonably needed, or data that relates to a longer time period than is reasonably needed, for it or its CDR representative to provide the goods or services requested by the consumer, and
 - may use the collected data only in accordance with the consent provided, and only as reasonably needed in order to provide the requested goods or services or to fulfil any other purpose consented to by the consumer.⁸⁷

Example: An accredited person is responding to a 'valid request' from a CDR consumer to collect their CDR data from their data holder in relation to the consumer's eligibility to open a bank account. The accredited person asks the consumer to consent to the collection of their transaction data. However, transaction data has no bearing on the applicant's eligibility for the delivery of the service. The accredited person would therefore likely be in breach of the data minimisation principle.

- C.54 Where an accredited person is seeking a collection consent or use consent,⁸⁸ the accredited person must explain how its collection and use is in line with the data minimisation principle.⁸⁹
- C.55 For a collection consent, this explanation must include an outline of why the accredited person believes collecting the data is 'reasonably needed' to provide the relevant goods or services or to fulfil another purpose for which the accredited person is seeking consent.⁹⁰

⁸⁵ CDR Rules, paragraph 4.11(3)(b). Where a CDR representative is seeking consent, it must instead include its name, the country in which it is located (if not Australia), the CDR representative principal's name and accreditation number, the fact that the data will be collected by the CDR representative principal at the CDR representative's request, a link to the CDR representative principal's CDR policy, and a statement that the CDR consumer can obtain further information about collections or disclosures from the CDR representative principal's CDR policy: CDR Rules, subrule 4.20E(3)(a)-(e), (j) and (l).

⁸⁶ CDR Rules, subrule 4.12(2).

⁸⁷ CDR Rules, rule 1.8.

⁸⁸ Including a de-identification consent (as defined in CDR Rules, rule 1.10A) and a direct marketing consent for an accredited data recipient of particular CDR data to use that CDR data for the purposes of direct marketing (as per CDR Rules, rule 1.10A).

⁸⁹ CDR Rules, paragraph 4.11(3)(c) (CDR Rules, paragraph 4.20E(3)(f) where a CDR representative is seeking consent). For further information regarding the data minimisation principle, see [Chapter B \(Key concepts\)](#).

⁹⁰ CDR Rules, paragraph 4.11(3)(c)(i).

- For example, the accredited person must explain how the data is necessary to deliver the service that it is providing.⁹¹
- C.56 The accredited person must also explain the reason for the data collection period. The collection period must be no longer than is ‘reasonably needed’ to provide the goods or services or to fulfil any other purpose for which the accredited person is seeking consent.⁹² This means that:
- the accredited person needs to explain why the data is collected over the collection period
 - there should be a reason why historical data is collected, and that reason must be both in line with the data minimisation principle and explained to the CDR consumer at the point of consent.
- C.57 For a use consent,⁹³ the accredited person must also explain how its use will not go beyond what is reasonably needed to provide the relevant goods or services or to fulfil another purpose for which the accredited person is seeking consent.⁹⁴

Insight disclosure consent

- C.58 When seeking an insight disclosure consent, an accredited data recipient must explain to the CDR consumer the CDR insight to be disclosed, including what the CDR insight would reveal or describe about them.⁹⁵

Outsourced service providers (OSPs)

- C.59 Where CDR data may be disclosed to or collected by a direct or indirect outsourced service provider (OSP)⁹⁶ of the accredited person (including one that is based overseas), the accredited person must:
- Tell the CDR consumer that the accredited person will use an OSP to collect CDR data and/or disclose the consumer’s CDR data to an OSP, and
 - provide the CDR consumer with a link to the accredited person’s CDR policy, noting that further information about OSPs can be found in that policy.^{97,98}

⁹¹ CDR Rules, paragraph 4.11(3)(c).

⁹² CDR Rules, paragraph 4.11(3)(c)(i).

⁹³ Including a de-identification consent (as defined in CDR Rules, rule 1.10A) and a direct marketing consent for an accredited data recipient of particular CDR data to use that CDR data for the purposes of direct marketing (as per CDR Rules, rule 1.10A).

⁹⁴ CDR Rules, paragraph 4.11(3)(c)(ii).

⁹⁵ CDR Rules, paragraph 4.11(3)(ca) (CDR Rules, paragraph 4.20E(3)(g) where a CDR representative is seeking consent).

⁹⁶ For further information regarding OSPs, see [Chapter B \(Key concepts\)](#).

⁹⁷ CDR Rules, paragraph 4.11(3)(f). An accredited data recipient’s CDR policy must include, amongst other things, a list of OSPs, the nature of their services, the CDR data and classes of CDR data that may be disclosed to those OSPs. For further information, see [Chapter 1 \(Privacy Safeguard 1\)](#) and the [Guide to developing a CDR policy](#).

⁹⁸ Where a CDR representative is seeking consent from the CDR consumer, this requirement applies in the case of direct or indirect OSPs engaged by either the CDR representative or their CDR representative principal -CDR Rules, paragraphs 4.20E(3)(k)-(l).

Withdrawal of consent

C.60 The accredited person must explain to the CDR consumer:⁹⁹

- that their consent/s can be withdrawn at any time
- how to withdraw consent, and
- the consequences (if any) of withdrawing consent.

Treatment of redundant data

C.61 The accredited person must tell the CDR consumer whether the accredited person has a general policy of:

- deleting redundant data,
- de-identifying redundant data, or
- deciding, when the CDR data becomes redundant, whether to delete or de-identify the redundant data.¹⁰⁰

C.62 Where the accredited person will¹⁰¹ or may¹⁰² de-identify redundant data, the accredited person must also:

- allow the CDR consumer to elect for their redundant data to be deleted,¹⁰³ including by outlining the consumer's right to elect for this to occur and providing instructions for how the consumer can make the election.¹⁰⁴ Where the accredited person is asking the consumer to amend an existing consent, and the consumer previously made an election, the accredited person may pre-select this election¹⁰⁵
- tell the CDR consumer that the accredited person would de-identify redundant data in accordance with the prescribed process for de-identification of CDR data, and explain what this means¹⁰⁶

⁹⁹ CDR Rules, paragraph 4.11(3)(g) (CDR Rules, paragraph 4.20E(3)(m) where a CDR representative is seeking consent from the CDR consumer).

¹⁰⁰ CDR Rules, paragraph 4.11(3)(h)(i) and subrule 4.17(1) (CDR Rules, paragraph 4.20E(3)(n)(i) and subrule 4.20N(1) where a CDR representative is seeking consent from the CDR consumer).

¹⁰¹ That is, because the accredited person communicated (when seeking consent) a general policy of de-identifying redundant data.

¹⁰² That is, because the accredited person communicated (when seeking consent) a general policy of deciding, when the CDR data becomes redundant, whether to delete or de-identify the redundant data.

¹⁰³ CDR Rules, paragraph 4.11(1)(e) and rule 4.16 (CDR Rules, paragraph 4.20E(1)(f) and rule 4.20M where a CDR representative is seeking consent from the CDR consumer). The accredited person must allow the consumer to make this election when providing consent to the accredited person in relation to their CDR data, and at any other point in time before the consent expires (CDR Rules, subrule 4.16(1)).

¹⁰⁴ CDR Rules, paragraph 4.11(3)(h) (CDR Rules, paragraph 4.20E(3)(n) where a CDR representative is seeking consent from the CDR consumer).

¹⁰⁵ CDR Rules, paragraph 4.12C(2)(b).

¹⁰⁶ CDR Rules, paragraphs 4.17(2)(a), 4.17(2)(b). The prescribed process is the CDR data de-identification process outlined in rule 1.17. Further information on the CDR data de-identification process is in [Chapter 12 \(Privacy Safeguard 12\)](#).

- tell the CDR consumer that, once the data is de-identified, the accredited person would be able to use or, if applicable, disclose the de-identified redundant data without seeking further consent from the consumer,¹⁰⁷ and
- if applicable, provide the CDR consumer with examples of how the accredited person could use the redundant data once de-identified.¹⁰⁸

C.63 See [Chapter 12 \(Privacy Safeguard 12\)](#) for further information on the treatment of redundant data (i.e. destruction or de-identification).

Collection by a sponsor at an affiliate's request

C.64 When an affiliate is seeking a collection consent from a CDR consumer, and a sponsor will collect the data at the affiliate's request under a sponsorship arrangement, the affiliate must provide the consumer with the following information:

- a statement of the fact that the sponsor will be collecting the consumer's CDR data at the request of the affiliate
- the sponsor's name
- the sponsor's accreditation number
- a link to the sponsor's CDR policy, and
- a statement that the consumer can obtain further information about the sponsor's collection of CDR data (and subsequent disclosure of that data to the affiliate) from the sponsor's CDR policy.¹⁰⁹

De-identification consents

C.65 Where an accredited person is asking the CDR consumer for a de-identification consent as defined under rule 1.10A of the CDR Rules, the accredited person must also tell the consumer the additional information in rule 4.15:¹¹⁰

- what the CDR de-identification process is¹¹¹
- if the accredited person would disclose (for example, by sale) the de-identified data to one or more other persons:
 - a statement of that fact

¹⁰⁷ CDR Rules, paragraph 4.17(2)(a).

¹⁰⁸ CDR Rules, paragraph 4.17(2)(c).

¹⁰⁹ See CDR Rules, subrule 4.3(2B) and paragraph 4.11(3)(i).

¹¹⁰ CDR Rules, paragraph 4.11(3)(e) and rule 4.15 (CDR Rules, paragraph 4.20E(3)(i) and rule 4.20L where a CDR representative is seeking consent from the CDR consumer).

¹¹¹ The CDR data de-identification process is outlined in CDR Rules, rule 1.17. More information on this requirement is in [Chapter 12 \(Privacy Safeguard 12\)](#).

- the classes of persons to whom the accredited person would disclose the de-identified data (for example, to market research organisations or university research centres), and
- the purpose/s for which the accredited person would disclose the de-identified data (for example, to sell the de-identified data or to provide to a university for research)
- if the accredited person would use the de-identified data for general research:¹¹²
 - a statement of that fact
 - that the CDR consumer can find further information in the accredited person’s CDR policy of the research to be conducted and any additional benefit to be provided to the consumer for consenting to this use of their data,¹¹³ and
 - a hyperlink to the relevant section/s of the accredited person’s CDR policy, and
- that the CDR consumer would not be able to elect to have the de-identified data deleted once it becomes redundant data.

C.66 When seeking a de-identification consent, the accredited person must explain how their collection and use is in line with the data minimisation principle.¹¹⁴ See paragraphs C.53 to C.57 above.

Tip: Where an accredited person is seeking a de-identification consent so that it may use the de-identified data for general research, the accredited person could inform the CDR consumer that the general research does not relate to the provision of the requested goods or services. This will help to ensure a consumer is aware of this fact so they may make an informed decision when deciding whether to provide the de-identification consent.

Amendment of consent

- C.67 Where an accredited person is inviting a CDR consumer to amend their existing consent, in addition to the other requirements outlined in the above sections, the accredited person must give the consumer statements that outline:¹¹⁵
- the consequences of amending a consent, and

¹¹² ‘General research’ is defined in CDR Rules, rule 1.7 to mean research undertaken by an accredited data recipient with CDR data de-identified in accordance with the CDR Rules that does not relate to the provision of goods or services to any particular CDR consumer. An example is product or business development: Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020* at [21].

¹¹³ For example, a benefit may include the accredited data recipient paying a fee to the consumer for using their data or providing a discount on the services they provide to the consumer: ACCC, CDR Rules Expansion Amendments Consultation Paper, September 2020, 48.

¹¹⁴ CDR Rules, paragraph 4.11(3)(c) (CDR Rules, paragraph 4.20E(3)(f) for CDR representatives). For further information regarding the data minimisation principle, see paragraphs C.53 to C.57 and [Chapter B \(Key concepts\)](#).

¹¹⁵ CDR Rules, subrule 4.12C(3) (CDR Rules, subrule 4.20I(3) for CDR representatives inviting a consumer to amend consent).

- the extent to which the accredited person will be able to use any CDR data that has already been disclosed to it.

Example: Laypac, an accredited person, offers CDR consumers the ability to amend their collection consent, in order to remove certain data types. Prior to making an amendment, Laypac tells a consumer:

“If you amend your consent, we will no longer collect your account balance and details, but we will use the data we’ve already collected [...]. When you withdraw your use consent or when it expires on 1 October, we will delete it,¹¹⁶ along with all your other data, in accordance with our CDR policy...”¹¹⁷

C.68 When inviting a CDR business consumer to amend a consent, an accredited person must take reasonable steps to re-confirm that either the CDR consumer is not an individual, or that the CDR consumer has an active ABN.¹¹⁸

Restrictions on seeking consents

C.69 CDR Rule 4.12 provides that when seeking consent from a CDR consumer, an accredited person must not ask for:¹¹⁹

- consent to collect, use or disclose CDR data over a period exceeding 12 months (unless the CDR consumer is a CDR business consumer)
- if the CDR consumer is a CDR business consumer who provides a business consumer statement, consent to use or disclose CDR data over a period exceeding 7 years. If a consent is sought for a period exceeding 12 months, the accredited person must give the CDR business consumer the option of choosing a period for the consent of 12 months or less
- consent to collect or use the data in a manner that is in breach of the data minimisation principle¹²⁰
- a consent that is not in a ‘category’ of consents (see paragraph C.17 for a list of the categories of consents), or¹²¹

¹¹⁶ See [Chapter 12 \(Privacy Safeguard 12\)](#) for information on when CDR data will become ‘redundant data’ that must be deleted or de-identified in accordance with the CDR Rules, unless an exception applies.

¹¹⁷ Example from Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020*, 16.

¹¹⁸ CDR Rules, subrule 4.12C(4).

¹¹⁹ CDR Rules, rule 4.12. Corresponding restrictions on CDR representatives seeking consent are in CDR Rules, rule 4.20F.

¹²⁰ The data minimisation principle is discussed in [Chapter B \(Key concepts\)](#), and at paragraph C.53 of this Chapter C.

¹²¹ See CDR Rules, subrule 1.10A(2).

- consent to use the CDR data, including by aggregating it, for the purpose of identifying, compiling insights or building a profile in relation to any identifiable person who is not the consumer who is providing the consent.¹²²
- C.70 However, in some circumstances an accredited person can use the CDR data, including by aggregating it, for the purpose of identifying, compiling insights or building a profile in relation to any identifiable person who is not the CDR consumer who is providing the consent. This is permitted where:¹²³
- the person’s identity is readily apparent
 - the accredited person is seeking consent to derive, from the consumer’s CDR data, CDR data about the non-CDR consumer’s interactions with the consumer, and
 - the accredited person will use that derived CDR data only for the purpose of providing the goods or services requested by the consumer.

Example

ChiWi is an accredited person offering a budgeting service that tracks a person’s spending. One category of spending is ‘gifts’.

Antonio has recently moved out of home and receives an allowance from his mother, Maria, each week. He has Maria’s account saved in his banking address book under her full name.

Antonio transfers his transaction data to ChiWi to track his spending. Maria’s identity is readily apparent from Antonio’s transaction data.

ChiWi may consider Maria’s behaviour only in so far as it is relevant to Antonio’s spending and saving habits for the purpose of providing Antonio with the budgeting service.

How consents must be managed

Consumer dashboards

- C.71 An accredited person must provide a consumer dashboard for each CDR consumer who has provided a consent in relation to their CDR data.¹²⁴
- C.72 Where an accredited person collects a consumer’s CDR data on behalf of another accredited person (the ‘OSP chain principal’) under a CDR outsourcing arrangement, only the OSP chain principal needs to provide the relevant consumer with a dashboard.¹²⁵

¹²² For example, where an accredited person receives information such as BSB numbers and account numbers as part of a consumer’s payee list, the accredited person is prohibited from using that information to discover the name or identity of the payee or compile insights or a profile of that payee.

¹²³ CDR Rules, subrule 4.12(4).

¹²⁴ CDR Rules, rule 1.14.

¹²⁵ See CDR Rules, subrule 1.7(5). For information regarding CDR outsourcing arrangements, see [Chapter B \(Key concepts\)](#).

- C.73 Where a sponsor collects a consumer's CDR data on behalf of their affiliate under a sponsorship arrangement, the affiliate must provide a consumer dashboard for each consumer who has provided a consent to the affiliate in relation to their CDR data.
- C.74 Where a CDR representative principal collects a consumer's CDR data on behalf of their CDR representative under a CDR representative arrangement, the CDR representative principal may arrange for the CDR representative to provide a consumer dashboard on its behalf.¹²⁶

Privacy tip: To enhance consumer understanding and reduce the risk of confusion, it may be preferable for the CDR representative, rather than the CDR representative principal, to provide the consumer dashboard. This is because it is the CDR representative, rather than the CDR representative principal, that has the consumer-facing relationship.

Where this option is chosen, the CDR representative principal should include an obligation for the CDR representative to provide the dashboard as an additional requirement in the written contract (CDR representative arrangement). The CDR representative principal should further monitor compliance with these obligations as part of ensuring the CDR representative complies with the minimum requirements of that written contract.

- C.75 An accredited person's consumer dashboard is an online service that can be used by each CDR consumer to manage consumer data requests¹²⁷ and consents for the accredited person to collect, use and disclose CDR data.
- C.76 The consumer dashboard should be provided to the CDR consumer as soon as practicable after the accredited person receives a valid request from that consumer for the collection and use of their CDR data.¹²⁸ This is so that the accredited data recipient can comply with its obligation under Privacy Safeguard 5 to notify of the collection of CDR data via the consumer's dashboard.¹²⁹
- C.77 The consumer dashboard must contain the following details of each consent that has been given by the CDR consumer:¹³⁰
- the CDR data to which the consents relate
 - for a use consent,¹³¹ the specific use or uses for which the consumer has given consent
 - the date on which the consumer gave the consents

¹²⁶ CDR Rules, subrule 1.14(5).

¹²⁷ See [Chapter B \(Key concepts\)](#).

¹²⁸ For further information regarding 'valid requests', see CDR Rules, rule 4.3 and [Chapter 3 \(Privacy Safeguard 3\)](#).

¹²⁹ Privacy Safeguard 5 requires an accredited person to notify the consumer of the collection of their CDR data by updating the consumer's dashboard as soon as practicable to include certain matters. For further information, see CDR Rules, rule 7.4 and [Chapter 5 \(Privacy Safeguard 5\)](#) of the CDR Privacy Safeguard Guidelines.

¹³⁰ CDR Rules, subrule 1.14(3).

¹³¹ Including a de-identification consent (as defined in CDR Rules, rule 1.10A) and a direct marketing consent for an accredited data recipient of particular CDR data to use that CDR data for the purposes of direct marketing (as per CDR Rules, rule 1.10A).

- whether the consents were for the collection of CDR data on a single occasion or over a period of time
- if the consumer consented to collection and/or disclosure of CDR data over a period of time – what that period is and how often data has been (and is expected to be) collected and/or disclosed over that period
- if the consents are current – when they will expire
- if the consents are not current – when they expired
- for an insight disclosure consent – a description of the CDR insight and to whom it was disclosed¹³²
- if a business consumer statement has been given in relation to the consent – that fact¹³³
- the information required to notify the consumer of the collection of their CDR data, being:
 - what CDR data was collected
 - when the CDR data was collected, and
 - the CDR participant of the CDR data that was collected¹³⁴
- the information required to notify the consumer of the disclosure of their CDR data to an accredited person, being:
 - what CDR data was disclosed
 - when the CDR data was disclosed, and
 - the accredited person to whom the CDR data was disclosed, identified in accordance with any entry on the Register of Accredited Persons specified as being for that purpose¹³⁵
- the information required to notify the consumer when their CDR data has been disclosed to a trusted adviser, being:
 - what CDR data was disclosed
 - when the CDR data was disclosed, and
 - who the trusted adviser was¹³⁶
- the information required to notify the consumer when a disclosure is made to a specified person under a business consumer disclosure consent, being:

¹³² CDR Rules, paragraph 1.14(3)(ea).

¹³³ CDR Rules, paragraph 1.14(3)(eb).

¹³⁴ Privacy Safeguard 5 requires an accredited person to notify the consumer of the collection of their CDR data by updating the consumer's dashboard to include certain matters. For further information, see CDR Rules, rule 7.4 and [Chapter 5 \(Privacy Safeguard 5\)](#).

¹³⁵ Privacy Safeguard 10 requires an accredited data recipient to notify the consumer of the disclosure of their CDR data by updating the consumer's dashboard to include certain matters. For further information, see CDR Rules, subrule 7.9(2) and [Chapter 10 \(Privacy Safeguard 10\)](#).

¹³⁶ CDR Rules, subrule 7.9(3).

- what CDR data was disclosed
 - when the CDR data was disclosed, and
 - the person to whom it was disclosed¹³⁷
 - the information required to notify the consumer when a CDR insight has been disclosed, being:
 - what CDR data was disclosed
 - when the CDR data was disclosed, and
 - the person to whom it was disclosed¹³⁸
 - where the accredited person is an affiliate¹³⁹ and the CDR data will be collected by a sponsor at its request under a sponsorship arrangement, the sponsor's name and accreditation number,¹⁴⁰ and
 - if applicable, details of each amendment that has been made to a consent.
- C.78 The consumer dashboard must also contain a statement that the CDR consumer is entitled to request further records in accordance with rule 9.5 of the CDR Rules (Request from CDR consumers for copies of records), and information about how to make such a request.¹⁴¹
- C.79 The consumer dashboard must have a functionality that allows the CDR consumer, at any time, to:¹⁴²
- withdraw each consent
 - elect for their CDR data be deleted once it becomes redundant, and
 - withdraw an election regarding whether their CDR data should be deleted once it becomes redundant.
- C.80 These functionalities must be simple and straightforward to use, and prominently displayed.¹⁴³

Tip: For best practice examples of how to present this information on the consumer dashboard, and other related recommendations, see the Consumer Experience Guidelines.

- C.81 The consumer dashboard may also include a functionality that allows a CDR consumer to amend an existing consent.¹⁴⁴

¹³⁷ CDR Rules, subrule 7.9(3A).

¹³⁸ CDR Rules, subrule 7.9(4).

¹³⁹ An affiliate is a person with sponsored accreditation who has entered into a sponsorship arrangement with another person with unrestricted accreditation (the 'sponsor'). See Chapter B for more information.

¹⁴⁰ CDR Rules, paragraph 1.14(3)(ha).

¹⁴¹ CDR Rules, subrule 1.14(3A).

¹⁴² CDR Rules, paragraph 1.14(1)(c).

¹⁴³ CDR Rules, paragraph 1.14(1)(c).

¹⁴⁴ See paragraphs C.32 to C.41 for information on amending consents.

- C.82 Data holders also have an obligation under the CDR Rules to offer, and in most circumstances provide, a consumer dashboard to a consumer when the data holder receives a consumer data request on behalf of the consumer by an accredited person.¹⁴⁵
- C.83 The data holder's consumer dashboard is used to manage the consumer's authorisations to disclose the consumer's CDR data to the accredited person.¹⁴⁶ For further information, see [Chapter B \(Key concepts\)](#) and the [Guide to privacy for data holders](#).

Consumers may withdraw consent

- C.84 A CDR consumer who has given a consent to an accredited person in relation to their CDR data may withdraw the consent at any time.¹⁴⁷
- C.85 An accredited person must allow a CDR consumer to withdraw each consent they have provided by:¹⁴⁸
- using the accredited person's consumer dashboard, or
 - using a simple alternative method of communication made available by the accredited person.¹⁴⁹
- C.86 The functionality to withdraw consent on the consumer dashboard must be simple and straightforward to use, and prominently displayed.¹⁵⁰
- C.87 The alternative method of communicating the withdrawal of consent must be simple.¹⁵¹ In addition, it:
- should be accessible and straightforward for a consumer to understand and use, and
 - may be written or verbal. Where it is written, the communication may be sent by electronic means (such as email) or non-electronic means (such as by post).
- C.88 An accredited person may wish to ensure its alternative method of communication is consistent with existing channels already made available to its customers,¹⁵² for example:

¹⁴⁵ Energy consumers may be eligible CDR consumers even if they do not have an online account with their retailer: see [Chapter B \(Key concepts\)](#) for further information. For eligible energy consumers without an online account, the retailer must offer the CDR consumer a dashboard and provide it if the CDR consumer accepts: CDR Rules, clause 2.3 of Schedule 4. For other CDR consumers, each data holder must provide a consumer dashboard: CDR Rules, rule 1.15.

¹⁴⁶ CDR Rules, rule 1.15.

¹⁴⁷ CDR Rules, rule 4.13.

¹⁴⁸ CDR Rules, rule 4.13. A consumer must be enabled by an accredited person to independently withdraw each type of consent. For example, where a consumer provided a collection consent and use consent, the consumer can choose to withdraw only the collection consent. See the Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020* at [7].

¹⁴⁹ Where the CDR consumer withdraws a consent that was originally given to a CDR representative, it is the CDR representative principal under the CDR representative arrangement that must allow the consumer to withdraw consent via their consumer dashboard, or by an alternative method made available by the CDR representative principal or CDR representative for that purpose (rule 4.20J).

¹⁵⁰ CDR Rules, paragraph 1.14(1)(c).

¹⁵¹ CDR Rules, subrule 4.13(1).

¹⁵² Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2020*.

- through its telephone helpline, or
 - in the case of direct marketing consents, through embedded links in any email communications that will allow a CDR consumer to notify the accredited person of their intention to ‘opt out’ of receiving direct marketing communications.¹⁵³
- C.89 Where an accredited person does not have a general policy of deleting redundant data, and the CDR consumer has not already requested that their redundant data be deleted, it should refer to the requirements in the Consumer Experience Standards.¹⁵⁴

Tip: For examples of how to implement the withdrawal functionality on the consumer dashboard, and best practice recommendations for how to do this, see the Consumer Experience Guidelines.

Effect of withdrawing consent

- C.90 The main consequence of the withdrawal of a consent is that the consent expires,¹⁵⁵ and the accredited person may no longer collect, use or disclose the CDR data (as applicable, depending on what category of consent has been withdrawn). Information about when a consent expires is contained in the following section.
- C.91 Where only a collection consent for particular CDR data is withdrawn, but other use consents,¹⁵⁶ and/or disclosure consents,¹⁵⁷ for that CDR data with the same accredited data recipient remain current, an accredited data recipient may continue to use and/or disclose the relevant CDR data.¹⁵⁸ For use consents in this situation, see 4.18A (for accredited persons) and 4.20Q (for CDR representatives) in relation to consumer notification requirements.
- C.92 Where a consent is withdrawn for an SR data request, the procedures and arrangements for withdrawal of consent in rule 4.18AA of the CDR Rules apply to the primary data holder as if it were the data holder for the SR data covered by that request.¹⁵⁹

¹⁵³ For information about the use and disclosure of CDR data for direct marketing, see [Chapter 7 \(Privacy Safeguard 7\)](#).

¹⁵⁴ The Consumer Experience Standards are available on the Consumer Data Standards website, consumerdatastandards.gov.au.

¹⁵⁵ CDR Rules, paragraphs 4.14(1)(a) and (1)(b).

¹⁵⁶ Including a de-identification consent (as defined in CDR Rules, rule 1.10A) and a direct marketing consent for an accredited data recipient of particular CDR data to use that CDR data for the purposes of direct marketing (as per CDR Rules, rule 1.10A).

¹⁵⁷ Including both an AP disclosure consent (as defined in CDR Rules, rule 1.10A) and a direct marketing consent for an accredited data recipient of particular CDR data to disclose that CDR data to another accredited person for the purposes of direct marketing: CDR Rules, paragraph 1.10A(1)(c)(ii).

¹⁵⁸ An accredited person may only collect CDR data in response to a ‘valid request’ from a consumer: Competition and Consumer Act, section 56EF. A request ceases to be ‘valid’ if the consumer withdraws their collection consent: CDR Rules, subrule 4.3(4). However, if the consumer does not also withdraw their use consent, the accredited person may continue to use the CDR data it has already collected to provide the requested goods or services: see the note under CDR Rules, subrule 4.3(4). See further CDR Rules, rule 4.18A for ongoing notification requirements in this circumstance. For further information, see [Chapter 3 \(Privacy Safeguard 3\)](#).

¹⁵⁹ CDR Rules, subrule 1.23(10). For more information on SR data, see [Chapter B \(Key Concepts\)](#).

- C.93 Where a CDR consumer withdraws each of their collection, use and disclosure consents, the CDR data is likely to become redundant data that the accredited person is required to delete or de-identify in accordance with Privacy Safeguard 12 (unless an exception applies).¹⁶⁰
- C.94 If a CDR consumer withdraws a consent using the accredited person’s consumer dashboard, the withdrawal is immediately effective.¹⁶¹
- C.95 If a withdrawal is communicated through a simple alternative method of communication, the accredited person must give effect to the withdrawal as soon as practicable, but not more than 2 business days after receiving the communication.¹⁶²
- C.96 The test of practicability is an objective test. In adopting a timetable that is ‘practicable’ an accredited person can take technical and resource considerations into account. However, the accredited person must be able to justify any delay in giving effect to the consumer’s communication of withdrawal.
- C.97 ‘Giving effect’ to the withdrawal includes updating the consumer dashboard to reflect that the consent has expired,¹⁶³ as required by rule 4.19 of the CDR Rules.¹⁶⁴
- C.98 Where a CDR consumer has elected for their CDR data to be deleted upon becoming redundant data, withdrawal of a consent will not affect this election.¹⁶⁵

Tip: For best practice examples of how to present this information on the consumer dashboard, and other related recommendations, see the Consumer Experience Guidelines.

When a consent expires

- C.99 Where a consent expires, the accredited person may no longer collect, use or disclose the CDR data (as applicable, depending on what category of consent has expired).

¹⁶⁰ More information on ‘redundant data’ and the requirement to destroy or de-identify redundant data is in [Chapter 12 \(Privacy Safeguard 12\)](#).

¹⁶¹ CDR Rules, paragraph 4.14(1)(b). The same occurs where a consent given to a CDR representative is withdrawn through the consumer dashboard provided by the CDR representative or CDR representative principal (rule 4.20K(1)(a)).

¹⁶² CDR Rules, paragraph 4.13(2)(a) and 4.14(1)(a). Similarly, where a simple alternative method of communication is used to notify a CDR representative or a CDR representative principal of the withdrawal of a consent, both must give effect to the withdrawal as soon as practicable and within 2 business days (subrules 4.20J(5) and (6)). They must also notify each other when one of them has received this withdrawal (subrule 4.20J(4)).

¹⁶³ See CDR Rules, paragraph 1.14(3)(g).

¹⁶⁴ CDR Rules, rule 4.19 requires an accredited person to update the consumer dashboard as soon as practicable after the information required to be contained on the dashboard changes. CDR Rules, rule 4.20T requires: the same of a CDR representative principal to make this update where the CDR consumer originally gave consent to a CDR representative, and for the CDR representative to notify the CDR representative principal after the information required to be contained on the CDR representative principal’s consumer dashboard changes.

¹⁶⁵ CDR Rules, subrule 4.13(3) provides that withdrawal of a consent does not affect an election under CDR Rules, rule 4.16 that the consumer’s collected CDR data be deleted once it becomes redundant. CDR Rules, rule 4.16 is discussed in [Chapter 12 \(Privacy Safeguard 12\)](#).

C.100 Where each of a CDR consumer's collection, use and disclosure consents expire, the CDR data is likely to become redundant data that the accredited person is required to delete or de-identify in accordance with Privacy Safeguard 12 (unless an exception applies).¹⁶⁶

C.101 For accredited persons, rule 4.14 of the CDR Rules provides that a consent expires in the following circumstances:¹⁶⁷

- **If the consent is withdrawn:** if a withdrawal notice is given via the consumer dashboard, the consent expires immediately.¹⁶⁸ Where withdrawal is not given through the consumer dashboard, the consent expires when the accredited person gives effect to the withdrawal, or 2 business days after receiving the communication, whichever is sooner.¹⁶⁹
- **At the end of the period of consent:** a consent expires at the end of the specified period for which the consumer gave the consent.¹⁷⁰ This specified period cannot be longer than 12 months for CDR consumers, and 7 years for CDR business consumers who give a business consumer statement.¹⁷¹
- **Twelve months (for CDR consumers) or 7 years (for CDR business consumers) after the consent was given or last amended:** a consent expires at the end of the period of 12 months (for CDR consumers) or 7 years (for CDR business consumers who give a business consumer statement) after:
 - the consent was given, or
 - if the duration of the consent has been amended, the consent was last amended.¹⁷²
- **For a collection consent, when the accredited person is notified:**
 - **by the data holder of the withdrawal of authorisation:** upon such notification, the consent expires immediately.¹⁷³
 - **by the accredited data recipient of the expiry of the AP disclosure consent:** upon such notification, the AP disclosure consent expires immediately.¹⁷⁴
- **For an AP disclosure consent, when the accredited data recipient is notified by the accredited person of the expiry of the collection consent:** upon such notification, the collection consent expires immediately.¹⁷⁵

¹⁶⁶ More information on 'redundant data' and the requirement to destroy or de-identify redundant data is in [Chapter 12 \(Privacy Safeguard 12\)](#).

¹⁶⁷ See rule 4.20K for equivalent provisions that relate to CDR representatives.

¹⁶⁸ CDR Rules, paragraph 4.14(1)(b).

¹⁶⁹ CDR Rules, paragraph 4.14(1)(a).

¹⁷⁰ CDR Rules, paragraph 4.14(1)(d).

¹⁷¹ CDR Rules, subrule 4.12(1) and (1A). CDR Rules, paragraph 4.14(1)(c) reinforces this maximum duration by providing that consent expires after the 12 month period after the consent was given.

¹⁷² CDR Rules, paragraph 4.14(1)(c) and 4.14(2).

¹⁷³ CDR Rules, subrule 4.14(3).

¹⁷⁴ CDR Rules, subrule 4.14(4).

¹⁷⁵ CDR Rules, subrule 4.14(4).

- **If the accredited person's accreditation is revoked or surrendered:** consent expires when the revocation or surrender takes effect.¹⁷⁶
- **If an accredited person becomes a data holder, rather than an accredited data recipient, of particular CDR data:** upon becoming a data holder,¹⁷⁷ all consents in relation to the particular CDR data expire.¹⁷⁸
- **If an affiliate ceases to have a registered sponsor:** upon an affiliate¹⁷⁹ ceasing to have a registered sponsor,¹⁸⁰ any collection consents for the affiliate expire (but any use or disclosure consents continue in effect).¹⁸¹ The affiliate would be required to notify a CDR consumer of this fact under rule 4.18A of the CDR Rules.
- **If another CDR Rule provides that a consent expires:**¹⁸² (there is only one applicable CDR Rule: CDR Rules, subrule 5.1B(6) in relation to affiliates.)

C.102 The expiry of a CDR consumer's collection consent does not automatically result in expiry of the use consent relating to any CDR data that has already been collected.¹⁸³

C.103 In light of this, where a CDR consumer's collection consent expires, but their use consent to provide the requested goods or services¹⁸⁴ remains current,¹⁸⁵ the accredited person must notify the consumer as soon as practicable that they may, at any time:¹⁸⁶

- withdraw the use consent, and
- make an election to delete redundant data in respect of that CDR data.¹⁸⁷

C.104 This notification must be given in writing (though not through the consumer's dashboard - although a copy of the notification may also be included in the consumer's dashboard).

C.105 This notification is important because where the collection consent expired as a result of the consumer's withdrawal, and the CDR consumer did not also withdraw their use consent, the

¹⁷⁶ CDR rules, subrule 4.14(6). A revocation or surrender takes effect when the fact that the accreditation has been revoked or surrendered is included in the Register of Accredited Persons: CDR Rules, rule 5.22. For further information, see the ACCC's Accreditation Guidelines.

¹⁷⁷ As a result of subsection 56AJ(4) of the Competition and Consumer Act and related clause 7.2 of Schedule 3 and 9.2 of Schedule 4.

¹⁷⁸ CDR Rules, subrule 4.14(5).

¹⁷⁹ An affiliate is a person with sponsored accreditation who has entered into a sponsorship arrangement with another person with unrestricted accreditation (the 'sponsor'). See [Chapter B \(Key concepts\)](#) for more information.

¹⁸⁰ For example, this would occur if the sponsorship arrangement between the sponsor and affiliate terminates.

¹⁸¹ CDR Rules, paragraph 4.14(1)(e) and subrule 5.1B(6).

¹⁸² CDR Rules, paragraph 4.14(1)(e).

¹⁸³ See the note under CDR Rules, subrule 4.3(4). See also the Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020* at [8].

¹⁸⁴ Being the goods or services requested under CDR Rules, subrule 4.3(1) as part of the valid request.

¹⁸⁵ For example, because the consumer withdraws only their collection consent.

¹⁸⁶ CDR Rules, rule 4.18A.

¹⁸⁷ See CDR Rules, rule 4.16.

accredited person may continue to use the CDR data it has already collected to provide the requested goods or services.¹⁸⁸ A consumer might not be aware of this.¹⁸⁹

Notification requirements

Notifications to consumers

C.106 The CDR Rules require an accredited person¹⁹⁰ to provide the following notifications to a CDR consumer about consents, collections and disclosures:

- **Notification following consent:** There is a requirement to provide a notice in the form of a CDR receipt to the CDR consumer after they provide, amend or withdraw a consent.¹⁹¹ The matters that must be included in the CDR receipt are outlined in rule 4.18 of the CDR Rules.¹⁹²
- **Ongoing notification for collection and use consents:** There is an ongoing notification requirement regarding the currency of the CDR consumer's collection and use consents. Rule 4.20 of the CDR Rules requires an accredited person to notify the consumer that their collection consent and/or use consent is still current where 90 days have elapsed since the latest of the following events:¹⁹³
 - the consumer consenting to the collection and/or use of their CDR data
 - the consumer last amending their collection and/or use consents
 - the consumer last using their consumer dashboard, or
 - the accredited person last sending the consumer a notification that their collection consent or use consent is still current.
- **Notification if collection consent expires:** Where a CDR consumer's collection consent expires, but their use consent to provide the requested goods or services remains current, the accredited person must notify the consumer of the matters in rule 4.18A of the CDR Rules as soon as practicable.¹⁹⁴

¹⁸⁸ See the note under CDR Rules, subrule 4.3(4).

¹⁸⁹ An accredited data recipient must also provide a statement in its CDR policy indicating the consequences to the consumer for withdrawing a consent to collect and use CDR data: CDR Rules, paragraph 7.2(4)(a).

¹⁹⁰ However, these notification requirements do not apply to an accredited person acting on behalf of a principal in its capacity as the provider of an outsourced service arrangement, in accordance with the arrangement, see CDR Rules, subrule 1.7(5). For information on 'CDR outsourcing arrangements', see [Chapter B \(Key concepts\)](#), 'Outsourced service provider'.

¹⁹¹ CDR Rules, subrule 4.18(1). A corresponding obligation applies to CDR representatives under CDR Rules, rule 4.20O.

¹⁹² CDR Rules, rule 4.18. A CDR receipt must be given in writing other than through the consumer dashboard (although a copy of the CDR receipt may be included in the consumer's consumer dashboard). For more information, see CDR Rules, rule 4.18.

¹⁹³ CDR Rules, subrules 4.20(3) and (4) state that this notification must be given in writing otherwise than through the consumer's consumer dashboard, however a copy may be included on the consumer dashboard. Corresponding obligations apply to CDR representatives under CDR Rules, rule 4.20U.

¹⁹⁴ CDR Rules, rule 4.18A. For further information on when a consent expires, see paragraphs C.99 to C.105. Corresponding obligations apply to CDR representatives under CDR Rules, rule 4.20Q.

- **Notification of collection:** There is a requirement to notify the CDR consumer of the collection of their CDR data as soon as practicable after the collection of CDR data.¹⁹⁵
- **Notification of disclosure:** There is requirement to notify the CDR consumer of the disclosure of their CDR data to an accredited person as soon as practicable after the disclosure of the CDR data.¹⁹⁶
- **Updating the consumer's dashboard:** There is a general obligation to update the CDR consumer's dashboard as soon as practicable after the information required to be contained on the consumer dashboard changes.¹⁹⁷

C.107 Data holders also have a general obligation under the CDR Rules to update the CDR consumer's consumer dashboard as soon as practicable, where there is a change in the information required for that dashboard.¹⁹⁸ In addition, data holders must notify the consumer of the disclosure of their CDR data as soon as practicable after the disclosure of CDR data.¹⁹⁹

Notifications to CDR participants

C.108 An accredited person must provide the following notifications about consents to CDR participants under the CDR Rules:

- **Notification to accredited data recipient if collection consent expires:** Where a CDR consumer's collection consent expires, and an accredited person has made a consumer data request to an accredited data recipient based on that collection consent, and the request has not been completely resolved, the accredited person must notify that accredited data recipient of the CDR data, as soon as practicable.²⁰⁰
- **Notification to data holder if collection consent expires:** Where a CDR consumer's collection consent expires, and an accredited person has made a consumer data request to a data holder based on that collection consent, and the request has not been completely

¹⁹⁵ Privacy Safeguard 5 requires an accredited data recipient to notify the consumer of the collection of their CDR data by updating the consumer's consumer dashboard to include certain matters. For further information, see CDR Rules, rule 7.4 and [Chapter 5 \(Privacy Safeguard 5\)](#).

¹⁹⁶ Privacy Safeguard 10 requires an accredited data recipient to notify the consumer of the disclosure of their CDR data to an accredited person by updating the consumer's consumer dashboard to include certain matters. For further information, see CDR Rules, subrules 7.9(2), 7.9(3) and 7.9(4) and [Chapter 10 \(Privacy Safeguard 10\)](#). Subrule 7.9(5) also requires a CDR representative principal to notify a CDR consumer where its CDR representative discloses the CDR consumer's CDR data.

¹⁹⁷ CDR Rules, rule 4.19.

¹⁹⁸ CDR Rules, rule 4.27.

¹⁹⁹ Privacy Safeguard 10 requires a data holder to notify the consumer of the collection of their CDR data by updating the consumer's consumer dashboard to include certain matters. For further information, see CDR Rules, rule 7.9 and [Chapter 10 \(Privacy Safeguard 10\)](#).

²⁰⁰ CDR Rules, subrule 4.18AA(2)(b). Where consent expires that was originally given to a CDR representative, it is the CDR representative principal under the CDR representative arrangement who must notify the accredited data recipient of the expiry of consent. See CDR Rules, subrule 4.18B(2) and rule 4.20P.

resolved, the accredited person must notify that data holder of the withdrawal in accordance with the data standards.²⁰¹

- **Notification if collection consent is amended:** Where a CDR consumer amends their collection consent, and the accredited person has made a consumer data request based on that collection consent, and the request has not been completely resolved, the accredited person must notify the relevant CDR participant/s that the consent has been amended, in accordance with rule 4.18C of the CDR Rules.²⁰²
- **Notification if AP disclosure consent expires:** Where a CDR consumer's AP disclosure consent expires, and an accredited person has made a consumer data request to an accredited data recipient on behalf of a CDR representative that has not been completely resolved, the accredited person must notify the accredited data recipient to whom the data is being disclosed to, as soon as practicable.²⁰³

Authorisation

C.109 Before an accredited person can receive a CDR consumer's CDR data from a data holder, the consumer must authorise the data holder to disclose the particular data to that accredited person.

C.110 After receiving a CDR consumer data request, the data holder must seek the consumer's authorisation for required or voluntary consumer data in accordance with Division 4.4 of the CDR Rules and the data standards,²⁰⁴ unless an exception applies.²⁰⁵

C.111 For requests that relate to joint accounts, in some cases, the data holder might need to seek an 'approval' from other joint account holders, in addition to the authorisation provided by the requesting CDR consumer.²⁰⁶

C.112 Once a data holder has received this authorisation it:

- must disclose the required consumer data, and
- may disclose the relevant voluntary consumer data

²⁰¹ CDR Rules, subrule 4.18AA(2)(a). Where consent expires that was originally given to a CDR representative, it is the CDR representative principal under the CDR representative arrangement who must notify the data holder of the expiry of consent. See CDR Rules, rule 4.20P.

²⁰² For further information on the requirements under CDR Rules, rule 4.18C, see paragraph C.39. Where consent is amended that was originally given to a CDR representative, it is the CDR representative principal under the CDR representative arrangement who must notify the relevant CDR participant that the consent has been amended. See CDR Rules, rule 4.20S.

²⁰³ CDR Rules, subrules 4.18B(3) and 4.20R(3).

²⁰⁴ See CDR Rules, rule 4.5.

²⁰⁵ See CDR Rules, rule 4.7.

²⁰⁶ See CDR Rules, subdivision 4A.3.2, which sets out how consumer data requests to data holders that relate to joint accounts are handled in the CDR system.

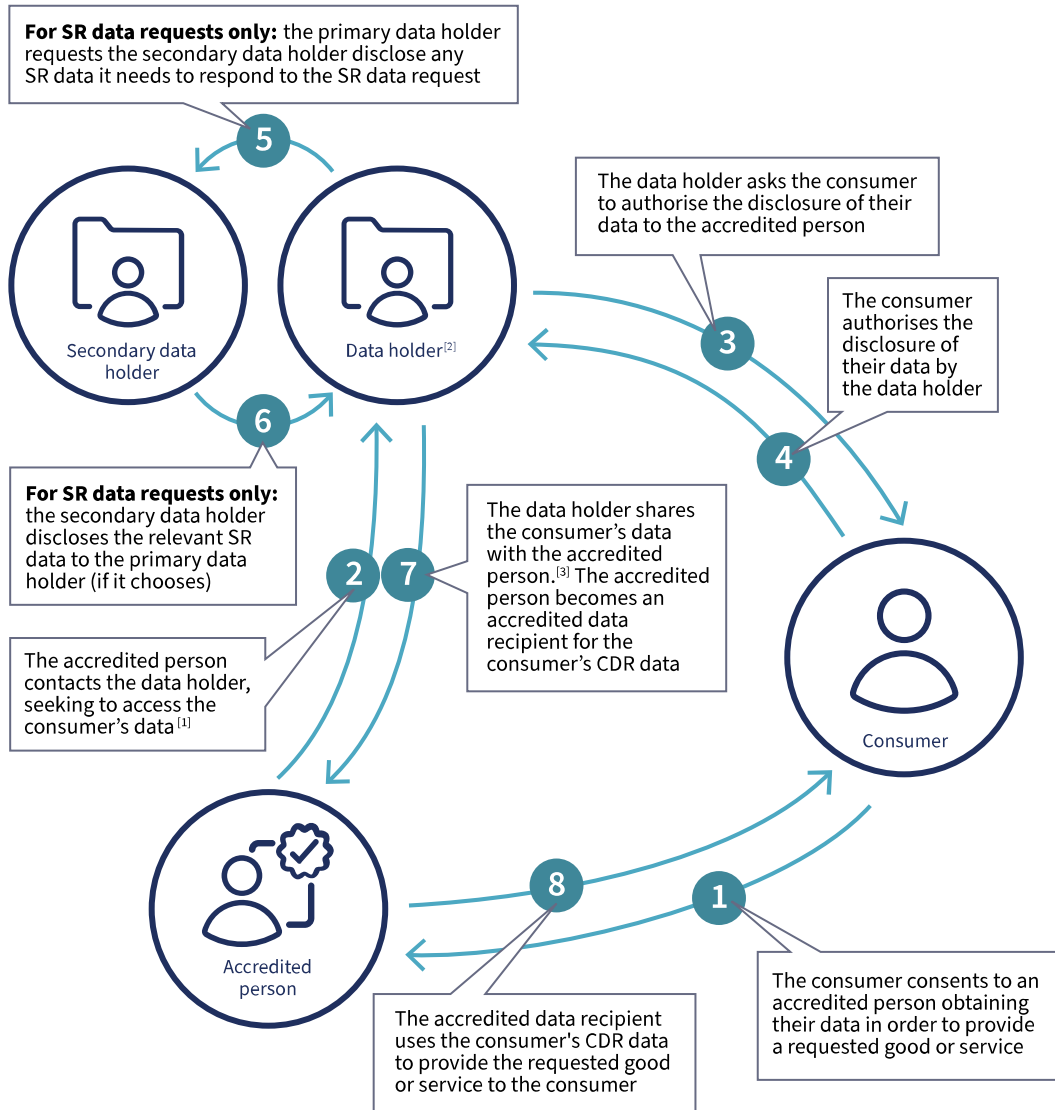
through its accredited person request service and in accordance with the data standards, unless an exception applies.²⁰⁷

- C.113 The flow charts below demonstrate the role of authorisation in the key information flow between a CDR consumer, accredited person and data holder.
- C.114 If the consumer data request relates to SR data, the primary data holder must request that the secondary data holder provide it with the SR data, so the primary data holder can disclose that SR data to the relevant accredited person.²⁰⁸ Currently, the energy sector is the only CDR sector with a secondary data holder (AEMO) and SR data.
- C.115 For further information on a data holder's authorisation obligations, see the [Guide to privacy for data holders](#).

²⁰⁷ See CDR Rules, rule 4.6A.

²⁰⁸ It is not mandatory for the secondary data holder to disclose the requested SR data to the primary data holder: CDR Rules, subrule 1.22(4). However, if a secondary data holder chooses not to disclose the requested SR data to the primary data holder, it must notify the primary data holder of its refusal: CDR Rules, subrule 1.22(5). For more information on SR data and primary data holders, see [Chapter B \(Key Concepts\)](#).

Overview: key information flow in the CDR system

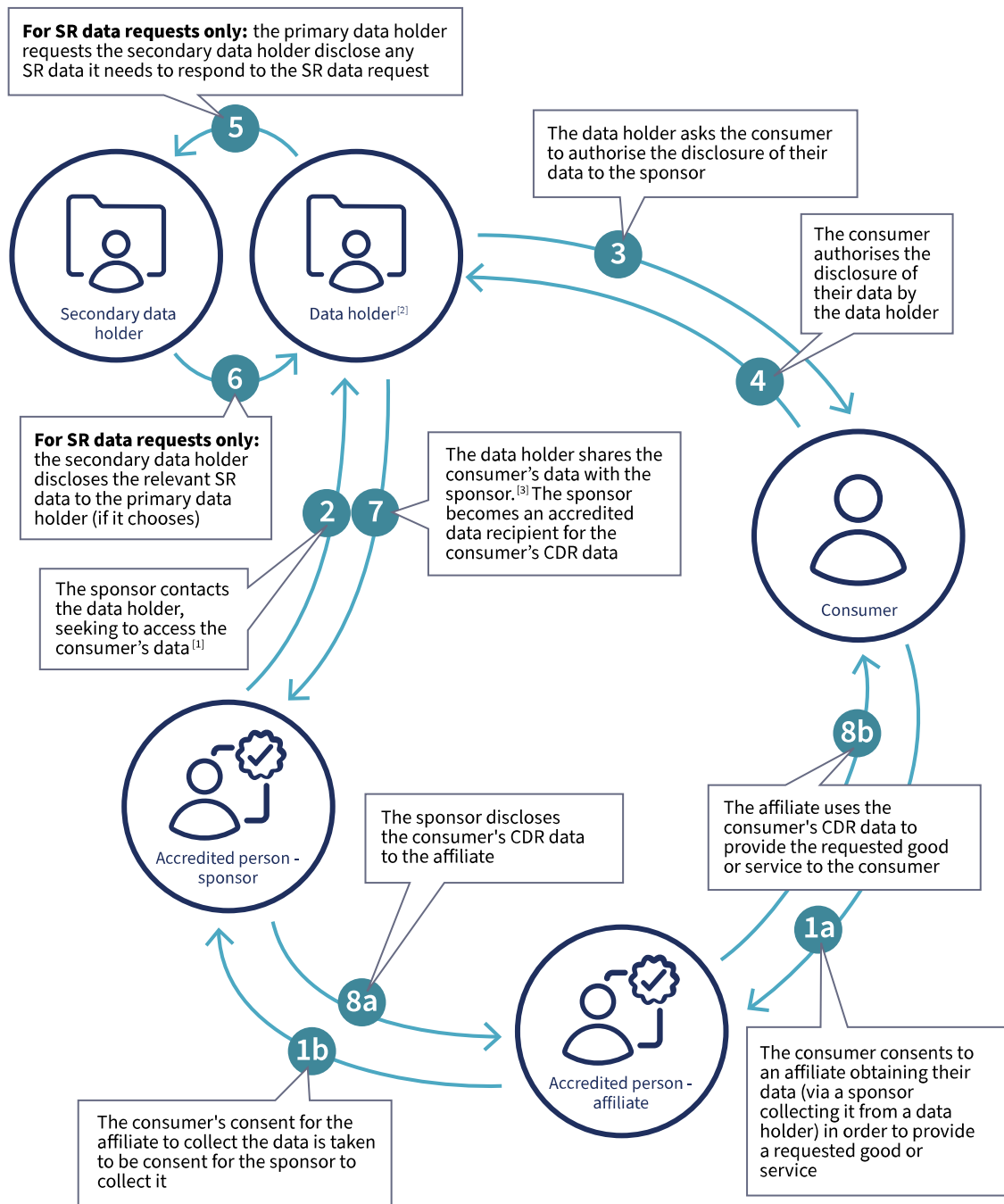


[1] If the accredited person is seeking CDR data that is or includes SR (shared responsibility) data, it contacts the primary data holder (rather than the secondary data holder)

[2] For SR data requests, this will be the primary data holder

[3] Where the data holder is a primary data holder and the secondary data holder has refused to disclose SR data to it, the primary data holder will not be able to share that SR data with the accredited person

Overview: key information flow for collection by sponsors

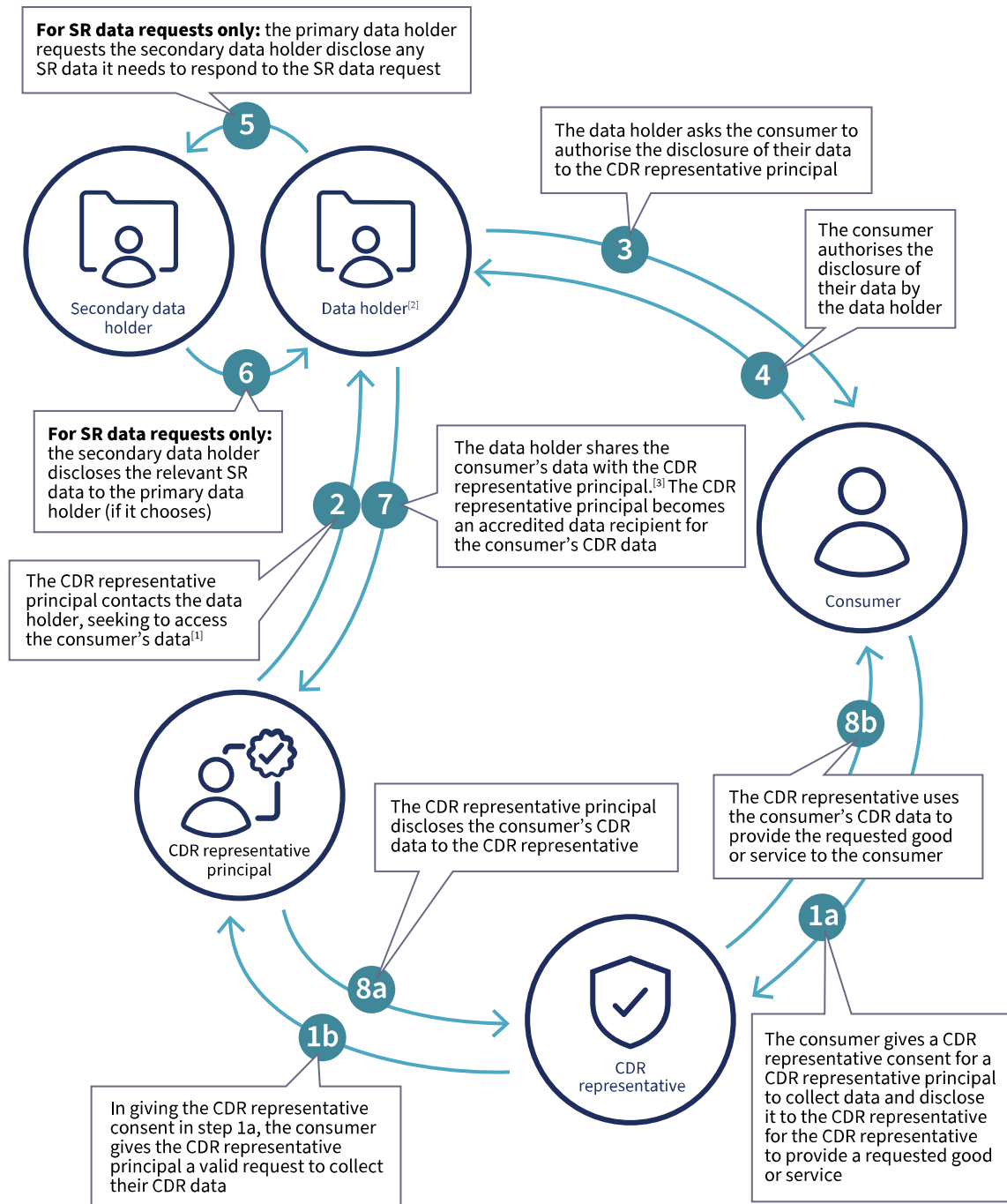


[1] If the sponsor is seeking CDR data that is or includes SR (shared responsibility) data, it contacts the primary data holder (rather than the secondary data holder)

[2] For SR data requests, this will be the primary data holder

[3] Where the data holder is a primary data holder and the secondary data holder has refused to disclose SR data to it, the primary data holder will not be able to share that SR data with the sponsor


Overview: key information flow for CDR representative arrangements



[1] If the CDR representative principal is seeking CDR data that is or includes SR (shared responsibility) data, it contacts the primary data holder (rather than the secondary data holder)

[2] For SR data requests, this will be the primary data holder

[3] Where the data holder is a primary data holder and the secondary data holder has refused to disclose SR data to it, the primary data holder will not be able to share that SR data with the CDR representative principal



Chapter 1:

Privacy Safeguard 1 —

Open and transparent management of CDR data

Version 5.0, November 2023

Contents

Key points	3
What does Privacy Safeguard 1 say?	3
Importance of open and transparent management of CDR data and having a CDR policy	3
Who Privacy Safeguard 1 applies to	4
How Privacy Safeguard 1 interacts with the Privacy Act	5
Implementing practices, procedures and systems to ensure compliance with the CDR system	7
Circumstances that affect reasonable steps	8
Existing privacy governance arrangements	12
Have a CDR data management plan	12
A suggested approach to compliance with Privacy Safeguard 1	12
Having a CDR policy	16
Information that must be included in a CDR policy	17
Availability of the CDR policy	21
Consumer requests for a CDR policy	21
Interaction between an entity’s privacy policy and CDR policy	22

Key points

- Privacy Safeguard 1,¹ together with consumer data rule (CDR Rule) 7.2 and the Competition and Consumer Regulations, outlines the requirements for all consumer data right (CDR) entities (accredited persons who are or who may become an accredited data recipient of CDR data, data holders, and designated gateways) to manage CDR data in an open and transparent way.
- All CDR entities must take steps as are reasonable in the circumstances to implement practices, procedures and systems that will ensure they comply with the CDR system, and deal with related inquiries and complaints from consumers.
- All CDR entities must have a clearly expressed and up-to-date policy about how they manage CDR data (CDR policy). The CDR policy must be provided free of charge and made available in accordance with the CDR Rules.
- The Australian Energy Market Operator Limited (AEMO) is not subject to Privacy Safeguard 1 in its capacity as a data holder.² Accordingly, unless otherwise indicated, references in this chapter to data holders and CDR entities exclude AEMO.

What does Privacy Safeguard 1 say?

1.1 Privacy Safeguard 1 requires all CDR entities to:

- take steps that are reasonable in the circumstances to implement practices, procedures and systems that ensure compliance with the CDR system, including the privacy safeguards and CDR Rules, and
- have a clearly expressed and up-to-date CDR policy describing how they manage CDR data. The policy must be available free of charge and in a form consistent with the CDR Rules and provided to the consumer upon request.

Importance of open and transparent management of CDR data and having a CDR policy

1.2 The objective of Privacy Safeguard 1 is to ensure CDR entities manage CDR data in an open and transparent way. It is the bedrock principle.

1.3 By complying with Privacy Safeguard 1, CDR entities will be establishing accountable and auditable practices, procedures and systems that will assist with compliance with all the other privacy safeguards. This leads to a trickle-down effect where privacy is automatically considered when handling CDR data, resulting in better overall privacy management, practice and compliance through a 'privacy-by-design' approach.

¹ Competition and Consumer Act, section 56ED.

² Competition and Consumer Regulations, paragraph 28RA(2)(a)(i). For information about how Privacy Safeguard 1 applies to retailers who receive CDR data from AEMO, see paragraph 1.7.

- 1.4 It is also important that consumers are aware of how their CDR data is handled, and can inquire or make complaints to resolve their concerns. A CDR policy achieves this transparency by outlining how the CDR entity manages CDR data, and by providing information on how a consumer can complain and how the CDR entity will deal with a complaint.
- 1.5 CDR policies are also a key tool for ensuring open and transparent management of CDR data which can build trust and engage consumers in the management of their data.

Who Privacy Safeguard 1 applies to

- 1.6 Privacy Safeguard 1 applies to data holders, designated gateways and accredited persons, who are or who may become accredited data recipients of CDR data.³
- 1.7 Privacy Safeguard 1 does not apply to AEMO in its capacity as a data holder.⁴ Instead, data holders that are retailers in the energy sector (primary data holders) must comply with Privacy Safeguard 1 in relation to CDR data held by AEMO, that AEMO discloses to them under the *Competition and Consumer Act 2010* (Competition and Consumer Act).⁵ This obligation applies alongside retailers' Privacy Safeguard 1 obligations in respect of their own data holdings.

Note: *There are currently no designated gateways in the banking sector or energy sector.*⁶ See Chapter B (Key concepts) for the meaning of designated gateway.

- 1.8 As a non-accredited entity, a CDR representative is not directly bound by Privacy Safeguard 1. However, under the terms of the CDR representative arrangement with their CDR representative principal,⁷ a CDR representative is required to adopt and comply with their CDR representative principal's CDR policy in relation to service data.⁸ A CDR representative principal must ensure the CDR representative complies with the requirements of the CDR representative arrangement, and is liable if the CDR representative breaches any of the CDR representative arrangement provisions which are required by the CDR Rules (including the requirement to adopt and comply with their CDR representative principal's CDR policy).⁹

³ An accredited person will be an 'accredited person ... who may become an accredited data recipient' when they are seeking to collect CDR data. This means that an accredited person must ensure that they comply with their Privacy Safeguard 1 obligations before they seek to collect CDR data.

⁴ Competition and Consumer Regulations, paragraph 28RA(2)(a)(i).

⁵ Competition and Consumer Regulations, paragraph 28RA(3)(a).

⁶ For the banking sector, see the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019. For the energy sector, the energy designation specifies AEMO as a gateway for certain information: subsection 6(4) of the Consumer Data Right (Energy Sector) Designation 2020. However, at the time of publication, AEMO is not a designated gateway for any CDR data because under current CDR Rules, no CDR data is (or is to be) disclosed to AEMO because of the reasons in paragraph 56AL(2)(c) of the Competition and Consumer Act.

There are also no designated gateways in the telecommunications sector, although unlike the banking and energy sectors, at the date of publication of these guidelines, there are no rules allowing for the sharing of designated telecommunications data under the CDR system: Consumer Data Right (Telecommunications Sector) Designation 2022.

⁷ A CDR representative arrangement is a written contract between a CDR representative and their CDR representative principal that meets the minimum requirements listed in CDR Rules, subrules 1.10AA(1), (3) and (4).

⁸ CDR Rules, paragraph 1.10AA(4)(f). Note that a CDR representative will also have obligations under APP 1 (open and transparent management of personal information) if they are an APP entity.

⁹ CDR Rules, rule 1.16A.

- 1.9 Where they are a non-accredited entity, an outsourced service provider (OSP) is not directly bound by Privacy Safeguard 1. However, under the terms of the CDR outsourcing arrangement with their OSP principal,¹⁰ an OSP is required to comply with the OSP principal's CDR policy as it relates to deletion and de-identification of CDR data and the treatment of redundant or de-identified CDR data.¹¹ An OSP chain principal must ensure its direct and indirect OSPs (or those of its CDR representatives) comply with the requirements of the CDR outsourcing arrangement. Further, the OSP chain principal is liable if one of those entities breaches any of the CDR outsourcing arrangement provisions which are required by the CDR Rules (including the requirement to comply with the OSP principal's CDR policy as it relates to deletion and de-identification of CDR data and the treatment of redundant or de-identified CDR data).¹²

How Privacy Safeguard 1 interacts with the Privacy Act

- 1.10 It is important to understand how Privacy Safeguard 1 interacts with the *Privacy Act 1988* (the Privacy Act) and APP 1.¹³
- 1.11 APP 1 requires APP entities to manage personal information in an open and transparent way (see APP Guidelines, [Chapter 1 \(APP 1\)](#)).

CDR entity	Privacy protections that apply in the CDR context
Accredited person who may become an accredited data recipient	<p>Privacy Safeguard 1</p> <p>When an accredited person is planning to handle a CDR consumer's CDR data, and may become an accredited data recipient of that CDR data (for example, because they are seeking to collect it), Privacy Safeguard 1 applies.</p> <p>APP 1 does not apply to the accredited person in relation to that CDR data.¹⁴</p>

¹⁰ A CDR outsourcing arrangement is a written contract between an OSP principal and their provider that meets the minimum requirements listed in CDR Rules, subrule 1.10(3).

¹¹ CDR Rules, paragraph 1.10(3)(b)(i)(A).

¹² CDR Rules, rule 1.16.

¹³ The Privacy Act includes 13 APPs that regulate the handling of personal information by APP entities. See APP Guidelines, [Chapter B \(Key concepts\)](#) for further information.

¹⁴ See Competition and Consumer Act, subsections 56EC(4) and 56ED(1).

Note: If Privacy Safeguard 1 does not apply, APP 1 may continue to apply to other open and transparent management of the individual's personal information where the accredited person is an APP entity (see Competition and Consumer Act, subsection 56EC(4) and paragraph 56EC(5)(aa)). Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See Privacy Act, subsection 6E(1D).

CDR entity	Privacy protections that apply in the CDR context
Accredited data recipient	<p>Privacy Safeguard 1</p> <p>An accredited data recipient of a consumer’s CDR data must comply with Privacy Safeguard 1 in relation to the management of that CDR data.</p> <p>APP 1 does not apply to the accredited data recipient in relation to that CDR data.¹⁵</p>
Designated gateway	<p>APP 1 and Privacy Safeguard 1</p> <p>A designated gateway must comply with:</p> <ul style="list-style-type: none"> • Privacy Safeguard 1 in relation to the handling of CDR data, and • APP 1 in relation to the handing of personal information (if they are an APP entity). <p>As the obligations in Privacy Safeguard 1 apply generally to an entity’s handling of data, a designated gateway must have systems, practices and procedures to comply with both the privacy safeguards and the APPs (including having both a CDR policy and a privacy policy in place).</p>
Data holder (other than AEMO)	<p>APP 1 and Privacy Safeguard 1</p> <p>A data holder must comply with:</p> <ul style="list-style-type: none"> • Privacy Safeguard 1 in relation to the handling of CDR data, and • APP 1 in relation to the handing of personal information (if they are an APP entity). <p>This means that a data holder must have systems, practices and procedures to comply with both the privacy safeguards and the APPs (including having both a CDR policy and a privacy policy in place).¹⁶</p>
Data holder (AEMO)	<p>APP 1</p> <p>Privacy Safeguard 1 does not apply to AEMO as a data holder.¹⁷ AEMO must comply with APP 1 in relation to the handling of personal information. This means that AEMO must have systems, practices and procedures to comply with the APPs (including having a privacy policy in place).</p>

¹⁵ The APPs do not apply to an accredited data recipient of the CDR data in relation to the CDR data (Competition and Consumer Act, paragraph 56EC(4)(a)). However, this does not affect how the APPs apply to accredited persons in relation to the open and transparent management of the individual’s other personal information outside the CDR system. It also does not affect how the APPs apply to CDR data where the accredited person does not become an accredited data recipient of the CDR data (see Competition and Consumer Act, subsection 56EC(4) and paragraph 56EC(5)(aa)). Note: Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See Privacy Act, subsection 6E(1D).

¹⁶ See section 56AJ of the Competition and Consumer Act for the meaning of data holder.

¹⁷ Competition and Consumer Regulations, paragraph 28RA(2)(a)(i).

Implementing practices, procedures and systems to ensure compliance with the CDR system

- 1.12 Privacy Safeguard 1 requires all CDR entities to take steps that are reasonable in the circumstances to implement practices, procedures and systems that:
- ensure compliance with the CDR system, including the privacy safeguards and the CDR Rules, and
 - enable the entity to deal with inquiries or complaints from consumers about the entity's compliance with the CDR system, including the privacy safeguards and CDR Rules.¹⁸
- 1.13 This is a distinct and separate obligation upon a CDR entity, in addition to being a general statement of its obligation to comply with the CDR system.
- 1.14 The CDR Rules contain several governance mechanisms, policies and procedures that will assist entities to take steps that are reasonable in the circumstances to comply with the CDR system.¹⁹ Compliance with the mandatory CDR Rules will assist entities to take steps that are reasonable but does not, of itself, demonstrate compliance with Privacy Safeguard 1.
- 1.15 To comply with Privacy Safeguard 1, CDR entities need to proactively consider, plan and address how to implement any practices, procedures and systems under the privacy safeguards and the CDR Rules (including how these interact with other obligations). This will assist CDR entities to manage CDR data in an open and transparent way, in accordance with the object of Privacy Safeguard 1.²⁰
- 1.16 Compliance with Privacy Safeguard 1 should therefore be understood as a matter of good governance.

Risk point: Entities who implement the requirements of the privacy safeguards and the CDR Rules in isolation or at a late stage risk incurring unnecessary costs, and/or implementing inadequate solutions that fail to address the full compliance picture.

Privacy tip: Entities should take a 'privacy-by-design' approach in relation to handling CDR data across and within their organisation.²¹ This ensures CDR requirements are considered holistically. A tool that may assist an entity in this regard is the CDR data management plan,

¹⁸ A CDR representative principal is responsible for dispute resolution in relation to its CDR representatives. Consumers may however complain directly to the CDR representative about that CDR representative's provision of goods or services. Such complaints will trigger the CDR representative principal's internal dispute resolution obligations in the CDR Rules, paragraph 5.12(1)(b).

¹⁹ For example, accredited persons/accredited data recipients are required to establish a formal governance framework for managing information security risks. See Privacy Safeguard 12, CDR Rules, rules 5.12 and 7.11 and Schedule 2 to the CDR Rules. For further information see [Chapter 12 \(Privacy Safeguard 12\)](#) and the ACCC's Supplementary Accreditation Guidelines on Information Security available on the ACCC's Accreditation Guidelines page.

²⁰ Competition and Consumer Act, subsection 56ED(1).

²¹ For further information on 'privacy by design', see OAIC Privacy by Design Guidance, <https://www.oaic.gov.au/privacy/privacy-for-organisations/privacy-by-design>.

as outlined in paragraphs 1.33 to 1.36. The OAIC's suggested approach to compliance with Privacy Safeguard 1 in paragraphs 1.37 to 1.46 may also be of assistance.

Circumstances that affect reasonable steps

- 1.17 The requirement under Privacy Safeguard 1 to implement practices, procedures and systems is qualified by a 'reasonable steps' test.
- 1.18 This requires an objective assessment of what is considered reasonable in the specific circumstances, which could include:
- the CDR Rules and other legislative obligations that apply to the CDR entity
 - the nature of the CDR entity
 - whether the CDR entity is handling, or will soon handle, CDR data
 - the amount of CDR data handled by the CDR entity
 - the possible adverse consequences for a consumer in the case of a breach, and
 - the practicability, including time and cost involved.

The CDR system obligations that apply to the CDR entity

- 1.19 The CDR system obligations (such as the privacy safeguards and the CDR Rules) that apply to the entity will be relevant to determining what steps will be reasonable for compliance with Privacy Safeguard 1.
- 1.20 For example, the obligations that apply to accredited persons/accredited data recipients are often different to those that apply to data holders and will therefore require the development and implementation of different practices, procedures and systems to achieve compliance.
- 1.21 Further, where an entity participates in the CDR system in more than one capacity (e.g. as a data holder and an accredited person), this will also affect what constitutes reasonable steps, and the entity will need to put in place mechanisms to ensure it complies with the CDR system in all its different CDR entity capacities.

Examples of key CDR system privacy obligations

The CDR system imposes a range of privacy obligations upon CDR entities. Some of these privacy obligations apply to all CDR entities, while other privacy obligations apply only to a particular entity type. Entities will need to ensure that all of the relevant obligations that apply to them are considered when deciding on the steps to be taken in relation to Privacy Safeguard 1.

For example, an accredited data recipient of CDR data must comply with the privacy safeguards in relation to the CDR data.

However, a data holder needs to comply with the APPs in relation to CDR data that is also personal information with the exception of APPs 10 and 13, which are replaced by Privacy Safeguards 11 and 13 once the data holder is required or authorised to disclose the CDR data under the CDR Rules. Data holders must also comply with both Privacy Safeguard 1 and APP

1, as well as Privacy Safeguard 10.²² Information regarding compliance with each of the privacy safeguards is available in the relevant chapters of these [Guidelines](#).

In addition to obligations under the privacy safeguards, accredited persons/accredited data recipients and data holders must also consider their obligations in the CDR Rules for the purposes of compliance with Privacy Safeguard 1. These obligations will need to be reflected in the steps taken under Privacy Safeguard 1. For example:

- Accredited persons/accredited data recipients have obligations to report regularly regarding their ongoing information security obligations,²³ including privacy and security training to staff.²⁴
- Data holders have obligations relating to consumer data request services.²⁵
- Both accredited data recipients and data holders have obligations to provide CDR consumers with access to copies of records upon request.²⁶
- Accredited persons who are CDR representative principals have an obligation to ensure their CDR representative complies with the requirements of the CDR representative arrangement.²⁷
- Accredited persons who are:
 - chain principals of direct or indirect OSPs, or
 - CDR representative principals of CDR representatives who are chain principals of direct or indirect OSPs,
 - must ensure the OSPs comply with their requirements under their CDR outsourcing arrangements.²⁸
- Primary data holders have obligations to only use or disclose SR (shared responsibility) data received from a secondary data holder for the purpose of responding to the relevant SR data request.²⁹

²² Privacy Safeguard 10 does not have an APP equivalent.

²³ CDR Rules, Part 2 of Schedule 1. For further information, see the ACCC's Supplementary Accreditation Guidelines on Information Security available on the ACCC's Accreditation Guidelines page.

²⁴ Accredited persons/accredited data recipients must ensure all users undergo mandatory security and privacy training prior to interacting with the CDR data environment, with 'refresher courses' provided at least annually: see Privacy Safeguard 12, CDR Rules, rule 5.12 and Part 2 of Schedule 2. For further information, see the ACCC's Supplementary Accreditation Guidelines on Information Security available on the ACCC's Accreditation Guidelines page.

²⁵ For further information on consumer data request services, authorisation, disclosure of CDR data and a data holder's privacy obligations more generally, see the [Guide to privacy for data holders](#).

²⁶ CDR Rules, rule 9.5. Accredited data recipients and data holders are required to keep and maintain certain records as outlined in CDR Rules, rule 9.3. They are also required to comply with the reporting requirements in CDR Rules, rule 9.4.

²⁷ CDR Rules, rule 1.16A.

²⁸ CDR Rules, rule 1.16.

²⁹ CDR Rules, rule 1.24. See [Chapter B \(Key concepts\)](#) for additional information about primary data holders and SR data. See definition of 'primary data holder' and 'SR data' in CDR Rules, subrule 1.7(1).

- Primary data holders have obligations to destroy unsolicited SR data received from a secondary data holder as soon as practicable, unless the primary data holder is required to retain that SR data by or under an Australian law or a court/tribunal order.³⁰
- In the banking sector, both accredited persons and data holders must have internal dispute resolution processes that meet the requirements under the Australian Securities and Investments Commission’s [Regulatory Guide 271](#) on internal dispute resolution, as specified in subclause 5.1(1) of Schedule 3.³¹
- In the energy sector:³²
 - accredited persons (other than an accredited person who is also a retailer) must have internal dispute resolution processes that meet the requirements under the Australian Securities and Investments Commission’s [Regulatory Guide 271](#) on internal dispute resolution, as specified in subclause 5.1(1) of Schedule 4, and
 - retailers (including retailers that are also an accredited person) must have internal dispute resolution processes that satisfy the applicable requirements for the retailer’s standard complaints and dispute resolution procedures under the National Energy Retail Law or the Energy Retail Code (Victoria).

Privacy tip: A CDR representative principal is required by rule 1.16A in the CDR Rules to ensure that their CDR representative complies with the requirements of the CDR representative arrangement, and complies with Division 4.3A (Giving and amending consent – CDR representatives).³³ As part of discharging this obligation, a CDR representative principal could consider:

- undertaking review and assurance activities at least annually
- requiring the CDR representative to provide regular reports against its compliance with the written contract, and/or
- providing the CDR representative with any appropriate assistance or training in technical and compliance matters.

Prior to entering the written contract, it would be appropriate for the CDR representative

³⁰ CDR Rules, rule 1.25. See [Chapter B \(Key concepts\)](#) for additional information about primary data holders and SR data.

³¹ See CDR Rules, subrule 5.12(1) (for accredited persons), rule 6.1 (for data holders) and clause 5.1 of Schedule 3 (for accredited persons and data holders).

³² See CDR Rules, subrule 5.12(1) (for accredited persons), rule 6.1 (for data holders) and clause 5.1 of Schedule 4 of the CDR Rules (for accredited persons and data holders).

³³ CDR Rules, subrule 1.16A(1) requires a CDR representative principal to ensure the CDR representative complies with all requirements under the CDR representative arrangement. Under CDR Rules, subrule 1.16A(2), a CDR representative principal is in breach if the CDR representative fails to comply with a provision of the CDR representative arrangement which is required by r 1.10AA to be part of that arrangement, or seeks a use or disclosure consent, or makes a use or disclosure, in circumstances where the CDR representative arrangement does not provide for the CDR representative to do that thing. CDR Rules, subrule 1.16A(3) requires a CDR representative principal to ensure the CDR representative complies with Division 4.3(A), and the CDR representative principal breaches subrule 1.16A(4) if the CDR representative fails to comply.

principal to make enquiries of the proposed CDR representative, with a focus on their personal information handling capabilities, procedures and practices.

Taking these steps may assist the CDR representative principal in avoiding a breach of CDR Rule 1.16A, and in doing so, may also assist the CDR representative principal in avoiding a breach of other privacy-related CDR Rules (given the CDR representative principal is liable for the actions of the CDR representative).

Nature of the entity

- 1.22 The size of the CDR entity, its resources, the complexity of its operations and the business model are all relevant to determining what steps would be reasonable when putting in place practices, procedures and systems.
- 1.23 For instance, where a CDR entity uses OSPs, the reasonable steps it should take may be different to those it would take if it did not operate in this manner.

Handling of CDR data

- 1.24 In some cases, there may be a period of time in between a CDR entity becoming accredited and actively taking steps to handle CDR data. To meet the reasonable steps requirement, a CDR entity will be expected to be more advanced in its preparations under Privacy Safeguard 1 as it approaches the milestone of handling CDR data.

The amount of CDR data handled by the CDR entity

- 1.25 More rigorous steps may be required as the amount of CDR data handled by a CDR entity increases. Generally, as the amount of CDR data that is held increases, so too will the steps required to satisfy the reasonable steps test.

Adverse consequences for a consumer

- 1.26 Entities should consider the possible adverse consequences for CDR consumers if CDR data is not managed in accordance with the CDR system. For example, the nature of the CDR data or amount of data held could result in material harm from identity theft or fraud, discrimination, or humiliation or embarrassment. The likelihood of harm occurring will be relevant in considering whether it is reasonable to take a particular step.

Practicability of implementation

- 1.27 The practicability of implementing a particular step, including the time and cost involved, will influence the reasonableness. A 'reasonable steps' test recognises that privacy protection should be viewed in the context of the practical options available to a CDR entity.
- 1.28 However, a CDR entity is not excused from implementing particular practices, procedures or systems by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take a particular step will depend on whether the burden is excessive in all the circumstances.
- 1.29 CDR entities are also not excused from compliance with any specific processes, procedures or systems that are required by the CDR system, regardless of whether that requirement would be in excess of a reasonable step for the purposes of Privacy Safeguard 1.

Existing privacy governance arrangements

- 1.30 Where an entity has existing privacy practices and procedures for personal information it manages under the Privacy Act, it may be appropriate to extend these to its CDR data.³⁴
- 1.31 However, the mere extension of current practices and procedures does not, of itself, mean that an entity has taken *reasonable steps* to implement practices, procedures and systems.
- 1.32 Where an entity extends existing practices and procedures to its CDR data handling activities, it will need to consider to what extent it may need to modify those practices, procedures and systems to ensure compliance with the particularities of the CDR system, including the Privacy Safeguards and CDR Rules.³⁵

Have a CDR data management plan

- 1.33 A useful tool that can help CDR entities to plan and document the steps they will take to implement practices, procedures and systems under Privacy Safeguard 1 is a CDR data management plan.
- 1.34 A CDR data management plan is a document that identifies specific, measurable goals and targets, and sets out how an entity will meet its ongoing compliance obligations under Privacy Safeguard 1. As part of this, the CDR data management plan could set out the tasks an entity will undertake to ensure compliance with Privacy Safeguard 1.
- 1.35 The CDR data management plan could also set out the processes that will be used to measure and document the CDR entity's performance against their CDR data management plan.
- 1.36 Where entities have an existing privacy management plan, they may wish to update it with CDR activities so that it is integrated into the entity's privacy management processes. Alternatively, they may choose to have a separate CDR data management plan.

A suggested approach to compliance with Privacy Safeguard 1

- 1.37 The ongoing compliance requirement in Privacy Safeguard 1 can be addressed in a range of different ways, but should be tailored to the circumstances of the particular entity.
- 1.38 The following sections outline a suggested method for how steps could be taken to implement practices, procedures and systems under Privacy Safeguard 1.
- 1.39 The suggested method consists of 4 overarching steps:
- **Embed** a culture that respects and protects CDR data.
 - **Establish** robust and effective privacy practices, procedures and systems.
 - **Review** and evaluate privacy processes.
 - **Enhance** response to privacy issues.

³⁴ CDR data protected by the privacy safeguards will also be 'personal information' under the Privacy Act. For further information, see [Chapter A \(Introductory matters\)](#).

³⁵ For information about the interaction between an entity's privacy policy and CDR policy, see paragraphs 1.64 to 1.66.

Privacy tip: Where a CDR entity has a CDR data management plan, they may choose to structure that plan around the 4 overarching steps outlined in paragraph 1.39.

Embed a culture that respects and protects CDR data

- 1.40 Good CDR data management stems from good data and information governance that creates a culture of privacy that respects and protects CDR data.
- 1.41 To embed a culture of privacy, entities could:
- Appoint a member of senior management to be responsible for the strategic leadership and overall management of CDR data.
 - Appoint an officer (or officers) to be responsible for the day to day managing, advising and reporting on privacy safeguard issues.
 - Record and report on how datasets containing CDR data are treated, managed and protected.
 - Implement reporting mechanisms that ensure senior management are routinely informed about privacy and data management issues.

Establish robust and effective privacy practices, procedures and systems

- 1.42 Good privacy management requires the development and implementation of robust and effective practices, procedures and systems.
- 1.43 For example, an entity should:
- Implement risk management processes that allow identification, assessment and management of privacy risks, including CDR security risks. As part of this, accredited persons/accredited data recipients should consider their obligations to implement strong minimum information security controls under Schedule 2 to the CDR Rules.³⁶
 - Establish clear processes for reviewing and responding to CDR data complaints. CDR entities should consider their obligations to have internal dispute resolution processes under the CDR Rules.³⁷
 - Integrate privacy safeguards training into induction processes and provide regular training to those staff who deal with CDR data. This regular training should occur at least once per year. Note that accredited persons/accredited data recipients already have obligations to ensure all users undergo mandatory security and privacy training prior to interacting with the CDR data environment, with ‘refresher courses’ provided at least annually.³⁸

³⁶ See Privacy Safeguard 12, CDR Rules, rule 5.12 and Schedule 2. For further information see [Chapter 12 \(Privacy Safeguard 12\)](#) and the ACCC’s Supplementary Accreditation Guidelines on Information Security available on the ACCC’s Accreditation Guidelines page.

³⁷ See CDR Rules, rule 5.12(1) (for accredited persons) and rule 6.1 (for data holders). For the banking sector, see CDR Rules, Part 5 of Schedule 3; for the energy sector, see CDR Rules, Part 5 of Schedule 4.

³⁸ See Privacy Safeguard 12, CDR Rules, subrule 5.12(1), rule 7.11 and Schedule 2.

- Establish processes that allow CDR consumers to promptly and easily access and correct their CDR data, in accordance with the privacy safeguards and CDR Rules. As part of this, and in relation to access, data holders should consider their obligations to provide consumer data request services.³⁹ In relation to correction, CDR entities should consider their obligations under Privacy Safeguard 13 to respond to correction requests from consumers.⁴⁰
- If the entity is a primary data holder:
 - establish processes to ensure the entity only uses the secondary data holder's online service to request SR data it needs to respond to a SR data request⁴¹
 - establish processes to ensure the entity only uses and discloses the SR data received from a secondary data holder for the purpose of responding to the SR data request, and after responding to the request, deletes any of the SR data it holds in accordance with the CDR data deletion process,⁴² and
 - establish processes to ensure that any unsolicited SR data is identified and destroyed as soon as practicable, unless the data is required to be retained by or under an Australian law or a court/tribunal order.⁴³

Note: *In the energy sector, the primary data holder will be the relevant retailer.⁴⁴ There are no primary data holders in the banking sector.*

Privacy tip: As a starting point for deciding what practices, procedures and systems should be established, a CDR entity should consider their privacy obligations under the privacy safeguards and CDR Rules.

See paragraphs 1.19 to 1.21 for examples of the CDR system privacy obligations that apply to a CDR entity.

Regularly reviewing and evaluating privacy processes

1.44 To evaluate privacy practices, procedures and systems, entities should make a commitment to:

- Monitor and review CDR privacy processes regularly. This could include assessing the adequacy and currency of practices, procedures and systems, to ensure they are up to date and being adhered to.

³⁹ See CDR Rules, rule 1.13. For further information regarding consumer data request services, see the [Guide to privacy for data holders](#).

⁴⁰ See [Chapter 13 \(Privacy Safeguard 13\)](#) for further information.

⁴¹ See CDR Rules, subrule 1.24(1). See CDR Rules, subrule 1.20(2) for secondary data holders' obligations in relation to the provision of an online service that can be used by primary data holders. See [Chapter B \(Key concepts\)](#) for additional information about primary data holders and SR data.

⁴² See CDR Rules, subrule 1.24(2). See CDR Rules, rule 1.18 for the definition of 'CDR data deletion process'. See [Chapter B \(Key concepts\)](#) for additional information about primary data holders and SR data.

⁴³ See CDR Rules, rule 1.25. See [Chapter B \(Key concepts\)](#) for additional information about primary data holders and SR data.

⁴⁴ CDR Rules, subclause 4.3(b) of Schedule 4.

- Create feedback channels for both staff and consumers to continue to learn lessons from complaints and breaches, as well as customer feedback more generally.

1.45 Notably, accredited persons are required to provide regular assurance reports (an audit report) and attestation statements concerning compliance with certain information security requirements.⁴⁵

Risk point: Changes to a CDR entity’s role in the CDR system and/or information handling practices may mean that existing practices, procedures and systems are no longer fit for purpose.

Privacy tip: When reviewing and evaluating privacy processes, a CDR entity should consider a range of factors including:

- Role in the CDR system – has the entity taken on a new role, for example by becoming an accredited person in addition to being a data holder, or becoming a CDR representative principal in a CDR representative arrangement?⁴⁶
- Method of service delivery – has the entity changed the way in which it provides goods or services to CDR consumers, for example, by using OSPs to perform any of its functions?⁴⁷
- Online platforms – has the entity changed the online platforms used to communicate with consumers, for example by creating a new mobile application?⁴⁸

The answers to these questions will assist a CDR entity to make the necessary and appropriate changes to practices, procedures and systems (as recommended in the following ‘Enhance response to privacy issues’ section).

Privacy tip: Where a CDR entity has a CDR data management plan, it should set out the processes that will be used to measure and document the CDR entity’s performance against its CDR data management plan, and measure performance against this plan as part of reviewing and evaluating privacy processes.

⁴⁵ These obligations are contained in CDR Rules, rule 5.9 and clause 2.1 of Part 2 of Schedule 1 regarding default conditions on accreditation. For further information, see the ACCC’s Supplementary Accreditation Guidelines on Information Security available on the ACCC’s Accreditation Guidelines page.

⁴⁶ Different CDR regime obligations apply depending on what capacity an entity is acting in. See paragraphs 1.19 to 1.21 for further information.

⁴⁷ An outsourced service provider (OSP) is a person who does one or both of the following:

- collects CDR data from a CDR participant on behalf of an OSP chain principal under a CDR outsourcing arrangement in accordance with the CDR Rules
- uses or discloses service data to provide goods or services to their OSP principal.

Accredited persons must ensure they comply with the CDR Rules relating to OSPs. For further information, see [Chapter B \(Key concepts\)](#).

⁴⁸ By way of example, a CDR entity would need to ensure its CDR policy was available on these new online platforms: see CDR Rules, subrule 7.2(8), which requires accredited data recipients and data holders to make their CDR policy readily available through the online service that they ordinarily use to deal with consumers, such as their website or mobile applications.

Enhance response to privacy issues

- 1.46 Good privacy management requires entities to be proactive, forward thinking and to anticipate future challenges. To enhance response to privacy issues, entities should make a commitment to:
- Use the results of the evaluations to make necessary and appropriate changes to an organisation’s practices, procedures and systems.
 - Consider having practices, procedures and systems externally assessed to identify areas where privacy processes may be improved.⁴⁹
 - Continuously monitor and address new privacy risks.

Privacy tip: Where a CDR entity has a CDR data management plan, it should ensure this plan is updated to reflect any changes to the entity’s role, practices, procedures and systems and accommodate new privacy risks.

Having a CDR policy

- 1.47 Privacy Safeguard 1 requires all CDR entities to have and maintain a clearly expressed and up-to-date CDR policy.
- 1.48 The CDR policy must be in the form of a document that is distinct from any of the CDR entity’s privacy policies.⁵⁰ The Information Commissioner may, but has not, approved a form for the CDR policy.⁵¹
- 1.49 Privacy Safeguard 1 and CDR Rule 7.2 set out the requirements for what information must be included in a CDR policy and how it must be made available.⁵²
- 1.50 There are different requirements depending on whether the CDR entity is an accredited person/accredited data recipient, a data holder, or a designated gateway, as set out below. There are also some additional requirements for accredited persons who are also sponsors, affiliates or CDR representative principals under a CDR representative arrangement.
- 1.51 Where an entity occupies more than one role in the CDR system (for example is both a data holder and an accredited person), the entity can either have a single CDR policy that outlines how CDR data is managed in both capacities, or a separate CDR policy for each role.

⁴⁹ Accredited persons have obligations to provide regular assurance reports (an audit report) and attestation statements concerning compliance with certain Privacy Safeguard 12 CDR Rules. See the ACCC’s Supplementary Accreditation Guidelines on Information Security available on the ACCC’s Accreditation Guidelines page.

⁵⁰ CDR Rules, subrule 7.2(2).

⁵¹ Competition and Consumer Act, paragraph 56ED(3)(b) and CDR Rules, subrule 7.2(1).

⁵² The Information Commissioner may, but has not, approved a form for the CDR policy: Competition and Consumer Act, paragraph 56ED(3)(b) and CDR Rules, subrule 7.2(1).

Privacy tip: The OAIC has prepared a [Guide to developing a CDR policy](#) to assist CDR entities to prepare and maintain a CDR policy. It provides detailed guidance about what must be included in a CDR policy, as well as a suggested CDR policy development process, and a checklist to help ensure all requirements have been met.

Information that must be included in a CDR policy

- 1.52 The following sections outline the minimum requirements for information that must be included in a CDR policy.
- 1.53 For further information and discussion about the requirements for a CDR policy, see the OAIC's [Guide to developing a CDR policy](#).

Accredited persons/Accredited data recipients

- 1.54 Privacy Safeguard 1 requires that accredited persons who are or may become accredited data recipients must include the following in their CDR policy:
- the classes of CDR data that are (or may be) held by (or on behalf of) the entity as an accredited data recipient.⁵³ The classes of CDR data for each sector will be set out in the relevant designation instrument. The banking sector designation instrument sets out 3 classes of information: customer information,⁵⁴ product use information,⁵⁵ and information about a product.⁵⁶ The energy sector designation instrument sets out 4 classes of information: information about a customer or associate,⁵⁷ information about the sale or supply of electricity,⁵⁸ information about retail arrangements,⁵⁹ and information about retail arrangements (natural gas)⁶⁰
 - how the CDR data is (or is to be) held by or on behalf of the entity as an accredited data recipient⁶¹
 - purposes for which the entity may do each of the following (with the consent of a consumer for the CDR data): collect, hold, use or disclose CDR data⁶²
 - how a CDR consumer may both access CDR data and seek correction of CDR data⁶³
 - how a CDR consumer can complain and how the entity will deal with a complaint⁶⁴

⁵³ Competition and Consumer Act, paragraph 56ED(5)(a).

⁵⁴ Specified in Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019, section 6.

⁵⁵ Specified in Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019, section 7.

⁵⁶ Specified in Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019, section 8.

⁵⁷ Specified in Consumer Data Right (Energy Sector) Designation 2020, section 7.

⁵⁸ Specified in Consumer Data Right (Energy Sector) Designation 2020, section 8.

⁵⁹ Specified in Consumer Data Right (Energy Sector) Designation 2020, section 9.

⁶⁰ Specified in Consumer Data Right (Energy Sector) Designation 2020, section 10.

⁶¹ Competition and Consumer Act, paragraph 56ED(5)(a).

⁶² Competition and Consumer Act, paragraph 56ED(5)(b).

⁶³ Competition and Consumer Act, paragraph 56ED(5)(c).

⁶⁴ Competition and Consumer Act, paragraph 56ED(5)(d).

- whether overseas disclosure to accredited persons is likely, and the countries those persons are likely to be based in, if practicable to specify this⁶⁵
- circumstances in which the entity may disclose CDR data to a person who is not an accredited person⁶⁶
- events about which the entity will notify the consumers of such CDR data,⁶⁷ and
- when the entity must delete or de-identify CDR data in accordance with a request by a consumer.⁶⁸

1.55 In addition, subrules 7.2(4)-(7) in the CDR Rules provides other matters that an accredited data recipient (or accredited person who may become an accredited data recipient) must include in the CDR policy, including:

- a statement indicating the consequences to the CDR consumer if they withdraw a consent to collect or to use CDR data. This could include information about any early cancellation fees or loss of access to goods or services based on CDR data
- where the entity is a sponsor, a list of affiliates with whom they have a sponsorship arrangement, and the nature of the services one party provides to the other under each arrangement
- where the entity is an affiliate, a list of sponsors with whom they have a sponsorship arrangement, and the nature of the services one party provides to the other under each arrangement
- where the entity is a CDR representative principal under a CDR representative arrangement:
 - a list of their CDR representatives
 - for each CDR representative, the nature of the goods and services that the CDR representative provides to customers using CDR data

⁶⁵ Competition and Consumer Act, paragraph 56ED(5)(e) and (f).

⁶⁶ Competition and Consumer Act, paragraph 56ED(5)(g). An accredited data recipient can only disclose CDR data to a non-accredited person in accordance with CDR Rules, subrule 7.5(1). Examples of permitted disclosures include disclosures to the consumer or to an OSP, or to a CDR representative, trusted adviser or specified person (for insight and business consumer disclosures) with the consumer's consent.

⁶⁷ Competition and Consumer Act, paragraph 56ED(5)(h). The events about which an accredited person will notify a consumer will include:

- when a consumer gives consent to the person collecting, using and/or disclosing their CDR data or amends or withdraws such a consent (for further information, see [Chapter C \(Consent\)](#))
- the collection of a consumer's CDR data (see [Chapter 5 \(Privacy Safeguard 5\)](#))
- the disclosure of a consumer's CDR data to an accredited person (see [Chapter 10 \(Privacy Safeguard 10\)](#))
- any ongoing notification requirements concerning a consumer's consent (see [Chapter C \(Consent\)](#))
- any notification requirements concerning or in relation to the expiry of a consumer's consent (see [Chapter C \(Consent\)](#))
- any response to a consumer's correction request under Privacy Safeguard 13 (see [Chapter 13 \(Privacy Safeguard 13\)](#)), and
- any eligible data breach affecting a consumer under the Notifiable Data Breach scheme (see Chapter 12 (Privacy Safeguard 12)) and the OAIC's [Data breach preparation and response guide](#)).

⁶⁸ Competition and Consumer Act, paragraph 56ED(5)(i).

- a list of direct and indirect OSPs (whether based in Australia or based overseas, and whether or not any is an accredited person) of the accredited person and of any of their CDR representatives
- for each such service provider, the nature of the services it provides and the CDR data or classes of CDR data that may be disclosed to it or collected by it⁶⁹
- where the entity wishes to undertake general research using de-identified CDR data, a description of the research to be conducted and any benefits to be provided to the consumer for consenting to the use⁷⁰
- where the accredited person, any CDR representative of the accredited person, or any direct or indirect OSP of either the accredited person or CDR representative is likely to disclose CDR data to an overseas, non-accredited direct or indirect OSP, the countries in which such persons are likely to be based, if practicable to specify this⁷¹
- if applicable, the following information about de-identification of CDR data that is not redundant data:
 - how the entity uses CDR data that has been de-identified in accordance with the CDR data de-identification process to provide goods or services to consumers
 - how the entity de-identifies CDR data, including a description of techniques that it uses to de-identify CDR data, and
 - if the entity ordinarily discloses (by sale or otherwise) de-identified CDR data to one or more persons: the fact of this disclosure; the classes of persons such data is ordinarily disclosed to; and the purposes for which the entity discloses de-identified CDR data
- the following information about deletion of redundant CDR data:
 - when it deletes redundant data
 - how a CDR consumer may elect for this to happen, and
 - how it deletes redundant data⁷²
- if applicable, the following information about de-identification of redundant CDR data:
 - if the de-identified CDR data is used by the accredited data recipient—examples of how the accredited data recipient ordinarily uses de-identified CDR data
 - how the entity de-identifies CDR data, including a description of techniques that it uses to de-identify CDR data, and
 - if the entity ordinarily discloses (by sale or otherwise) de-identified CDR data to one or more persons: the fact of this disclosure; the classes of persons such data is

⁶⁹ Paragraph 1.54 outlines where to find the classes of data for the banking and energy sectors.

⁷⁰ CDR Rules, paragraph 7.5(1)(aa) permits the use or disclosure of CDR data for general research, where it has been de-identified in accordance with the CDR data de-identification processes.

⁷¹ See Competition and Consumer Act, paragraphs 56ED(5)(e)-(f) and CDR Rules, paragraph 7.2(4)(i).

⁷² This could include whether it is irretrievably destroyed, reference to any applicable standards, how the accredited data recipient manages hard copy information, how it confirms third party deletion and whether back-ups are secured. Part B of the OAIC's [Guide to securing personal information](#) outlines questions entities should consider when destroying personal information, as well as Chapter 12 – Security of CDR data and destruction or de-identification of redundant CDR data for information on the CDR deletion process.

ordinarily disclosed to; and the purposes for which the entity discloses de-identified CDR data

- the following information about the CDR consumer’s election to delete their CDR data:
 - how the election operates and its effect, and
 - how consumers can exercise the election
- further information regarding how a CDR consumer can complain and how the entity will deal with the complaint, specifically:
 - where, how and when a complaint can be lodged
 - when a consumer should expect an acknowledgement of their complaint
 - what information is required from the complainant
 - the complaint handling process, including time periods associated with the various stages
 - options for redress,⁷³ and
 - options for review, both internal and external⁷⁴
- if an entity proposes to store CDR data other than in Australia or an external territory, any country in which the entity proposes to store CDR data.

Data holder

- 1.56 Privacy Safeguard 1 requires that data holders must include in their CDR policy how a CDR consumer can access and seek correction of their CDR data, how they may complain, and how the entity will deal with a complaint.
- 1.57 In addition, the CDR Rules provide the following other matters that a data holder must include in their CDR policy:
- whether the data holder accepts consumer data requests for voluntary product data or voluntary consumer data, and, if so whether the data holder charges fees for disclosure of such data and what those fees are,⁷⁵ and
 - how a CDR consumer can complain and how the entity will deal with a complaint, specifically:
 - where, how and when a complaint can be lodged
 - when a consumer should expect an acknowledgement of their complaint
 - information required from the complainant

⁷³ ‘Redress’ in this context means options for remedy rather than options for review. This could include resolution options such as correction, apology, etc.

⁷⁴ This would include the relevant external dispute resolution scheme and the Office of the Australian Information Commissioner.

⁷⁵ Voluntary product data means CDR data for which there are no consumers that is not required product data: for the banking sector see CDR Rules, clause 3.1 of Schedule 3 and for the energy sector CDR Rules, clause 3.1 of Schedule 4. Voluntary consumer data means CDR data for which there are consumers that is not required consumer data: CDR Rules, clause 3.2 of Schedule 3 and clause 3.2 of Schedule 4.

- complaint handling process, including time periods associated with the various stages
- options for redress,⁷⁶ and
- options for review, both internal and external.⁷⁷

1.58 Finally, the Competition and Consumer Regulations provide that data holders that are energy retailers must ensure that their CDR policy also explains how a CDR consumer can access and correct their AEMO data.⁷⁸

Designated gateway

1.59 Privacy Safeguard 1 requires that designated gateways must include the following in their CDR policy:

- an explanation of how the entity will act between persons to facilitate the disclosure of the CDR data, the accuracy of the CDR data, or any other matters required under the CDR Rules, and
- how a CDR consumer may complain about a failure of the CDR entity to comply with the privacy safeguards or the CDR Rules, and how the CDR entity will deal with such a complaint.

Availability of the CDR policy

1.60 A CDR entity's CDR policy must be publicly and freely available in accordance with the CDR Rules.⁷⁹ This furthers the objective of Privacy Safeguard 1 of ensuring that CDR data is managed in an open and transparent way.

1.61 The CDR Rules provide that the CDR entity must make its CDR policy readily available on each online service where the CDR entity, or a CDR representative of the CDR entity, ordinarily deals with CDR consumers.⁸⁰ This includes making the CDR policy available through the consumer dashboard.⁸¹

Consumer requests for a CDR policy

1.62 If a copy of the CDR entity's policy is requested by a CDR consumer, the CDR entity must give the consumer a copy in accordance with CDR Rule 7.2.

1.63 CDR Rule 7.2 provides that, if requested by CDR consumer, the CDR entity must give the consumer a copy of the policy electronically or hard copy as requested by the consumer.

⁷⁶ 'Redress' in this context means options for remedy rather than options for review. This could include resolution options such as correction, apology, etc.

⁷⁷ This would include the relevant external dispute resolution scheme and the Office of the Australian Information Commissioner.

⁷⁸ Competition and Consumer Regulations, paragraph 28RA(3)(a).

⁷⁹ Competition and Consumer Act, subsection 56ED(7).

⁸⁰ CDR Rules, subrule 7.2(8).

⁸¹ CDR entities ordinarily deal with CDR consumers through the consumer dashboard, and under CDR Rules, subrules 1.14(1) and 1.15(1), the consumer dashboard is an online service. See Chapter B for more information about consumer dashboards.

Interaction between an entity's privacy policy and CDR policy

- 1.64 An entity should be aware that its privacy policy and CDR policy obligations may overlap or relate to each other.
- 1.65 While the privacy policy and CDR policy need to be separate,⁸² the entity's CDR policy and privacy policy may reference and link to each other where appropriate or required.
- 1.66 For example, Privacy Safeguard 1 requires a data holder's CDR policy to explain how a CDR consumer may access their CDR data and seek its correction.⁸³ As a consumer who is an individual may also access their data through APP 12 or seek correction of their data under APP 13 (where the data holder has not been authorised or required to disclose that data), the CDR policy must explain these alternative processes to those under the CDR system.

⁸² CDR Rules, subrule 7.2(2).

⁸³ Competition and Consumer Act, paragraph 56ED(4)(a).

Chapter 2:

Privacy Safeguard 2 —

Anonymity and pseudonymity

Version 5.0, November 2023

Contents

Key points	3
What does Privacy Safeguard 2 say?	3
Who does Privacy Safeguard 2 apply to?	3
How Privacy Safeguard 2 interacts with the Privacy Act	4
Why anonymity and pseudonymity are important	5
What is the difference between anonymity and pseudonymity?	5
Providing anonymous and pseudonymous options	6
Exceptions	6
Requiring identification — required or authorised by law	6
Requiring identification — impracticability	7

Key points

- Privacy Safeguard 2¹ requires an accredited person (who is or who may become an accredited data recipient of a consumer's CDR data) to provide a consumer with the option of dealing anonymously or pseudonymously with the entity in relation to that CDR data, unless an exception applies.

What does Privacy Safeguard 2 say?

- 2.1 Privacy Safeguard 2 provides that a consumer must have the option of not identifying themselves, or of using a pseudonym, when dealing with an accredited person (who is or who may become an accredited data recipient of the consumer's CDR data) in relation to that CDR data.²
- 2.2 'Anonymity' and 'pseudonymity' are different concepts. Privacy Safeguard 2 requires that both options be made available to consumers dealing with an accredited person unless an exception applies. The exceptions are set out in subrule 7.3(1) of the consumer data rules (CDR Rules).
- 2.3 Subrule 7.3(1) of the CDR Rules sets out that an accredited data recipient or accredited person who may become an accredited data recipient of a consumer's CDR data does not need to allow anonymity or pseudonymity where:
 - the accredited person is required or authorised by or under a law, or a court/tribunal order, to deal with an identified consumer in relation to particular CDR data, or
 - if the accredited person is an accredited data recipient, it is impracticable to deal with a consumer who has not identified themselves or has used a pseudonym in relation to the CDR data.

Who does Privacy Safeguard 2 apply to?

- 2.4 Privacy Safeguard 2 applies to accredited persons who are or who may become accredited data recipients of a consumer's CDR data. It does not apply to data holders or designated gateways.
- 2.5 Data holders and designated gateways must ensure that they are adhering to their obligations under the *Privacy Act 1988* (the Privacy Act) and the APPs, including APP 2 when dealing with individuals.
- 2.6 As a non-accredited entity, a CDR representative is not directly bound by Privacy Safeguard 2. However, under the terms of the CDR representative arrangement with their CDR representative principal,³ a CDR representative is required to comply with Privacy Safeguard

¹ *Competition and Consumer Act 2010* (Competition and Consumer Act), section 56EE.

² *Competition and Consumer Act*, section 56EE.

³ A CDR representative arrangement is a written contract between a CDR representative and their CDR representative principal. The requirements for this arrangement are outlined in CDR Rules, rule 1.10AA.

2 in its handling of service data as if it were the CDR representative principal.^{4,5} A CDR representative principal breaches subrule 7.3(2) of the CDR Rules if its CDR representative fails to comply with Privacy Safeguard 2 as if it were an accredited person (regardless of whether the CDR representative's actions accord with the CDR representative arrangement).⁶

How Privacy Safeguard 2 interacts with the Privacy Act

- 2.7 It is important to understand how Privacy Safeguard 2 interacts with the Privacy Act and the APPs.⁷
- 2.8 APP 2 requires relevant accredited persons to provide individuals with the option of not identifying themselves or of using a pseudonym.

CDR entity	Privacy protections that apply in the CDR context
Accredited person who may become an accredited data recipient	<p>Privacy Safeguard 2</p> <p>When an accredited person is dealing with a CDR consumer's data, and may become an accredited data recipient of that CDR data (for example, because they are seeking to collect it), Privacy Safeguard 2 applies.</p> <p>APP 2 does not apply to the accredited person in relation to dealings with the consumer regarding that CDR data.⁸</p>
Accredited data recipient⁹	<p>Privacy Safeguard 2</p> <p>An accredited data recipient of CDR data must comply with Privacy Safeguard 2 when dealing with the CDR consumer in relation to their CDR data. APP 2 does not apply to the accredited data recipient in relation to that CDR data.¹⁰</p>

⁴ CDR Rules, paragraph 1.10AA(4)(a)(i).

⁵ See [Chapter B \(Key concepts\)](#) for more information on 'CDR representative principal', 'CDR representative', 'CDR representative arrangement' and 'service data'.

⁶ CDR Rules, subrules 7.3(2) and 7.3(3).

⁷ The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies.

⁸ See Competition and Consumer Act, subsection 56EC(4) and paragraph 56EE(1)(b).

Note: If Privacy Safeguard 2 does not apply, APP 2 may continue to apply to other dealings with the individual's personal information where the accredited person is an APP entity (see Competition and Consumer Act, subsection 56EC(4) and paragraph 56EC(5)(aa)). Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See Privacy Act, subsection 6E(1D).

⁹ An accredited person becomes an accredited data recipient for CDR data when:

- CDR data is held by (or on behalf of) the person
- the CDR data, or any other CDR data from which it was directly or indirectly derived, was disclosed to the person under the CDR Rules, and
- the person is neither a data holder, nor a designated gateway, for the first mentioned CDR data. See s 56AK of the Competition and Consumer Act.

¹⁰ The APPs do not apply to an accredited data recipient of the CDR data in relation to the CDR data (Competition and Consumer Act, subsection 56EC(4)).

Designated gateway**APP 2**

Privacy Safeguard 2 does not apply to a designated gateway.

However, a designated gateway may have obligations relating to Privacy Safeguard 2 where an accredited data recipient provides the option of anonymity or pseudonymity to a consumer through a designated gateway for the CDR data.

Data holder¹¹**APP 2**

Privacy Safeguard 2 does not apply to a data holder.

Note: *Examples of dealings with consumers are set out in paragraph 2.14 below.*

Why anonymity and pseudonymity are important

- 2.9 Anonymity and pseudonymity are important privacy concepts. They enable consumers to choose the extent to which they are identifiable by the accredited person.
- 2.10 There can be benefits to anonymity and pseudonymity, as consumers may be more likely to inquire about products and services under the CDR system if they are able to do so without being identified. It can also reduce the risk of a data breach as less consumer data is collected.

What is the difference between anonymity and pseudonymity?

- 2.11 Anonymity means that a consumer may deal with an accredited person (who is or who may become an accredited data recipient of the consumer's CDR data) in relation to that CDR data without providing any personal information or identifiers. The accredited person should not be able to identify the consumer at the time of the dealing or subsequently. An example of an anonymous dealing is when a consumer has consented to the transfer of CDR data about their current service with no identifying information, to enquire generally about a service an accredited person can provide, and after receiving the consumer's CDR data, the accredited data recipient continues to deal with the consumer without any identifying information.
- 2.12 Pseudonymity means that a consumer may use a name, term or descriptor that is different to the consumer's actual name (e.g. an email address that does not contain the consumer's actual name). However, unlike anonymity, the use of a pseudonym does not necessarily mean that a consumer cannot be identified. The consumer may choose to divulge their identity, or to provide the CDR data necessary to identify them, such as an address.

¹¹ In this chapter, references to data holders include AEMO. See [Chapter B \(Key concepts\)](#) for further information about how the privacy safeguards apply to AEMO.

Providing anonymous and pseudonymous options

- 2.13 An accredited person (who is or who may become an accredited data recipient of the consumer's CDR data) must provide each consumer with the option of using a pseudonym, or not identifying themselves, when dealing with the accredited person in relation to that data.
- 2.14 Examples of 'dealings' include:
- asking for the consumer's consent to collect, use and/or disclose their CDR data
 - providing a consumer with a consumer dashboard
 - communicating with the consumer (for example, when providing a CDR receipt to the consumer¹² or notifying of collection under Privacy Safeguard 5)¹³
 - using the consumer's CDR data to provide the requested goods or services to the consumer, and
 - the consumer electing that their redundant data be deleted under CDR Rule 4.16.¹⁴

Note: In some cases, an accredited data recipient may not be able to deal with a consumer on an anonymous or pseudonymous basis. See paragraphs 2.15 to 2.21 following.

Exceptions

Requiring identification — required or authorised by law

- 2.15 Paragraph 7.3(1)(a) of the CDR Rules provides that an accredited person who is or may become an accredited data recipient is not required to offer a consumer the option of dealing anonymously or pseudonymously if the recipient 'is required or authorised by law or by a court/tribunal order to deal with an identified consumer in relation to particular CDR data'.¹⁵
- 2.16 The meaning of 'required or authorised by law or court/tribunal order' is discussed in [Chapter B \(Key concepts\)](#).
- 2.17 If the relevant accredited person is 'required' by a law or order to deal only with an identified consumer, it will be necessary for the consumer to provide adequate identification.
- 2.18 If the relevant accredited person is 'authorised' by a law or order to deal with an identified consumer, it can require the consumer to identify themselves, but equally will have discretion to allow the consumer to deal with the entity anonymously or pseudonymously.

¹² See [Chapter C \(Consent\)](#).

¹³ See [Chapter 5 \(Privacy Safeguard 5\)](#).

¹⁴ See [Chapter C \(Consent\)](#).

¹⁵ The exception in paragraph 7.3(1)(a) of the CDR Rules does not apply to an accredited person who is not yet an accredited data recipient of CDR data.

The nature of any discretion, and whether it is appropriate to rely upon it, will depend on the terms of the law or order and the nature of the dealing.¹⁶

- 2.19 The following are examples of where a law or order may require or authorise a relevant accredited person to deal only with an identified consumer:
- discussing or accessing certain consumer information (e.g. bank account information), or
 - opening certain accounts for a consumer, or providing other services where legislation requires the consumer to be identified.

Requiring identification — impracticability

- 2.20 Paragraph 7.3(1)(b) of the CDR Rules provides that a consumer may not have the option of dealing anonymously or pseudonymously with an accredited data recipient if it is impracticable to deal with a consumer who has not identified themselves.¹⁷
- 2.21 Examples of where it may be open to an accredited data recipient to rely on the ‘impracticability’ exception include where:
- the CDR data required to meet a consumer’s request will almost certainly identify or reasonably identify the consumer (for example account, payment or transaction details)
 - the burden of the inconvenience, time and cost of dealing with an unidentified or pseudonymous consumer, or
 - changing internal systems or practices to include the option of anonymous or pseudonymous dealings, would be excessive in all the circumstances.

Example: Anonymity and pseudonymity in the banking sector

Generally, an accredited data recipient in the banking sector may not be able to deal with a consumer on an anonymous or pseudonymous basis.¹⁸ This may be for a range of reasons, including because there may be obligations under law to verify the identity of the customer prior to providing goods or services.

Further, consumers should be aware that even where it is possible for a consumer to use a pseudonym, as CDR data in the banking sector is highly granular the consumer may remain identifiable.

¹⁶ For further information, see [Chapter B \(Key concepts\)](#).

¹⁷ The exception in paragraph 7.3(1)(b) of the CDR Rules does not apply to an accredited person who is not yet an accredited data recipient of CDR data.

¹⁸ Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019, paragraph 1.322.

Chapter 3:

Privacy Safeguard 3 —

Seeking to collect CDR data from CDR participants

Version 5.0, November 2023

Contents

Key points	3
What does Privacy Safeguard 3 say?	3
Why is it important?	4
Who does Privacy Safeguard 3 apply to?	4
How Privacy Safeguard 3 interacts with the Privacy Act	4
What is meant by ‘seeking to collect’ CDR data?	5
When can an accredited person seek to collect CDR data?	6
What is a ‘valid request?’	6
Process for asking for consent	7
Consumer data request	8
Data minimisation principle	9
Can an accredited person engage a third party to seek to collect CDR data on their behalf?	10
Interaction with other privacy safeguards	15

Key points

- Privacy Safeguard 3¹ prohibits an accredited person from attempting to collect CDR data under the CDR system unless it is in response to a ‘valid request’ from the consumer.
- The consumer data rules (CDR Rules) set out what constitutes a valid request, including requirements and processes for seeking the consumer’s consent.
- The accredited person must also comply with all other requirements in the CDR Rules for collection of CDR data. This includes the ‘data minimisation principle’, which requires that an accredited person must not seek to collect data beyond what is reasonably needed to provide the good or service to which a consumer has consented, or for a longer time period than is reasonably needed.
- Privacy Safeguard 3 applies whether the collection is directly from the CDR participant or indirectly through a designated gateway.²

What does Privacy Safeguard 3 say?

- 3.1 An accredited person must not seek to collect CDR data directly from a CDR participant (i.e. a data holder or an accredited data recipient) or indirectly through a designated gateway unless:
- the consumer has requested the accredited person seek to collect the relevant data by providing a valid request under the CDR Rules, and
 - the accredited person complies with all other requirements in the CDR Rules for the collection of CDR data from the CDR participant.³
- 3.2 Under the CDR Rules:
- the valid request must meet specific requirements, including compliance with the CDR Rules regarding consent,⁴ and
 - accredited persons must have regard to the data minimisation principle,⁵ which limits the scope of a consumer data request that an accredited person may make on behalf of a consumer.
- 3.3 The requirement in Privacy Safeguard 3 applies where an accredited person seeks to collect CDR data directly from a CDR participant, or via a designated gateway.⁶ Privacy Safeguard 3

¹ Competition and Consumer Act, section 56EF.

² There are currently no designated gateways in the banking sector or energy sector. See [Chapter B \(Key concepts\)](#) for further information on designated gateways.

³ Competition and Consumer Act, section 56EF.

⁴ CDR Rules, rule 4.3 (for requests for accredited persons to seek to collect CDR data) and rule 4.3A (for requests for CDR representative principals to seek to collect CDR data on behalf of CDR representatives).

⁵ CDR Rules, subrule 4.12(2); see subrule 4.20F(2) which applies where a CDR representative is seeking the collection consent.

⁶ Competition and Consumer Act, subsection 56EF(2).

will also apply to an accredited person where they engage an outsourced service provider (OSP) to seek to collect CDR data on their behalf.⁷

Why is it important?

- 3.4 The CDR system is driven by consumers. Consumer consent for the collection of their CDR data is at the heart of the CDR system.
- 3.5 By adhering to Privacy Safeguard 3, an accredited person will ensure consumers have control over what CDR data is collected, and for what purposes and time-period. This will assist in enhancing consumer trust, as well as minimise the possibility of over-collection.

Who does Privacy Safeguard 3 apply to?

- 3.6 Privacy Safeguard 3 applies to accredited persons.
- 3.7 Privacy Safeguard 3 does not apply to data holders and designated gateways. These entities must continue to ensure that they are adhering to their obligations under the *Privacy Act 1988* (the Privacy Act) and the APPs, including APP 3 and APP 5, when collecting personal information.

How Privacy Safeguard 3 interacts with the Privacy Act

- 3.8 It is important to understand how Privacy Safeguard 3 interacts with the Privacy Act and the APPs.⁸
- 3.9 APP 3 outlines when an entity may collect solicited personal information (See APP Guidelines, [Chapter 3 \(APP 3\)](#)).

CDR entity	Privacy protections that apply in the CDR context
Accredited person	<p>Privacy Safeguard 3</p> <p>When an accredited person is seeking to collect CDR data under the CDR Rules, Privacy Safeguard 3 applies.</p> <p>APP 3 does not apply to the accredited person in relation to that CDR data.⁹</p>

⁷ The CDR Rules requirements for engaging an outsourced service provider (OSP) to collect data on an accredited person's behalf are outlined in paragraphs 3.36– 3.41.

⁸ The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies (APP entities). See also APP Guidelines, [Chapter B \(Key concepts\)](#).

⁹ See Competition and Consumer Act, subsection 56EC(4) and section 56EF.

CDR entity	Privacy protections that apply in the CDR context
Designated gateway	APP 3 Privacy Safeguard 3 does not apply to a designated gateway.
Data holder¹⁰	APP 3 Privacy Safeguard 3 does not apply to a data holder.

What is meant by ‘seeking to collect’ CDR data?

- 3.10 Privacy Safeguard 3 applies when an accredited person ‘seeks to collect CDR data’ (before the CDR data is actually collected).
- 3.11 ‘Seeking to collect’ CDR data refers to any act of soliciting CDR data, which includes explicitly requesting another entity to provide CDR data, or taking active steps to collect CDR data.
- 3.12 The main way in which an accredited person will ‘seek to collect’ CDR data under the CDR Rules is by making a ‘consumer data request’ to a CDR participant on behalf of the consumer. Consumer data requests are explained at paragraphs 3.24 to 3.32. The point at which an accredited person makes a consumer data request is demonstrated by the flow chart on page 10 of this chapter.
- 3.13 The term ‘collect’ is discussed in detail in [Chapter B \(Key concepts\)](#). An accredited person ‘collects’ information if they collect the information for inclusion in a ‘record’ or a ‘generally available publication’.¹¹ ‘Record’¹² and ‘generally available publication’¹³ have the same meaning as within the Privacy Act.

Note: If Privacy Safeguard 3 does not apply, APP 3 may continue to apply to other collections of the individual’s personal information where the accredited person is an APP entity (see Competition and Consumer Act, subsection 56EC(4) and paragraph 56EC(5)(aa)). Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See Privacy Act, subsection 6E(1D).

¹⁰ In this chapter, references to data holders include AEMO. See [Chapter B \(Key concepts\)](#) for further information about how the privacy safeguards apply to AEMO.

¹¹ Competition and Consumer Act, subsection 4(1).

¹² Subsection 6(1) of the Privacy Act: ‘record’ includes a document or an electronic (or other) device. Some items are excluded from the definition, such as anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition, and Commonwealth records in the open access period.

¹³ Subsection 6(1) of the Privacy Act: ‘generally available publication’ means a ‘magazine, book, article, newspaper or other publication that is, or will be, generally available to members of the public’, regardless of the form in which it is published and whether it is available on payment of a fee.

When can an accredited person seek to collect CDR data?

3.14 An accredited person must not seek to collect CDR data from a CDR participant, either directly or through a designated gateway,¹⁴ unless it is in response to a valid request from a consumer, and the accredited person complies with all other requirements in the CDR Rules for the collection of CDR data.

What is a ‘valid request?’

3.15 Under rule 4.3 of the CDR Rules, a consumer gives an accredited person a ‘valid’ request to seek to collect their CDR data from a CDR participant if:

- the request is for the accredited person to provide goods or services
- the accredited person needs to collect the consumer’s CDR data from a CDR participant and use it in order to provide the requested goods or services
- the accredited person asks the consumer for a collection consent and a use consent,¹⁵ in accordance with Division 4.3 of the CDR Rules (see paragraphs 3.19–3.23 for further information), and
- the consumer expressly consents to this collection and use of their CDR data.

3.16 In relation to a CDR representative arrangement, under rule 4.3A of the CDR Rules, a consumer gives a CDR representative principal a ‘valid’ request to seek to collect their CDR data from a CDR participant if:

- the request is for the principal's CDR representative to provide goods or services
- the CDR representative needs to request its CDR representative principal to collect the consumer’s CDR data from a CDR participant, and the CDR representative needs to use it in order to provide the requested goods or services, and
- the CDR representative asks the consumer for a collection consent (for the CDR representative principal to collect their data and disclose it to the CDR representative), and a use consent (for the CDR representative to use it to provide the requested goods or services), in accordance with Division 4.3A of the CDR Rules (see paragraphs 3.19 to 3.23 for further information), and the consumer expressly consents to this collection and use of their CDR data.

3.17 A request ceases to be ‘valid’ if the consumer withdraws their collection consent.¹⁶

¹⁴ There are currently no designated gateways in the banking sector or energy sector. See [Chapter B \(Key concepts\)](#) for further information on designated gateways.

¹⁵ The consumer must provide a collection consent for the accredited person to collect their data from a CDR participant and a use consent for the accredited person to use that CDR data. See [Chapter C \(Consent\)](#) for further information.

¹⁶ CDR Rules, subrules 4.3(4) and 4.3A(5). If the consumer does not also withdraw their use consent, the accredited person may continue to use the CDR data it has already collected to provide the requested goods or services (see the note under

- 3.18 Entities should also be mindful that the *Competition and Consumer Act 2010* (Competition and Consumer Act) prohibits persons from engaging in conduct that misleads or deceives another person into believing certain matters, including that the person is making a valid request or has given their consent.¹⁷

Process for asking for consent

- 3.19 Division 4.3 of the CDR Rules outlines the requirements for consents given to accredited persons for the purposes of making a valid request for the collection and use of CDR data.
- 3.20 Specifically, the CDR Rules provide the following processes and requirements must be met to ensure that consent is voluntary, express, informed, specific as to purpose, time limited, and easily withdrawn:
- **Processes for asking for consent** (rule 4.10 of the CDR Rules): to ensure that the consent is as easy to understand as practicable.
 - **Requirements when asking for consent** (rules 4.11, 4.16 and 4.17 of the CDR Rules): including to allow the consumer to actively select the types and uses of data to which they provide consent, and provide express consent for the accredited person to collect and use the selected data for those specified purposes. Additional requirements apply where the accredited person is seeking consent to de-identify CDR data (rule 4.15 of the CDR Rules).
 - **Restrictions on seeking consent** (rule 4.12 of the CDR Rules): including that an accredited person cannot seek to collect or use CDR data for a period exceeding 12 months (or, in the case of a CDR business consumer, cannot seek consent to use CDR data for longer than 7 years).
 - Obligations about **managing the withdrawal of consent** (rule 4.13 of the CDR Rules): including that a consumer may withdraw their consent at any time through their consumer dashboard or by using a simple alternative method made available by the accredited person.
 - Time of **expiry of consent** (rule 4.14 of the CDR Rules): consent generally expires upon withdrawal of consent or at the end of the specified period in which the consumer gave consent for the accredited person to collect the CDR data (which cannot be longer than 12 months).

CDR Rule 4.3(4)), and the CDR representative principal could continue to disclose CDR data it had already collected to the CDR representative and the CDR representative could use it to provide the requested goods or services (see the note under CDR Rules, subrule 4.3A(5)). See further CDR Rules, rules 4.18 and 4.18A (for the accredited person) and rules 4.20O and 4.20Q (for the CDR representative) for ongoing notification requirements in this circumstance.

If the consumer also withdraws their use consent, the CDR data is likely to become redundant data that the accredited person is required to delete or de-identify in accordance with Privacy Safeguard 12 (unless an exception applies). More information on 'redundant data' and the requirement to destroy or de-identify redundant data is in [Chapter 12 \(Privacy Safeguard 12\)](#).

¹⁷ Competition and Consumer Act, sections 56BN and 56BO.

- 3.21 The accredited person is also required to have regard to the Consumer Experience Guidelines¹⁸ when asking a consumer to give consent.
- 3.22 The specific requirements and processes for the above CDR Rule requirements are explained in [Chapter C \(Consent\)](#).
- 3.23 Division 4.3A of the CDR Rules outlines the requirements for consents given to CDR representatives. It contains similar requirements to those in Division 4.as outlined above in paragraphs 3.20 - 3.21. . A CDR representative principal must ensure that when their CDR representative asks for a consumer’s consent, it does so in accordance with the requirements of Division 4.3A.¹⁹

Consumer data request

- 3.24 If a consumer has given an accredited person a valid request (see paragraphs 3.15 to 3.18 above),²⁰ and the consumer’s consent for the accredited person to collect and use their CDR data is current,²¹ the accredited person may request the relevant CDR participant to disclose some or all of the CDR data that:
- is the subject of the relevant collection consent and use consent, and
 - it is able to collect and use in compliance with the data minimisation principle.²²
- 3.25 In doing so, the accredited person makes a ‘consumer data request’ to a CDR participant on behalf of the consumer.²³ The accredited person may make consumer data requests to more than one CDR participant where the relevant CDR data required to provide the requested goods or services is held by different CDR participants. The accredited person may also need to make repeated consumer data requests over a period of time in order to provide the requested goods or services.
- 3.26 In relation to a sponsorship arrangement, a person with sponsored accreditation (affiliate) cannot make a consumer data request directly to a data holder. They may only make a consumer data request:
- to an accredited data recipient under rule 4.7A of the CDR Rules, or
 - through its registered sponsor acting at its request under a sponsorship arrangement.²⁴
- 3.27 Where a sponsor has collected CDR data at the request of a person with sponsored accreditation (affiliate), the CDR data is taken to have been also collected by the affiliate.²⁵

¹⁸ CDR Rules, paragraph 4.10(1)(a)(ii). The Consumer Experience Guidelines provide best practice interpretations of the CDR Rules relating to consent and are discussed in [Chapter B \(Key concepts\)](#).

¹⁹ CDR Rules, subrule 1.16A(3) and (4).

²⁰ This includes valid requests given to a CDR representative principal to collect CDR data on behalf of a CDR representative.

²¹ See paragraphs 3.15 and 3.16 above.

²² CDR Rules, subrules 4.4(1) and 4.7A(1).

²³ CDR Rules, subrules 4.4(2) and 4.7A(2).

²⁴ CDR Rules, subrule 5.1B(3).

²⁵ CDR Rules, subrule 7.6(3).

- 3.28 An accredited person may also make a consumer data request to a CDR representative as if the CDR representative were an accredited data recipient.²⁶ CDR representatives that receive such a consumer data request are able to obtain a disclosure consent from the consumer.²⁷
- 3.29 When the accredited person makes a consumer data request on behalf of a consumer, they must not seek to collect more CDR data than is reasonably needed, or for a longer time period than reasonably needed, in order to provide the requested goods or services.²⁸
- 3.30 When an accredited person makes a consumer data request to a data holder, they must make the request:
- using the data holder’s accredited person request service, and
 - in accordance with the data standards.²⁹
- 3.31 If a consumer data request includes SR data, an accredited person must make the consumer data request to the primary data holder (rather than the secondary data holder).³⁰ The primary data holder must then make a request for the SR data to the secondary data holder:
- using the secondary data holder’s request service, and
 - in accordance with the data standards.³¹
- 3.32 An accredited person complies with Privacy Safeguard 3 after giving the relevant CDR participant/s a consumer data request in the manner set out above at paragraph 3.30.³²

Data minimisation principle

- 3.33 Collection of CDR data is limited by the data minimisation principle,³³ which requires that an accredited person:
- must not collect more data than is reasonably needed in order to provide the requested goods or services or for a time period longer than what is reasonably needed, and
 - may only use the collected data consistently with the consent provided, and only as reasonably needed in order to provide the requested goods or services or to fulfill any other purpose as consented to by the consumer.

²⁶ CDR Rules, subrule 4.3B(1).

²⁷ CDR Rules, subrule 4.3B(2).

²⁸ CDR Rules, subrule 1.8(a) and paragraphs 4.4(1)(d) and 4.7A(1)(d).

²⁹ CDR Rules, subrule 4.4(3).

³⁰ CDR Rules, subrule 1.23(2). If a CDR consumer is eligible to initiate a consumer data request from an accredited person to a primary data holder for SR data, the CDR consumer is not also eligible to initiate a consumer data from an accredited person to the secondary data holder for that data: see CDR Rules, rule 1.19. Under current arrangements, this is only relevant to the energy sector as the only sector with SR data and a secondary data holder (AEMO). For further information on SR data and primary and secondary data holders, see [Chapter B \(Key concepts\)](#).

³¹ CDR Rules, subrule 1.23(4).

³² The effect of CDR Rules, subrules 4.4(2) and 4.7A(2) is that a request for CDR data from an accredited person on behalf of a consumer that does not comply with subrules 4.4(1) or CDR Rule 4.7A(1) is not a ‘consumer data request’.

³³ CDR Rules, subrule 4.12(2) (for accredited persons), subrule 4.20F (for CDR representatives) and rule 1.8.

- 3.34 The data minimisation principle is relevant both when an accredited person seeks consent from the consumer to collect their CDR data, and then when the accredited person gives a CDR participant a consumer data request.
- 3.35 The data minimisation principle is discussed further in [Chapter B \(Key concepts\)](#).

Example

MiddleMan Ltd, an accredited person, makes a consumer data request on behalf of a consumer, Athena, to seek information about Athena's eligibility to open a bank account.

MiddleMan has asked Athena for her consent to collect information about her transaction history from the data holder (in addition to other data), when this information would not be required to determine her eligibility for the service.

MiddleMan will likely be in breach of Privacy Safeguard 3 as it has sought to collect CDR data beyond what is reasonably needed to provide the requested service (as required by the data minimisation principle) and therefore has not sought to collect Athena's CDR data from a CDR participant in accordance with the CDR Rules.

Can an accredited person engage a third party to seek to collect CDR data on their behalf?

- 3.36 An accredited person (other than those with sponsored accreditation)³⁴ who is an OSP chain principal may engage a third party to seek to collect CDR data on their behalf, in accordance with the CDR Rules.³⁵
- 3.37 Rule 1.10 of the CDR Rules requires the accredited person (the 'OSP chain principal') to have a CDR outsourcing arrangement with the third party (the 'OSP' or 'provider'). A CDR outsourcing arrangement is a written contract between the OSP principal (in this collection scenario, an OSP chain principal) and provider which meets the requirements set out in subrule 1.10(3) of the CDR Rules.³⁶
- 3.38 The level to which an entity is accredited affects the purpose for which they can engage a provider:
- entities accredited to the unrestricted level and who are OSP chain principals can engage providers to collect data (in addition to disclosing data to providers to enable them to provide goods or services to the entity), and

³⁴ CDR Rules, subrule 5.1B(4).

³⁵ CDR Rules, paragraph 1.10(3)(a)(i).

³⁶ For more guidance on CDR outsourcing arrangements, see [Chapter B \(Key Concepts\)](#), [CDR outsourcing arrangement: privacy obligations for an outsourced service provider](#) and [CDR outsourcing arrangement: privacy obligations for a principal of an outsourced service provider](#).

- entities accredited to the sponsored level cannot engage a provider to collect CDR data on their behalf³⁷ (but are permitted to disclose data to providers under a CDR outsourcing arrangement to enable them to provide goods or services to the entity).
- 3.39 Where an accredited person intends to use an OSP to seek to collect a consumer's CDR data, the accredited person must:
- at the time of seeking the consumer's consent to collect and use the consumer's CDR data, advise the consumer that CDR data may be disclosed to, or collected by, an OSP and that further information can be obtained from the accredited person's CDR policy (with the link to the accredited person's CDR policy provided),³⁸ and
 - include certain information about OSPs in its CDR policy, including a list of providers, and for each provider, the nature of the services it provides and the CDR data that it may collect.³⁹
- 3.40 The accredited person must ensure the provider complies with its requirements under the CDR outsourcing arrangement, and is in breach if the provider fails to comply with a required provision of the arrangement.⁴⁰
- 3.41 Rule 7.6 of the CDR Rules provides that where an accredited person has collected CDR data under the CDR Rules, it must not use or disclose the CDR data (or CDR data derived from it) other than for a permitted use or disclosure. For the purposes of this rule, any use, disclosure or collection of data by the provider in a CDR outsourcing arrangement will be taken to have been by the principal under the arrangement. This occurs regardless of whether the use, disclosure or collection is in accordance with the CDR outsourcing arrangement.⁴¹

Risk point: Entities that fail to take robust measures in their CDR outsourcing arrangements risk non-compliance by their third parties.

Privacy tip: To ensure the third party complies with the outsourcing arrangement, the accredited person should ensure that:

- the relevant CDR outsourcing arrangement requires the third party to adhere to the accredited person's privacy safeguard obligations, and
- the contract provides an appropriate level of transparency to allow them to monitor the third party where relevant, and audit the CDR outsourcing arrangement.

³⁷ CDR Rules, subrule 5.1B(4).

³⁸ CDR Rules, subrule 4.11(3)(f). See [Chapter C \(Consent\)](#).

³⁹ CDR Rules, subrule 7.2(4). See [Chapter 1 \(Privacy Safeguard 1\)](#).

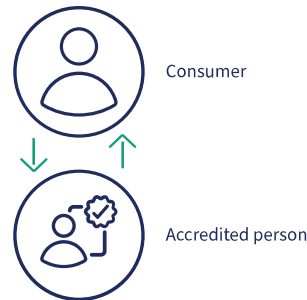
⁴⁰ CDR Rules, subrules 1.16(1) and (2). The requirements for a CDR outsourcing arrangement are set out in CDR Rules, subrule 1.10(3).

⁴¹ CDR Rules, subrules 7.6(2) and (5).

Consent and collection process for accredited persons

Obtaining consumer consent for the collection and use of CDR data

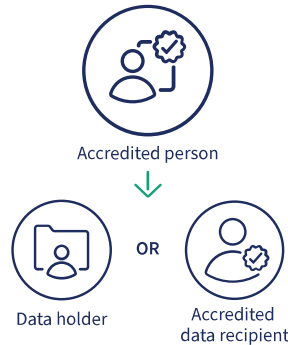
- Accredited person offers a good or service which requires CDR data
- Consumer wishes to be provided the good or service
- Accredited person asks the consumer to consent to the collection and use of their CDR data for this purpose
- Consumer provides their express consent to the collection and use of their CDR data



The consumer has given the accredited person a valid request ✓

Making a consumer data request on behalf of the consumer

- Consumer gives accredited person a valid request
- Accredited person asks the CDR participant ^[1] to disclose the consumer's CDR data
- Where the request is to a data holder, the accredited person makes the request using the data holder's 'accredited person request service', in accordance with the data standards ^[2]



The CDR participant obtains:

- the consumer's authorisation (in the case of a data holder)
- the consumer's AP disclosure consent (in the case of an accredited data recipient)

Where the CDR data is or includes SR data, the primary data holder obtains the consumer's authorisation. The primary data holder then requests any SR data it needs from the secondary data holder, using the secondary data holder's relevant online service. The secondary data holder discloses the SR data to the primary data holder (if it chooses)

The CDR participant sends the consumer's CDR data to the accredited person^[3]



The accredited person becomes an accredited data recipient for the consumer's CDR data

[1] This may be a data holder or accredited data recipient. However, an affiliate may only make a consumer data request directly to another accredited person

[2] Note: there are no equivalent requirements for how an accredited person makes a request to an accredited data recipient. Where the CDR data is or includes SR (shared responsibility) data, the request is made to the primary data holder.

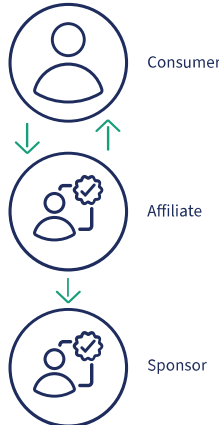
[3] Where the CDR participant is a primary data holder and the secondary data holder chooses not to disclose SR data to it, the primary data holder will not be able to send that SR data to the accredited person

[4] Note: For SR data requests, this will be the primary data holder

Consent and collection process for collection by sponsor

Obtaining consumer consent for the collection and use of CDR data

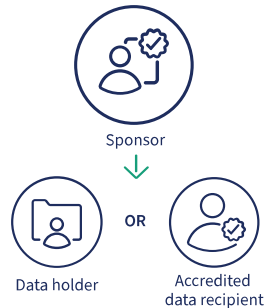
- Accredited person with sponsored accreditation (affiliate) offers a good or service which requires CDR data
- Consumer wishes to be provided the good or service
- A sponsor will collect the CDR data at the affiliate's request
- The affiliate asks the consumer to consent to the collection and use of their CDR data for this purpose
- Consumer provides their express consent to the collection and use of their CDR data
- The consumer's consent is taken to be consent for the sponsor to collect



The consumer has given the sponsor a valid request ✓

Making a consumer data request on behalf of the consumer

- Consumer gives sponsor a valid request
- Sponsor asks the CDR participant ^[1] to disclose the consumer's CDR data
- Where the request is to a data holder, the sponsor makes the request using the data holder's 'accredited person request service', in accordance with the data standards ^[2]

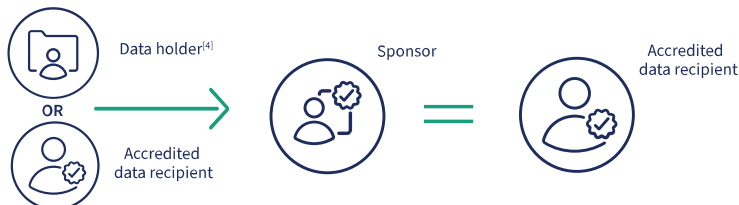


The CDR participant obtains:

- the consumer's authorisation (in the case of a data holder)
- the consumer's AP disclosure consent (in the case of an accredited data recipient)

Where the CDR data is or includes SR data, the primary data holder obtains the consumer's authorisation. The primary data holder then requests any SR data it needs from the secondary data holder, using the secondary data holder's relevant online service. The secondary data holder discloses the SR data to the primary data holder (if it chooses)

The CDR participant sends the consumer's CDR data to the sponsor^[3]



The sponsor becomes an accredited data recipient for the consumer's CDR data and discloses the data under the sponsorship arrangement to the affiliate (who also becomes an accredited data recipient)

[1] This may be a data holder or accredited data recipient.

[2] Note: there are no equivalent requirements for how an accredited person makes a request to an accredited data recipient. Where the CDR data is or includes SR (shared responsibility) data, the request is made to the primary data holder.

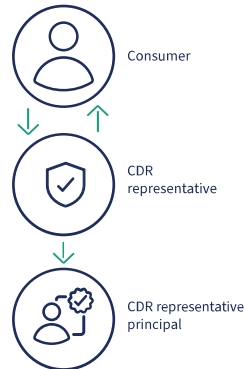
[3] Where the CDR participant is a primary data holder and the secondary data holder chooses not to disclose SR data to it, the primary data holder will not be able to send that SR data to the sponsor

[4] Note: For SR data requests, this will be the primary data holder

Consent and collection process for CDR representative arrangements

Obtaining consumer consent for the collection and use of CDR data

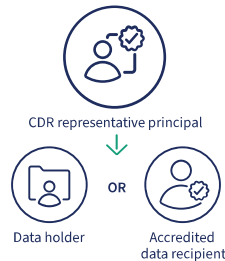
- CDR representative offers a good or service which requires CDR data
- Consumer wishes to be provided the good or service
- The CDR representative asks the consumer to consent to the collection and use of their CDR data for this purpose
- Consumer provides their express consent to the CDR representative principal collecting their CDR data, and disclosing it to the CDR representative for use



The consumer has given the CDR representative principal a valid request ✓

Making a consumer data request on behalf of the consumer

- Consumer gives CDR representative principal a valid request
- CDR representative principal asks the CDR participant^[1] to disclose the consumer's CDR data
- Where the request is to a data holder, the CDR representative principal makes the request using the data holder's 'accredited person request service', in accordance with the data standards^[2]

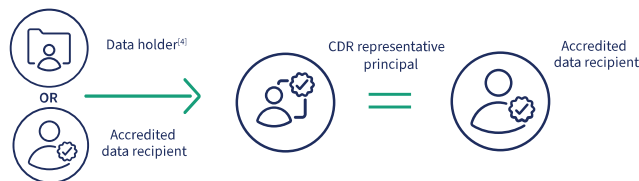


The CDR participant obtains:

- the consumer's authorisation (in the case of a data holder)
- the consumer's AP disclosure consent (in the case of an accredited data recipient)

Where the CDR data is or includes SR data, the primary data holder obtains the consumer's authorisation. The primary data holder then requests any SR data it needs from the secondary data holder, using the secondary data holder's relevant online service. The secondary data holder discloses the SR data to the primary data holder (if it chooses)

The CDR participant sends the consumer's CDR data to the CDR representative principal^[3]



The CDR representative principal becomes an accredited data recipient for the consumer's CDR data

CDR representative principal (accredited data recipient) discloses the consumer's CDR data to the CDR representative in accordance with the earlier consent from the consumer



The CDR representative has obtained the consumer's CDR data, and must comply with the terms of its CDR representative arrangement in handling the data

[1] This may be a data holder or accredited data recipient.

[2] Note: there are no equivalent requirements for how an accredited person makes a request to an accredited data recipient. Where the CDR data is or includes SR (shared responsibility) data, the request is made to the primary data holder

[3] Where the CDR participant is a primary data holder and the secondary data holder chooses not to disclose SR data to it, the primary data holder will not be able to send that SR data to the CDR representative principal

[4] Note: For SR data requests, this will be the primary data holder

Interaction with other privacy safeguards

Privacy Safeguard 4

- 3.42 The privacy safeguards distinguish between an accredited person collecting solicited CDR data ([Privacy Safeguard 3](#)) and unsolicited CDR data ([Privacy Safeguard 4](#)).
- 3.43 Privacy Safeguard 4 requires an accredited person to destroy unsolicited CDR data collected from a data holder, unless an exception applies (see [Chapter 4 \(Privacy Safeguard 4\)](#)).
- 3.44 Where an accredited person seeks to collect data in accordance with Privacy Safeguard 3 but additional data that is not requested is nonetheless disclosed by the data holder, Privacy Safeguard 4 applies to that additional data.

Privacy Safeguard 5

- 3.45 Privacy Safeguard 5 requires an accredited data recipient who collected data in accordance with Privacy Safeguard 3 to notify the consumer of the collection in accordance with the CDR Rules (see [Chapter 5 \(Privacy Safeguard 5\)](#)).

Chapter 4:

Privacy Safeguard 4 —

Dealing with unsolicited CDR data from CDR participants

Version 5.0, November 2023



Contents

Key points	3
What does Privacy Safeguard 4 say?	3
Why is it important?	3
Who does Privacy Safeguard 4 apply to?	3
How Privacy Safeguard 4 interacts with the Privacy Act	4
Unsolicited CDR data	5
In what circumstances does Privacy Safeguard 4 apply?	6
Meaning of ‘purportedly under the CDR Rules’	6
Meaning of ‘not as the result of seeking to collect that data under the CDR Rules’	6
What is the obligation to destroy unsolicited data?	7
‘Destroy’	7
As soon as practicable	7
Not required to retain the data	7
How does Privacy Safeguard 4 interact with the other privacy safeguards?	7

Key points

- Privacy Safeguard 4¹ requires an accredited person to destroy unsolicited CDR data that the entity collects and is not required to retain by Australian law or court/tribunal order.

What does Privacy Safeguard 4 say?

- 4.1 The privacy safeguards distinguish between an accredited person collecting solicited CDR data (Privacy Safeguard 3) and unsolicited CDR data (Privacy Safeguard 4).
- 4.2 Privacy Safeguard 4 requires an accredited person to, as soon as practicable, destroy CDR data that the person has collected from a data holder or accredited data recipient ('CDR participant'), purportedly under the consumer data rules (CDR Rules), where the accredited person has not sought to collect that particular data and is not required to retain it by or under an Australian law or court/tribunal order.²
- 4.3 This obligation applies regardless of whether the accredited person collects the CDR data directly from a CDR participant or indirectly through a designated gateway.³

Why is it important?

- 4.4 The objective of Privacy Safeguard 4 is to ensure that CDR data collected by an accredited person is afforded appropriate privacy protection, even where the accredited person has not solicited the CDR data.
- 4.5 Privacy Safeguard 4 requires accredited persons to destroy CDR data they have collected but not requested, unless an exception applies. This destruction requirement strengthens the protections for consumers under the CDR system and ensures that accredited persons cannot retain unsolicited CDR data unless another Australian law or court/tribunal order requires them to.

Who does Privacy Safeguard 4 apply to?

- 4.6 Privacy Safeguard 4 applies to accredited persons. It does not apply to data holders or designated gateways.
- 4.7 Data holders and designated gateways must ensure that they are adhering to their obligations under the *Privacy Act 1988* (Privacy Act) and APP 4 when dealing with unsolicited personal information.
- 4.8 Although data holders do not have obligations under Privacy Safeguard 4, primary data holders (being, under current arrangements, retailers in the energy sector) must ensure that they comply with rule 1.25 of the CDR Rules in relation to SR data which they collect from a secondary data holder purportedly under the CDR rules, but not as the result of seeking to

¹ *Competition and Consumer Act 2010* (Competition and Consumer Act), section 56EG.

² *Competition and Consumer Act*, subsection 56EG(1).

³ *Competition and Consumer Act*, subsection 56EG(2).

collect that SR data under the CDR Rules.⁴ Rule 1.25 of the CDR Rules provides that primary data holders must, as soon as practicable, destroy such SR data (provided that the primary data holder is not required to retain it by or under an Australian law or court/tribunal order).⁵

- 4.9 As a non-accredited entity, a CDR representative is not directly bound by Privacy Safeguard 4. However, under the terms of the CDR representative arrangement with their CDR representative principal,⁶ a CDR representative is required to comply with Privacy Safeguard 4 in its handling of service data as if it were the CDR representative principal.^{7,8} A CDR representative principal breaches subrule 7.3A(1) of the CDR Rules if its CDR representative fails to comply with Privacy Safeguard 4 as if it were an accredited person who had collected the service data (regardless of whether the CDR representative's actions accord with the CDR representative arrangement).⁹
- 4.10 Where they are a non-accredited entity, an outsourced service provider (OSP) is not directly bound by Privacy Safeguard 4. However, under the terms of the CDR outsourcing arrangement with their OSP principal,¹⁰ an OSP is required to comply with Privacy Safeguard 4 in its handling of service data as if it were the OSP principal.¹¹ An accredited person breaches subrule 7.3B(1) of the CDR Rules if a direct or indirect OSP of the accredited person or of their CDR representative fails to comply with Privacy Safeguard 4 as if it were an accredited person that had collected the service data (regardless of whether the OSP's actions accord with the CDR outsourcing arrangement).¹²

How Privacy Safeguard 4 interacts with the Privacy Act

- 4.11 It is important to understand how Privacy Safeguard 4 interacts with the Privacy Act and APPs.¹³
- 4.12 APP 4 applies to unsolicited personal information. APP 4 requires an APP entity to destroy or de-identify unsolicited personal information it receives if the entity determines that it could not have collected the information under APP 3.¹⁴

⁴ See [Chapter B \(Key concepts\)](#) for more information on SR data, primary data holder and secondary data holder.

⁵ CDR Rules, rule 1.25.

⁶ A CDR representative arrangement is a written contract between a CDR representative and their CDR representative principal. The requirements for this arrangement are outlined in CDR Rules, rule 1.10AA.

⁷ CDR Rules, paragraph 1.10AA(4)(a)(ii).

⁸ See [Chapter B \(Key concepts\)](#) for more information on 'CDR representative principal', 'CDR representative', 'CDR representative arrangement' and 'service data'.

⁹ CDR Rules, rule 7.3A. See also rule 1.16A in relation to a CDR representative principal's obligations and liability.

¹⁰ A CDR outsourcing arrangement is a written contract between an OSP principal and their provider that meets the minimum requirements listed in CDR Rules, subrule 1.10(3).

¹¹ CDR Rules, rule 1.10(3)(b)(i)(B),

¹² CDR Rules, rule 7.3B. See also rule 1.16 in relation to an OSP principal's obligations and liability.

¹³ The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies (APP entities). See also APP Guidelines, [Chapter B \(Key concepts\)](#).

¹⁴ See APP Guidelines, [Chapter 3 \(APP 3\)](#).

CDR Entity	Privacy protections that apply in the CDR context
Accredited person	<p>Privacy Safeguard 4</p> <p>When an accredited person collects unsolicited CDR data purportedly under the CDR Rules, Privacy Safeguard 4 applies.</p> <p>APP 4 does not apply to the accredited person in relation to that CDR data.¹⁵</p>
Designated gateway	<p>APP 4</p> <p>Privacy Safeguard 4 does not apply to a designated gateway.</p>
Data holder ¹⁶	<p>APP 4</p> <p>Privacy Safeguard 4 does not apply to a data holder. However, rule 1.25 of the CDR Rules does apply similar obligations to primary data holders in relation to unsolicited SR data (see above at paragraph 4.8).</p>

Unsolicited CDR data

4.13 The term ‘unsolicited’ is used in the heading to Privacy Safeguard 4 and refers to CDR data collected by an accredited person who has not sought to collect that data under the CDR Rules.

4.14 An example of how an accredited person might collect such ‘unsolicited’ CDR data is where:

- the accredited person makes a consumer data request on a consumer’s behalf to collect CDR data from a data holder, in accordance with Privacy Safeguard 3 and rule 4.4 of the CDR Rules
- the data holder has or receives authorisation from the consumer, and
- the data holder then discloses CDR data that includes data outside the scope of the consumer data request (and which may also be outside the data holder’s authorisation).¹⁷

4.15 A discussion of how an accredited person may properly seek to collect CDR data is contained in [Chapter 3 \(Privacy Safeguard 3\)](#).

¹⁵ See Competition and Consumer Act, subsection 56EC(4) and section 56EG.

Note: If Privacy Safeguard 4 does not apply, APP 4 may continue to apply to other unsolicited collections of the individual’s personal information where the accredited person is an APP entity (see Competition and Consumer Act, subsection 56EC(4) and paragraph 56EC(5)(aa)). Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See Privacy Act, subsection 6E(1D).

¹⁶ In this chapter, references to data holders include AEMO. See [Chapter B \(Key concepts\)](#) for further information about how the privacy safeguards apply to AEMO.

¹⁷ In these circumstances the data holder may be in breach of APP 6 if personal information was disclosed outside the authorisation provided by the consumer.

In what circumstances does Privacy Safeguard 4 apply?

4.16 Privacy Safeguard 4 applies to CDR data collected by an accredited person from a CDR participant:

- purportedly under the CDR Rules, but
- not as the result of seeking to collect that CDR data under the CDR Rules.¹⁸

Meaning of ‘purportedly under the CDR Rules’

4.17 Privacy Safeguard 4 applies to CDR data collected ‘purportedly under the CDR Rules’.¹⁹

4.18 ‘Purportedly’ in this context means that the mechanisms of the CDR rules appear to have been used but this did not validly occur because the accredited person did not, in fact, seek to collect the CDR data.

Meaning of ‘not as the result of seeking to collect that data under the CDR Rules’

4.19 Privacy Safeguard 4 applies to CDR data that is collected other than as a result of the accredited person seeking to collect it under the CDR Rules.²⁰

4.20 In practice, Privacy Safeguard 4 will typically apply to CDR data received by the accredited person that is outside the scope of the accredited person’s consumer data request to the CDR participant.

Example

Friedrich makes a valid request for Green Company (an accredited person) to collect his CDR data. Green Company then seeks to collect Friedrich’s CDR data from Yellow Company, a data holder for Friedrich’s CDR data, through a consumer data request in accordance with the CDR Rules.

Yellow Company mistakenly discloses Salome’s CDR data to Green Company, rather than Friedrich’s data. A Green Company employee realises the error and immediately arranges for the collected data to be destroyed, in compliance with Privacy Safeguard 4. The next day, Yellow Company discloses Friedrich’s CDR data pursuant to the consumer data request. Unfortunately, Yellow Company also discloses data outside the scope of the request.

Green Company soon realises that additional CDR data outside the scope of the request has been disclosed to it, which it is not required to retain. However, Green Company does not take any steps to destroy the additional data. Green Company has likely breached Privacy Safeguard 4.

¹⁸ Competition and Consumer Act, paragraph 56EG(1)(a).

¹⁹ Competition and Consumer Act, paragraph 56EG(1)(a)(i).

²⁰ Competition and Consumer Act, paragraph 56EG(1)(a)(ii).

What is the obligation to destroy unsolicited data?

‘Destroy’

4.21 Privacy Safeguard 4 requires unsolicited CDR data to be ‘destroyed’. Destruction of CDR data should follow the CDR data deletion process discussed in detail in [Chapter 12 \(Privacy Safeguard 12\)](#).

As soon as practicable

4.22 Privacy Safeguard 4 requires unsolicited CDR data to be destroyed ‘as soon as practicable’.²¹

4.23 The test of practicability is an objective test. It is the responsibility of the accredited person to be able to justify that it is not practicable to destroy unsolicited data promptly after its collection.

4.24 Accredited persons should ensure that they have systems and processes to quickly recognise and review CDR data collected which is outside the scope of a consumer data request.

4.25 In adopting a timetable that is ‘practicable’ an accredited person can take technical and resource considerations into account. However, it is the responsibility of the accredited person to justify any delay in destroying unsolicited CDR data.

4.26 The timeframe in which an accredited person must destroy unsolicited CDR data begins at the time the entity becomes aware that the data was not solicited. How quickly an accredited person becomes aware of unsolicited CDR data may depend on its available technical and other resources.

Not required to retain the data

4.27 The obligation to destroy unsolicited data does not apply to CDR data that an accredited person is required to retain by or under an Australian law or court/tribunal order.²²

4.28 The concept ‘required by or under another Australian law or court/tribunal order’ is discussed in [Chapter B \(Key concepts\)](#).

How does Privacy Safeguard 4 interact with the other privacy safeguards?

4.29 Privacy Safeguard 3 prohibits an accredited person from seeking to collect CDR data from a CDR participant unless in response to a valid request from a consumer, and in compliance with the CDR Rules (see [Chapter 3 \(Privacy Safeguard 3\)](#)).

4.30 Privacy Safeguard 12 requires an accredited data recipient to destroy or de-identify redundant data unless the entity is required by or under an Australian law or court/tribunal

²¹ Competition and Consumer Act, subsection 56EG(1).

²² Competition and Consumer Act, paragraph 56EG(1)(b).

order to retain it, or if the data relates to current or anticipated legal or dispute resolution proceedings to which the recipient is a party (see [Chapter 12 \(Privacy Safeguard 12\)](#)).

- 4.31 Privacy Safeguard 12 and Privacy Safeguard 4 together ensure that both unsolicited CDR data as well as solicited data that is no longer needed for CDR purposes are destroyed (or alternatively de-identified for the purposes of solicited data).

Chapter 5:

Privacy Safeguard 5 —

Notifying of the collection of CDR data

Version 5.0, November 2023



Contents

Key points	3
What does Privacy Safeguard 5 say?	3
Why is this important?	3
Who does Privacy Safeguard 5 apply to?	4
How Privacy Safeguard 5 interacts with the Privacy Act	4
How must notification be given?	5
Who must be notified?	6
When must notification be given?	6
What matters must be included in the notification?	7
What CDR data was collected	8
When the CDR data was collected	8
From whom the CDR data was collected	9
Sponsorship arrangements	9
Other notification requirements under the CDR Rules	10
How does Privacy Safeguard 5 interact with the other privacy safeguards?	11

Key points

- Privacy Safeguard 5¹ provides that an accredited data recipient of a consumer's CDR data must notify the consumer when they collect the data.
- This notification must occur through the consumer's dashboard as soon as practicable after the accredited data recipient has received the consumer's CDR data.

What does Privacy Safeguard 5 say?

- 5.1 If an accredited data recipient collected a consumer's CDR data under Privacy Safeguard 3, the accredited data recipient must notify that consumer of the collection by taking the steps identified in the consumer data rules (CDR Rules).²
- 5.2 The notification must:
- be given to the consumer at whose request the CDR data was collected
 - cover the matters set out in the CDR Rules, and
 - be given at or before the time specified in the CDR Rules.
- 5.3 Under rule 7.4 of the CDR Rules, an accredited data recipient of a consumer's CDR data must notify the consumer by updating the consumer's dashboard to include certain matters as soon as practicable after CDR data is collected from a data holder or accredited data recipient. Where the CDR data was collected by a sponsor on behalf of an affiliate under a sponsorship arrangement, the sponsor and affiliate may choose which of them will update the dashboard.³ In those circumstances the dashboard must also indicate that the CDR data was collected by the sponsor on behalf of the affiliate.⁴
- 5.4 For information about the concept of 'collects' refer to [Chapter B \(Key concepts\)](#). For information about seeking to collect CDR data under Privacy Safeguard 3, see [Chapter 3 \(Privacy Safeguard 3\)](#).

Why is this important?

- 5.5 Notification of collection of CDR data is an integral element of the CDR system as it provides confirmation to the consumer that their CDR data has been collected in accordance with their valid request.
- 5.6 This ensures consumers are informed when their CDR data is collected and builds trust between consumers and accredited data recipients.

¹ *Competition and Consumer Act 2010* (Competition and Consumer Act), section 56EH.

² *Competition and Consumer Act*, section 56EH.

³ CDR Rules, subrule 7.4(2).

⁴ CDR Rules, paragraph 7.4(2)(c).

Who does Privacy Safeguard 5 apply to?

- 5.7 Privacy Safeguard 5 applies to accredited data recipients of a consumer's CDR data. It does not apply to data holders or designated gateways.
- 5.8 Data holders and designated gateways must ensure that they are adhering to their obligations under the *Privacy Act 1988* (the Privacy Act) and the APPs, including APP 3 and APP 5, when collecting personal information.
- 5.9 Data holders must also ensure they adhere to Privacy Safeguard 10,⁵ which requires them to notify consumers of the disclosure of their CDR data.
- 5.10 Where:
- a sponsor collects a consumer's CDR data on behalf of an affiliate under a sponsorship arrangement, while the affiliate is responsible for providing the consumer dashboard (as the accredited person that made the consumer data request through the sponsor), the sponsor and affiliate may decide which of them will be responsible for updating the consumer dashboard to notify the consumer of that collection (including that the collection was made by the sponsor on the affiliate's behalf) under Privacy Safeguard 5⁶
 - a CDR representative principal collects a consumer's CDR data on behalf of a CDR representative under a CDR representative arrangement, the CDR representative principal must update the consumer dashboard to notify the consumer of that collection under Privacy Safeguard 5 (but may arrange for their CDR representative to do this on their behalf)⁷
 - an accredited person who is a direct or indirect outsourced service provider (OSP) collects CDR data on behalf of another accredited person (the OSP chain principal), only the OSP chain principal is required to make a notification of the collection for the purposes of Privacy Safeguard 5.⁸

How Privacy Safeguard 5 interacts with the Privacy Act

- 5.11 It is important to understand how Privacy Safeguard 5 interacts with the Privacy Act and the APPs.⁹

⁵ See [Chapter 10 \(Privacy Safeguard 10\)](#) for more information.

⁶ CDR Rules, subrule 7.4(2).

⁷ CDR Rules, subrules 1.14(5) and 4.19(2).

⁸ CDR Rules, rule 7.4 Note 2 and subrule 1.16(5). Subrule 1.16(5) provides that where an accredited principal under a CDR outsourcing arrangement uses an accredited person to collect CDR data on its behalf as a direct or indirect OSP, rule 7.4 applies only in relation to the principal. Where a collecting OSP is not an accredited person, the chain principal must still notify the consumer of the collection under Privacy Safeguard 5. Additionally, if an OSP uses other OSPs to satisfy a consumer data request, the chain principal must notify the consumer of the collection under Privacy Safeguard 5. For information on 'CDR outsourcing arrangements', see [Chapter B \(Key concepts\)](#).

⁹ The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies.

- 5.12 Like Privacy Safeguard 5, APP 5 outlines when an entity must notify of collection, as well as what information must be included in the notification.
- 5.13 The Privacy Act and APP 5 provide protection where collected data is personal information, but not CDR data.

CDR entity	Privacy protections that apply in the CDR context
Accredited data recipient	<p>Privacy Safeguard 5</p> <p>For accredited data recipients of a consumer's CDR data, the Privacy Safeguard 5 notification requirements apply to any of that consumer's CDR data that has been collected in accordance with Privacy Safeguard 3.¹⁰</p> <p>APP 5 does not apply in relation to that CDR data.¹¹</p>
Designated gateway	<p>APP 5</p> <p>Privacy Safeguard 5 does not apply to a designated gateway.</p>
Data holder¹²	<p>APP 5</p> <p>Privacy Safeguard 5 does not apply to a data holder.</p>

How must notification be given?

- 5.14 An accredited data recipient must provide the notification by updating a consumer's consumer dashboard to include the matters discussed in paragraphs 5.27 to 5.40 as soon as practicable after collecting CDR data relating to that consumer.¹³
- 5.15 The consumer dashboard is an online service that must be provided by an accredited person to each consumer who has provided consent to the collection, use and/or disclosure of their CDR data. Accredited persons are required by rule 1.14 of the CDR

¹⁰ Privacy Safeguard 5 applies from the point when the accredited person becomes an accredited data recipient of the CDR data. An accredited person becomes an accredited data recipient for CDR data when:

- CDR data is held by (or on behalf of) the person
- the CDR data, or any other CDR data from which it was directly or indirectly derived, was disclosed to the person under the CDR Rules, and
- the person is neither a data holder, nor a designated gateway, for the first mentioned CDR data. See Competition and Consumer Act, section 56AK.

¹¹ The APPs do not apply to an accredited data recipient of CDR data, in relation to that CDR data: Competition and Consumer Act, paragraph 56EC(4)(a). However, subsection 56EC(4) does not affect how the APPs apply to accredited persons and accredited data recipients who are APP entities, in relation to the handling of personal information outside the CDR system. (Note: Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See Privacy Act, subsection 6E(1D).) Subsection 56EC(4) of the Competition and Consumer Act also does not affect how the APPs apply to an accredited person who does not become an accredited data recipient of the CDR data (other than for Privacy Safeguards 1 – 4). See Competition and Consumer Act, paragraph 56EC(5)(aa).

¹² In this chapter, references to data holders include AEMO. See [Chapter B \(Key concepts\)](#) for further information about how the privacy safeguards apply to AEMO.

¹³ CDR Rules, subrule 7.4(1).

Rules to include within the consumer’s dashboard certain details of each consent to collect, use and disclose CDR data that has been given by the consumer.¹⁴

- 5.16 If a CDR representative principal makes a consumer data request at the request of a CDR representative under a CDR representative arrangement, the CDR representative principal may arrange for the CDR representative to provide the consumer dashboard on its behalf, and to update that dashboard to notify the consumer on its behalf of the collection of information.¹⁵
- 5.17 If an accredited person who is a direct or indirect OSP collects CDR data on behalf of another accredited person (the OSP principal), only the OSP chain principal needs to notify the relevant consumer/s by updating the relevant dashboard.¹⁶
- 5.18 Further guidance about the consumer dashboard is set out in [Chapter B \(Key concepts\)](#) and [Chapter C \(Consent\)](#).

Who must be notified?

- 5.19 The accredited data recipient must notify the consumer who gave the consent to collect the CDR data.
- 5.20 There may be more than one consumer to whom a set of CDR data applies, for example, where there are joint account holders of an account. In this example, the accredited data recipient is required by rule 7.4 of the CDR Rules to update only the consumer dashboard of the requesting joint account holder.¹⁷

When must notification be given?

- 5.21 An accredited data recipient must notify the consumer as soon as practicable after the CDR data is collected.
- 5.22 As a matter of best practice, notification should generally occur in as close to real time as possible (for example, in relation to ongoing collection, as close to the time of first collection as possible). In most cases, notification will occur on the same day as the CDR data is collected.
- 5.23 The test of practicability is an objective test. It is the responsibility of the accredited data recipient to be able to justify any delay in notification.
- 5.24 In determining what is ‘as soon as practicable’, the accredited data recipient may take the following factors into account:
- time and cost involved, when combined with other factors
 - technical matters, and

¹⁴ This includes the CDR data to which the consents relate and when the consents will expire. For further information regarding the requirements for an accredited person’s consumer dashboard, see CDR Rules, rule 1.14, [Chapter C \(Consent\)](#) and [Chapter B \(Key concepts\)](#).

¹⁵ CDR Rules, subrules 1.14(5) and 4.19(2).

¹⁶ CDR Rules, rule 7.4 Note 2 and subrule 1.16(5).

¹⁷ Different dashboard obligations apply to data holders: see rule 4A.13 of the CDR Rules for further information.

- any individual needs of the consumer (for example, additional steps required to make the content accessible).
- 5.25 An accredited data recipient is not excused from providing prompt notification by reason only that it would be inconvenient, time consuming or costly to do so.
- 5.26 Notifications about collections should remain on a consumer’s consumer dashboard, even where the relevant consent has expired.¹⁸

Risk point: Delays in notification of collection may result in confusion for a consumer, and non-compliance for an accredited data recipient.

Privacy tip: Accredited data recipients should ensure that they have systems and processes in place to allow for real-time and automated notification.

What matters must be included in the notification?

- 5.27 The minimum matters that must be included in the notification, and provided via the consumer’s dashboard, are:
- what CDR data was collected
 - when the CDR data was collected
 - the data holder or accredited data recipient from which the CDR data was collected, and
 - where applicable, that the data was collected by a sponsor on behalf of an affiliate.¹⁹
- 5.28 Accredited data recipients should provide information about these matters clearly and simply, but also with enough specificity to be meaningful for the consumer. How much information is required may differ depending on the circumstances.
- 5.29 Guidance on each of the minimum matters is provided below.

¹⁸ Paragraphs 1.14(3)(h) and 1.15(3)(f) of the CDR Rules provide that the consumer dashboard must include certain information about a consent or authorisation (respectively), including where that consent or authorisation is not current. This includes information about when CDR data was collected or disclosed pursuant to the consent, or disclosed pursuant to the authorisation.

¹⁹ CDR Rules, subrules 7.4(1) and (2).

Risk point: Consumers may not read or understand a notification where the details of collection are complex.

Privacy tip: An accredited data recipient should ensure that the notification is as simple and easy to understand as possible. To do this, an accredited data recipient should consider a range of factors when formulating a notification, such as:

- what the data is being used for
- the language used (including the level of detail), and
- the presentation of the information (e.g. layout, format and any visual aids used). For more complex notifications, the accredited data recipient could consider providing a condensed summary of key matters in the notification and linking to more comprehensive information or, where it may assist the consumer, a full log of access.

What CDR data was collected

- 5.30 The accredited data recipient must notify the consumer of what CDR data was collected.²⁰
- 5.31 In doing so, the accredited data recipient should ensure CDR data is described in a manner that allows the consumer to easily understand what CDR data was collected.
- 5.32 The accredited data recipient must use the Data Language Standards when describing what CDR data was collected.²¹ This will aid consumer comprehension by ensuring consistency between how CDR data was described in the consent-seeking process and how CDR data is described in the consumer dashboard.

When the CDR data was collected

- 5.33 The accredited data recipient must notify the consumer of when the CDR data was collected.²²

*‘One-off’ collection*²³

- 5.34 The accredited data recipient should include the date on which the CDR data was collected.

²⁰ CDR Rules, paragraph 7.4(1)(a).

²¹ The Data Language Standards are contained within the Consumer Experience Standards: [Data Language Standards: Common](#). They provide descriptions of the types of data to be used by accredited data recipients when making and responding to requests. Adherence to the Data Language Standards is mandatory and will help ensure there is a consistent interpretation and description of the consumer data that will be shared in the CDR system. See Competition and Consumer Act, section 56FA and CDR Rules, rule 8.11.

²² CDR Rules, paragraph 7.4(1)(b). Note this requirement refers to dates of collection, not the date that consent was provided or expired.

²³ This is where the accredited person indicated the CDR data would be collected on a single occasion (CDR Rules, paragraph 4.11(1)(b)(i)).

*Ongoing collection*²⁴

- 5.35 The accredited data recipient should, at a minimum, include the date range in which CDR data will be collected, with the starting date being the date on which the CDR data was first collected, and the end date being the date on which the accredited person will make its final collection. This end date might not necessarily be the same as the date the consent to collect expires.
- 5.36 Where an accredited data recipient is unsure of the end date, they may put the date the consent to collect expires, but must update the end date as soon as practicable after it becomes known.²⁵
- 5.37 The accredited data recipient should, in addition to stating the date range for collection, note:
- what activity will trigger ongoing collection (e.g. ‘We’ll continue to collect your transaction details from [e.g. data holder] each time you make a transaction’), and / or
 - if known, the frequency of any ongoing collection (e.g. ‘We’ll continue to collect your transaction details from [e.g. data holder] up to 3 times per day’).
- 5.38 If collection of particular CDR data stops (because a collection consent or disclosure authorisation is withdrawn for that data), but collection later recommences under an amended consent or authorisation, then the collection is not continuous and 2 separate date ranges should be included.

From whom the CDR data was collected

- 5.39 In its notification to the consumer, the accredited data recipient must indicate from whom the CDR data was collected. There may be multiple data holders and/or accredited data recipients from whom the CDR data was collected.

Sponsorship arrangements

- 5.40 Where the CDR data was collected by a sponsor on behalf of an affiliate under a sponsorship arrangement:
- the sponsor is not required to provide the consumer dashboard (rather, it is the affiliate’s responsibility as the accredited person who made the consumer request through their sponsor)
 - the sponsor and the affiliate may choose which of them will notify the consumer, and
 - the notification to the consumer must identify that the CDR data was collected by the sponsor on behalf of the affiliate.²⁶

²⁴ This is where the accredited person indicated the CDR data would be collected over a specified period of time (CDR Rules, paragraph 4.11(1)(b)(ii)).

²⁵ Rule 4.19 of the CDR Rules requires an accredited person to update the consumer dashboard as soon as practicable, after the information required to be contained on the dashboard changes.

²⁶ CDR Rules, subrule 7.4(2).

Example

Watson and Co is an accredited person that provides a budgeting service through its Watspend application. Watspend uses transaction details to provide real-time, accurate budgeting recommendations to its users.

Zoe wants to use the Watspend application, so provides Watson and Co with a valid request to collect her transaction details from Bank Belle. Zoe provides consent for Watson and Co to collect and use her transaction details for the provision of the Watspend service from 1 July 2020 to 1 January 2021.

Watson and Co collects Zoe's transaction details from Bank Belle on 1 July 2020 and becomes an accredited data recipient for this CDR data.

Watson and Co updates Zoe's consumer dashboard on 1 July 2020 to include the following notification statement:

We collected your transaction details from Bank Belle on 01.07.20. We'll continue to collect your transaction details from Bank Belle each time you make a transaction until 01.01.21.

The above statement is an example of how Watson and Co could notify Zoe of the collection of her CDR data in accordance with rule 7.4 of the CDR Rules.

Other notification requirements under the CDR Rules

5.41 In addition to the Privacy Safeguard 5 notification requirements in relation to collection, there are other notification requirements relating to consent that accredited persons must comply with:²⁷

- providing CDR receipts to the consumer (rule 4.18 of the CDR Rules)
- notification requirements where certain consents expire or are amended (rules 4.18AA, 4.18A, 4.18B and 4.18C of the CDR Rules)
- general obligation to update the consumer dashboard (rule 4.19 of the CDR Rules), and
- ongoing notification requirements for consents to collect and use (rule 4.20 of the CDR Rules).

²⁷ For an accredited data recipient who collected CDR data on behalf of a principal in a CDR outsourcing arrangement, note the effect of subrule 1.7(5) of the CDR Rules which provides that, in the CDR Rules, 'unless the contrary intention appears, a reference to an accredited person making a consumer data request, collecting CDR data, obtaining consents, providing a consumer dashboard, or using or disclosing CDR data does not include a reference to an accredited person doing those things on behalf of a principal in its capacity as the provider in an outsourced service arrangement, in accordance with the arrangement'.

For information on 'CDR outsourcing arrangements', see [Chapter B \(Key concepts\)](#), 'Outsourced service provider'.

- 5.42 Where CDR data has been collected under a sponsorship arrangement, the sponsor and affiliate may choose which will give these notices.²⁸
- 5.43 For further information regarding these notification requirements, see [Chapter C \(Consent\)](#).

How does Privacy Safeguard 5 interact with the other privacy safeguards?

- 5.44 The requirement in Privacy Safeguard 5 to notify consumers about the collection of their CDR data relates to all CDR data collected under Privacy Safeguard 3 (see [Chapter 3 \(Privacy Safeguard 3\)](#)).
- 5.45 While Privacy Safeguard 5 relates to notification on *collection*, Privacy Safeguard 10 sets out when an accredited data recipient and data holder must notify consumers about the *disclosure* of their CDR data (see [Chapter 10 \(Privacy Safeguard 10\)](#)).

²⁸ CDR Rules, rule 4.20A.

Chapter 6:

Privacy Safeguard 6 —

Use or disclosure of CDR data by accredited data recipients or designated gateways

Version 5.0, November 2023



Contents

Key points	3
What does Privacy Safeguard 6 say?	3
Accredited data recipients	3
Designated gateways	3
Who does Privacy Safeguard 6 apply to?	4
How Privacy Safeguard 6 interacts with the Privacy Act	5
Why is it important?	6
What is meant by ‘use’ and ‘disclose’?	6
‘Use’	6
‘Disclose’	7
When can an accredited data recipient use or disclose CDR data?	7
Use or disclosure required or authorised under the CDR Rules	10
Use or disclosure under Australian law or a court/tribunal order	19
Interaction with other Privacy Safeguards	20

Key points

- Privacy Safeguard 6,¹ together with rules 7.5, 7.5A, 7.6 and 7.7 of the consumer data rules (CDR Rules), applies to accredited data recipients of a consumer's CDR data, placing restrictions and obligations on them in relation to the use and disclosure of that data.²
- Generally, accredited data recipients of CDR data and designated gateways can use or disclose CDR data only where required or authorised under the CDR Rules. The consumer must consent to these uses and disclosures of their CDR data.
- Subrule 7.5(1) of the CDR Rules outlines the permitted uses and disclosures of CDR data.
- In addition, subrule 7.5(2), rule 7.5A and subrule 7.6(1) of the CDR Rules prohibit certain uses or disclosures of CDR data.
- Accredited data recipients of CDR data must comply with the data minimisation principle when using that data to provide the goods or services requested by the consumer, or to fulfil any other purpose consented to by the consumer.

What does Privacy Safeguard 6 say?

Accredited data recipients

- 6.1 An accredited data recipient of a consumer's CDR data must not use or disclose that data unless the:
- disclosure is required under the CDR Rules in response to a valid request from a consumer for the CDR data
 - use or disclosure is otherwise required or authorised under the CDR Rules, or
 - use or disclosure is required or authorised by or under another Australian law or a court/tribunal order, and the accredited data recipient makes a written note of the use or disclosure.
- 6.2 To be compliant with Privacy Safeguard 6, an accredited data recipient of CDR data must satisfy the requirements under subrules 7.5(1) and (2), and rules 7.5A and 7.6 of the CDR Rules.

Designated gateways

- 6.3 A designated gateway for CDR data must not use or disclose CDR data unless the:
- disclosure is required under the CDR Rules
 - use or disclosure is authorised under the CDR Rules, or

¹ Competition and Consumer Act, section 56EI.

² Privacy Safeguard 6 also applies to designated gateways. However, there are currently no designated gateways in the banking or energy sector, and no CDR Rules for the use or disclosure of CDR data by designated gateways. See paragraphs 6.3 to 6.4 for further information about the current application of Privacy Safeguard 6 to designated gateways.

- use or disclosure is required or authorised by or under an Australian law, or a court/tribunal order, and the designated gateway makes a written note of the use or disclosure.
- 6.4 While Privacy Safeguard 6 applies to designated gateways, there are currently no designated gateways in the banking or energy sector.³ There are also currently no CDR Rules for the use or disclosure of CDR data by designated gateways.⁴

Who does Privacy Safeguard 6 apply to?

- 6.5 Privacy Safeguard 6 applies to accredited data recipients of CDR data and designated gateways for CDR data.
- 6.6 It does not apply to data holders. However, data holders should ensure that they adhere to their obligations under the *Privacy Act 1988* (the Privacy Act) and the APPs, including APP 6, when using or disclosing personal information.⁵
- 6.7 Data holders should also ensure that if they are a primary data holder, they comply with rule 1.24 of the CDR Rules in relation to SR data they receive from a secondary data holder in response to an SR data request.⁶ Rule 1.24 states that primary data holders must not use or disclose such SR data for a purpose other than responding to the SR data request. Once the primary data holder has responded to the SR data request, it must follow the CDR data deletion process in rule 1.18 of the CDR Rules.
- 6.8 As a non-accredited entity, a CDR representative is not directly bound by Privacy Safeguard 6. However, under the terms of the CDR representative arrangement with their CDR representative principal,⁷ a CDR representative is required to comply with Privacy Safeguard 6 as if it were the CDR representative principal.⁸ It also must not use or disclose the service data unless doing so would be in accordance with the CDR representative arrangement,⁹ and a permitted use or disclosure under certain provisions in CDR Rules, rule 7.5.¹⁰ Further, any use or disclosure of service data by the CDR representative is taken to

³ For the banking sector, see the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019. For the energy sector, the energy designation specifies AEMO as a gateway for certain information: Consumer Data Right (Energy Sector) Designation 2020, subsection 6(4). However, at the time of publication, AEMO is not a designated gateway for any CDR data because under current CDR Rules, no CDR data is (or is to be) disclosed to AEMO because of the reasons in paragraph 56AL(2)(c) of the Competition and Consumer Act.

There are also no designated gateways in the telecommunications sector or non-bank lending sectors, although unlike banking and energy at the date of publication of these guidelines, there are no rules allowing for the sharing of designated telecommunications or non-bank lending data under the CDR system: Consumer Data Right (Telecommunications Sector) Designation 2022; Consumer Data Right (Non-Bank Lenders) Designation 2022.

⁴ CDR Rules, rule 7.7, which relates to Privacy Safeguard 6, only applies to accredited data recipients.

⁵ For the purposes of APP 6.2(b), the Competition and Consumer Act is an Australian law that may require or authorise a data holder to disclose personal information.

⁶ See [Chapter B \(Key concepts\)](#) for more information on SR data and primary and secondary data holders.

⁷ A CDR representative arrangement is a written contract between a CDR representative and their CDR representative principal. The requirements for this arrangement are outlined in CDR Rules, rule 1.10AA.

⁸ CDR rules, paragraph 1.10AA(4)(a)(ia).

⁹ CDR Rules, paragraph 1.10AA(4)(c).

¹⁰ CDR Rules, paragraph 1.10AA(4)(d).

have been a use or disclosure by their CDR representative principal (regardless of whether the CDR representative's actions accord with the CDR representative arrangement).¹¹

6.9 Where they are a non-accredited entity, an outsourced service provider (OSP) is not directly bound by Privacy Safeguard 6. However, under the terms of the CDR outsourcing arrangement with their OSP principal,¹² an OSP is required to comply with Privacy Safeguard 6 in its handling of service data as if it were the OSP principal.¹³ It also must not use or disclose the service data unless doing so would be in accordance with the CDR outsourcing arrangement.¹⁴ Further, any use or disclosure of service data by the OSP is taken to have been a use or disclosure by their OSP principal (regardless of whether the OSP's actions accord with the CDR outsourcing arrangement).¹⁵

How Privacy Safeguard 6 interacts with the Privacy Act

6.10 It is important to understand how Privacy Safeguard 6 interacts with the Privacy Act and the APPs.¹⁶

6.11 APP 6 relates to the use or disclosure of personal information.¹⁷

CDR entity	Privacy protections that apply in the CDR context
Accredited data recipient	<p>Privacy Safeguard 6</p> <p>For accredited data recipients of a consumer's CDR data, Privacy Safeguard 6 applies to the use or disclosure of that data.¹⁸</p> <p>APP 6 does not apply in relation to that CDR data.¹⁹</p>

¹¹ CDR Rules, subrule 7.6(4). See also rule 1.16A in relation to a CDR representative principal's obligations and liability.

¹² A CDR outsourcing arrangement is a written contract between an OSP principal and their provider that meets the minimum requirements listed in CDR Rules, subrule 1.10(3).

¹³ CDR Rules, paragraph 1.10(3)(b)(i)(C),

¹⁴ CDR Rules, paragraph 1.10(3)(b)(iv).

¹⁵ CDR Rules, subrule 7.6(5). See also rule 1.16 in relation to an OSP principal's obligations and liability.

¹⁶ The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies (APP entities).

¹⁷ APP 6 provides that if an APP entity holds personal information about an individual that was collected for a particular purpose, the entity must not use or disclose the information for another purpose unless an exception applies. See APP Guidelines, [Chapter 6 \(APP 6\)](#).

¹⁸ Privacy Safeguard 6 applies from the point when the accredited person becomes an accredited data recipient of the CDR data. An accredited person becomes an accredited data recipient for CDR data when:

- CDR data is held by (or on behalf of) the person
- the CDR data, or any other CDR data from which it was directly or indirectly derived, was disclosed to the person under the consumer data rules, and
- the person is neither a data holder, nor a designated gateway, for the first mentioned CDR data. See Competition and Consumer Act, section 56EK.

¹⁹ The APPs do not apply to an accredited data recipient of CDR data, in relation to that CDR data: Competition and Consumer Act, paragraph 56EC(4)(a). However, subsection 56EC(4) does not affect how the APPs apply to accredited

Designated gateway Privacy Safeguard 6

For designated gateways for CDR data, Privacy Safeguard 6 applies to the use and disclosure of the CDR data.²⁰

APP 6 does not apply in relation to that CDR data.²¹

Data holder²²**APP 6**

Privacy Safeguard 6 does not apply to a data holder.

Why is it important?

6.12 Consumer consent for the use and disclosure of their CDR data is at the heart of the CDR system.

6.13 By adhering to Privacy Safeguard 6 an accredited data recipient or designated gateway will ensure consumers have control over what their CDR data is being used for and who it is disclosed to. This is an essential part of the CDR system.

What is meant by ‘use’ and ‘disclose’?

‘Use’

6.14 The term ‘use’ is not defined within the *Competition and Consumer Act 2010* (Competition and Consumer Act).²³

6.15 An accredited data recipient or designated gateway ‘uses’ CDR data where it handles or undertakes an activity with the CDR data within its effective control. For further discussion of use, see [Chapter B \(Key concepts\)](#). For example, ‘use’ includes:

- the entity accessing and reading the CDR data
- the entity making a decision based on the CDR data
- the entity de-identifying the CDR data, and
- the entity passing the CDR data from one part of the entity to another.

persons and accredited data recipients who are APP entities, in relation to the handling of personal information outside the CDR system. (Note: Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See Privacy Act, subsection 6E(1D).) Subsection 56EC(4) also does not affect how the APPs apply to an accredited person who does not become an accredited data recipient of the CDR data (other than for Privacy Safeguards 1 – 4). See Competition and Consumer Act, paragraph 56EC(5)(aa).

²⁰ Competition and Consumer Act, subsection 56E(2). See paragraphs 6.3 to 6.4 for further information about the current application of Privacy Safeguard 6 to designated gateways.

²¹ The APPs do not apply to designated gateways for CDR data in relation to that CDR data: Competition and Consumer Act, paragraph 56EC(4)(d). However, subsection 56EC(4) does not affect how the APPs apply to designated gateways who are APP entities, in relation to the handling of personal information outside the CDR system. See Competition and Consumer Act, paragraph 56EC(5)(b).

²² In this chapter, references to data holders include AEMO. See Chapter B for further information about how the privacy safeguards apply to AEMO.

²³ The term ‘use’ is also not defined in the Privacy Act.

‘Disclose’

- 6.16 The term ‘disclose’ is not defined within the Competition and Consumer Act.²⁴
- 6.17 An accredited data recipient or designated gateway ‘discloses’ CDR data when it makes it accessible or visible to others outside the entity.²⁵ This focuses on the act done by the disclosing party, and not on the actions or knowledge of the recipient. There will be a disclosure in these circumstances even where the information is already known to the recipient. For further discussion of disclosure, see [Chapter B \(Key concepts\)](#).
- 6.18 Examples of disclosure include where an accredited data recipient or designated gateway:
- shares the CDR data with another entity or individual, including a related party of the entity (subject to some exceptions, as outlined in paragraph 6.19 below)
 - publishes the CDR data on the internet, whether intentionally or not
 - accidentally provides CDR data to an unintended recipient
 - reveals the CDR data in the course of a conversation with a person outside the entity, and
 - displays data on a computer screen so that the CDR data can be read by another entity or individual.
- 6.19 Where an accredited data recipient engages a third party to perform services on its behalf, the provision of CDR data to that third party will in most circumstances be a disclosure. However, in limited circumstances, providing CDR data to a third party to perform services on behalf of the entity may be a use, rather than a disclosure. See ‘use’ and ‘disclosure’ in [Chapter B \(Key concepts\)](#) for guidance on how to determine whether providing CDR data to a third party is a use or disclosure.

When can an accredited data recipient use or disclose CDR data?

- 6.20 This section outlines when an accredited data recipient may use or disclose CDR data.²⁶
- 6.21 This chapter does not consider when a designated gateway may use or disclose CDR data. This is because there are currently no designated gateways in the banking sector or energy sector.²⁷

²⁴ The term ‘disclose’ is also not defined in the Privacy Act.

²⁵ Information will be ‘disclosed’ under the CDR system regardless of whether an entity retains effective control over the data.

²⁶ Privacy Safeguard 6 allows for the use or disclosure of CDR data in certain circumstances. One of these circumstances is where the disclosure is required under the CDR Rules in response to a valid request from a consumer for the CDR data: Competition and Consumer Act, paragraph 56EI(1)(a). The CDR Rules do not currently require an accredited data recipient to disclose CDR data in response to a valid request – they only *authorise* the accredited data recipient to do so. As such, an accredited data recipient is currently only able to use or disclose CDR data where required or authorised under the CDR Rules or under an Australian law or a court/tribunal order. These circumstances are outlined in this chapter from paragraph 6.24 onwards.

²⁷ For the banking sector, see the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019. For the energy sector, the energy designation specifies AEMO as a gateway for certain information: Consumer Data Right (Energy

- 6.22 The following diagram outlines at a high-level the permitted and prohibited uses or disclosures of CDR data for an accredited data recipient. These uses and disclosures are discussed further below in this section.
- 6.23 An accredited data recipient must comply with the data minimisation principle when using CDR data. For further information on the data minimisation principle, see paragraphs 6.29-6.31 below.

Sector) Designation 2020, subsection 6(4). However, at the time of publication, AEMO is not a designated gateway for any CDR data because under current CDR Rules, no CDR data is (or is to be) disclosed to AEMO because of the reasons in paragraph 56AL(2)(c) of the Competition and Consumer Act.

Permitted uses or disclosures of CDR data by accredited data recipients^[1]

- ✓ Providing goods or services requested by the consumer
- ✓ Deriving CDR data to provide goods or services requested by the consumer
- ✓ Disclosing CDR data to the consumer to provide the requested goods or services
- ✓ Disclosing CDR data to a direct or indirect OSP in order to provide goods or services requested by the consumer
- ✓ Disclosing CDR data that has been de-identified in accordance with the CDR rules
- ✓ De-identifying CDR data for use in general research and/or for disclosure, with the consumer's consent and in accordance with the CDR data de-identification process
- ✓ Disclosing CDR data to an accredited person, in accordance with a consumer's 'AP disclosure consent'
- ✓ Disclosing CDR data to a trusted adviser in accordance with a consumer's 'TA disclosure consent'
- ✓ Disclosing CDR insights to a specified person in accordance with a consumer's 'insight disclosure consent'
- ✓ Disclosing a CDR business consumer's CDR data in accordance with a business consumer disclosure consent
- ✓ Disclosing CDR data to an accredited person if the CDR consumer has provided the accredited person and accredited data recipient with the appropriate consents
- ✓ Disclosing service data to the principal under a CDR outsourcing arrangement
- ✓ Disclosing CDR data to the other party in a sponsorship arrangement for the purpose of providing goods or services requested by the consumer
- ✓ For a CDR representative principal, disclosing CDR data to a CDR representative for certain permitted purposes
- ✓ Using or disclosing CDR data where required or authorised by law

Prohibited uses or disclosures of CDR data by accredited data recipients

- ✗ Using the CDR data to identify, compile insights or build a profile about a person who isn't the consumer, unless an exception applies
- ✗ Any uses or disclosures that an accredited data recipient is not permitted to seek consent for (permitted consents are listed in Rule 1.10A)
- ✗ Disclosing a CDR insight that includes or reveals sensitive information as defined in the *Privacy Act 1988*

[1] A disclosure is only a permitted use or disclosure if it is done in accordance with the data standards

Use or disclosure required or authorised under the CDR Rules

- 6.24 Privacy Safeguard 6 provides that an accredited data recipient of CDR data must not use or disclose CDR data unless the use or disclosure is required or authorised under the CDR Rules.²⁸
- 6.25 Subrule 7.5(1) of the CDR Rules authorises the following permitted uses or disclosures of CDR data by accredited data recipients:
- using CDR data to provide goods or services requested by the consumer in compliance with the data minimisation principle and in accordance with a current use consent from the consumer (other than a direct marketing consent)
 - de-identifying CDR data in accordance with the CDR de-identification process²⁹ to use for general research and/or for disclosing (including by selling) the de-identified data, in accordance with a current de-identification consent from the consumer³⁰
 - directly or indirectly deriving CDR data from the collected CDR data in accordance with the above uses
 - disclosing to the consumer any of their CDR data for the purpose of providing the existing goods or services³¹
 - disclosing the consumer’s CDR data in accordance with a current disclosure consent. This includes:³²
 - disclosing CDR data to an accredited person in accordance with a current ‘AP disclosure consent’
 - disclosing CDR data to a trusted adviser in accordance with a current ‘TA disclosure consent’
 - disclosing a CDR insight to a specified person for a permitted purpose in accordance with a current ‘insight disclosure consent’

²⁸ Competition and Consumer Act, paragraph 56E(1)(b). The use or disclosure of CDR data by accredited data recipients is not currently required under the CDR Rules. The use or disclosure of CDR data by accredited data recipients is authorised under the CDR Rules if it is a ‘permitted use or disclosure’ under CDR Rule 7.5 that does not relate to direct marketing: CDR Rules, subrule 7.6(1) and rule 7.7. See paragraphs 6.3 to 6.4 for further information about the current application of Privacy Safeguard 6 to designated gateways.

²⁹ See CDR Rules, rule 1.17.

³⁰ ‘General research’ is defined in rule 1.7 of the CDR Rules to mean research undertaken by an accredited data recipient with CDR data de-identified in accordance with the CDR Rules that does not relate to the provision of goods or services to any particular CDR consumer. Note that while paragraph 7.5(1)(b) of the CDR Rules refers to a current ‘use consent’, a de-identification consent is a form of ‘use consent’ and is the relevant category of consent that must be obtained for the purposes of paragraph 7.5(1)(b) of the CDR Rules.

³¹ The phrase, ‘existing goods or services’ is defined in paragraph 7.5(1)(a) of the CDR Rules to mean the goods or services requested by the consumer.

³² Note that a ‘TA disclosure consent’, an ‘insight disclosure consent’, an ‘AP disclosure consent’ and a ‘business consumer disclosure consent’ are all forms of ‘disclosure consents’ referred to in paragraph 7.5(1)(e) of the CDR Rules and are the relevant categories of consent that must be obtained for the purposes of this rule.

- disclosing a CDR business consumer’s CDR data to a specified person in accordance with a current ‘business consumer disclosure consent.’³³
 - disclosing the consumer’s CDR data to a direct or indirect OSP under a CDR outsourcing arrangement, or to the other party in a sponsorship arrangement:
 - for specific purposes, and
 - to the extent reasonably needed to do those things³⁴
 - disclosing (by sale or otherwise) to any person, CDR data that has been de-identified in accordance with the CDR data de-identification process on becoming redundant data³⁵
 - where the accredited data recipient collected CDR data on behalf of an OSP principal under a CDR outsourcing arrangement— using or disclosing service data to in accordance with the relevant CDR outsourcing arrangement ³⁶
 - disclosing CDR data to an accredited person if the CDR consumer has provided the accredited person and accredited data recipient the appropriate consents,³⁷ and
 - where the accredited data recipient is a CDR representative principal under a CDR representative arrangement – disclosing CDR data to a CDR representative for the purposes of a use or disclosure by the CDR representative that would be a permitted use or disclosure under certain provisions in rule 7.5(1) if the CDR representative were an accredited data recipient that had collected the CDR data under the consumer data request.³⁸
- 6.26 The disclosures outlined in paragraph 6.25 are only permitted disclosures if they are done in accordance with the data standards.³⁹
- 6.27 Subrule 7.5(2) and rule 7.5A of the CDR Rules prohibit the following uses or disclosures of CDR data by accredited data recipients:
- any uses or disclosures that an accredited data recipient is not permitted to seek consent for⁴⁰

³³ This will become a permitted use or disclosure on the earlier of 1 November 2023 or the day the Data Standards Chair makes standards about the process for obtaining and managing business consumer statements and business consumer disclosures – see CDR Rules, subrule 7.5A(5).

³⁴ CDR Rules, paragraph 7.5(1)(f).

³⁵ CDR Rules, paragraph 7.5(1)(g).

³⁶ CDR Rules, paragraph 7.5(1)(h).

³⁷ CDR Rules, paragraph 7.5(1)(i) permits the disclosure of CDR data to an accredited person if the consumer has given the accredited person a collection and use consent to collect CDR data from the accredited data recipient. The consumer must also have given the accredited data recipient an AP disclosure consent. For further information on the types of consents, see [Chapter C \(Consent\)](#).

³⁸ CDR Rules, paragraph 7.5(1)(j). A permitted use or disclosure includes those uses and disclosures outlined in paragraphs (a) to (g) or (i) of subrule 7.5(1) of the CDR Rules.

³⁹ CDR Rules, subrule 7.5(2)(a).

⁴⁰ CDR Rules, paragraphs 7.5(2)(b) and 4.12(3)(a) (and paragraph 4.20F(3)(a) in relation to CDR representatives). An accredited data recipient may only ask a consumer to consent to the use or disclosure of their CDR data where use or disclosure falls within a category of consents. The categories of consents are outlined subrule 1.10A(2) of the CDR Rules. For further information on consent, see [Chapter C \(Consent\)](#).

- disclosures of a CDR insight under an insight disclosure consent if the insight includes or reveals sensitive information as defined under section 6 of the Privacy Act.⁴¹ For the definition of sensitive information, see [Chapter B \(Key concepts\)](#).
- using CDR data for the purpose of identifying, compiling insights in relation to, or building a profile in relation to, any identifiable person who is not a consumer who made the consumer data request (including through aggregating the CDR data), unless the accredited data recipient is, in accordance with the consumer's consent:
 - deriving, from that CDR data, CDR data about that person's interactions with the consumer, and
 - using that derived CDR data in order to provide the requested goods or services.⁴²

6.28 The permitted uses and disclosures (in paragraph 6.25) are discussed further in this chapter.

Using CDR data in compliance with the data minimisation principle

6.29 An accredited data recipient must comply with the data minimisation principle when using CDR data to provide goods or services requested by the consumer, or to fulfil any other purpose consented to by the consumer.⁴³

6.30 An accredited data recipient complies with the data minimisation principle if, when providing the requested goods or services or using collected CDR data for any other purpose consented to by the CDR consumer, it does not use the collected CDR data, or CDR data derived from it, beyond what is reasonably needed to provide the goods or services requested by the consumer or fulfill the other purpose as consented to by the consumer.⁴⁴ The accredited data recipient must also not seek to collect more CDR data than is reasonably needed or CDR data that relates to a longer time period than is reasonably needed..⁴⁵

6.31 The data minimisation principle and meaning of 'reasonably needed' are discussed in more detail in [Chapter B \(Key concepts\)](#) and, as they relate to consent for collection, in [Chapter 3 \(Privacy Safeguard 3\)](#).

Risk point: An accredited person should pay careful attention to its processes and systems to ensure it complies with the data minimisation principle for all uses of CDR data. This includes consideration of the minimum CDR data needed to provide each good or service to a consumer.

Privacy tip: An accredited person should set up its systems and processes so that it can identify the minimum CDR data needed for a particular good or service. This will reduce the risk of over collection of CDR data and ensure that the person does not exceed the limitations imposed by the data minimisation principle.

⁴¹ CDR Rules, subrule 7.5A(4).

⁴² CDR Rules, paragraphs 7.5(2)(b) and 4.12(3)(b) (and paragraph 4.20F(3)(b) in relation to CDR representatives). Subrule 4.12(3) prohibits an accredited data recipient from asking a consumer to give consent to use or disclosure for these purposes. For further information regarding restrictions on seeking consent, see [Chapter C \(Consent\)](#).

⁴³ CDR Rules, paragraph 7.5(1)(a) and subrule 1.8(2).

⁴⁴ CDR Rules, subrule 1.8(2).

⁴⁵ CDR Rules, subrule 1.8 (1).

Using CDR data in accordance with a current consent to provide goods or services requested by the consumer

- 6.32 An accredited data recipient is authorised to use CDR data in accordance with a current use consent from the consumer to provide goods or services requested by the consumer.⁴⁶
- 6.33 The relevant uses are those uses to which the consumer expressly consented, when providing a valid request for the accredited person to collect their CDR data from a CDR participant under subrule 4.3(1) of the CDR Rules.⁴⁷ Valid requests are discussed further in [Chapter 3 \(Privacy Safeguard 3\)](#).
- 6.34 For information regarding use consents and how they must be managed, [see Chapter C \(Consent\)](#).

Example

SpendLess Pty Ltd is an accredited data recipient for Oliver's CDR data, and provides Oliver with budgeting tips through its mobile budgeting application.

SpendLess runs Oliver's transaction data through an algorithm to ascertain what other SpendLess products Oliver might be interested in.

When providing his valid request to SpendLess,⁴⁸ Oliver consented to the analysis of his transaction data so that SpendLess can identify how much money he has been spending in particular categories. He did not consent to his transaction data being used to allow SpendLess to develop and communicate offers about other products.

SpendLess has used Oliver's CDR data in a way that is not in accordance with his use consent, and this use would therefore not be a permitted use under paragraph 7.5(1)(a) of the CDR Rules.⁴⁹

Using or disclosing de-identified CDR data in accordance with a de-identification consent

- 6.35 An accredited data recipient is permitted to de-identify CDR data in accordance with a current de-identification consent from the consumer to:
- use the de-identified data for general research, and/or
 - disclose (including by selling) the de-identified data.⁵⁰

⁴⁶ CDR Rules, paragraph 7.5(1)(a). The requested goods or services are the goods or services requested under subrule 4.3(1) of the CDR Rules as part of the consumer's valid request.

⁴⁷ Note: paragraph 7.5(1)(a) of the CDR Rules permits the general 'use' of CDR data to provide the goods and services requested by the consumer. Paragraph 7.5(1)(a) of the CDR Rules does not authorise the specific types of uses defined under 'de-identification consent' or 'direct marketing consent' as per rule 1.10A. (These uses are instead authorised by CDR Rules, paragraph 7.5(1)(b) and subrule 7.5(3), respectively.)

⁴⁸ 'Valid requests' are defined in rule 4.3 of the CDR Rules. A key component of a 'valid request' is the consumer's collection consent and use consent. For further information, see [Chapter 3 \(Privacy Safeguard 3\)](#).

⁴⁹ SpendLess has used Oliver's CDR data in a manner that may constitute direct marketing under the CDR system. For information regarding direct marketing, see [Chapter 7 \(Privacy Safeguard 7\)](#).

⁵⁰ CDR Rules, paragraph 7.5(1)(b).

- 6.36 The CDR data must be de-identified in accordance with the CDR data de-identification process outlined in rule 1.17 of the CDR Rules.⁵¹
- 6.37 ‘General research’ means research undertaken using de-identified CDR data that does not relate to the provision of goods or services to any particular consumer⁵² (for example, research for product or business development).⁵³
- 6.38 Before de-identifying CDR data under a de-identification consent in accordance with rule 1.17 of the CDR Rules, the accredited data recipient must have first:
- received a de-identification consent from the consumer,⁵⁴ and
 - provided the consumer with additional information relating to the de-identification of CDR data.⁵⁵

Deriving or indirectly deriving CDR data

- 6.39 An accredited data recipient is permitted to directly or indirectly derive CDR data from the collected CDR data in order to use the data to provide the goods or services requested by the consumer.⁵⁶
- 6.40 Derived CDR data is discussed in more detail in [Chapter B \(Key concepts\)](#).

Disclosing CDR data to the consumer

- 6.41 An accredited data recipient is permitted to disclose to a consumer any of their CDR data for the purpose of providing the existing goods or services.⁵⁷
- 6.42 This includes CDR data collected from a data holder or accredited data recipient in response to the consumer’s valid request, as well as data that has been directly and/or indirectly derived from such CDR data.
- 6.43 This is a permitted disclosure under subrule 7.5(1) of the CDR Rules and does not require the consent of the consumer.

Disclosing CDR data to an accredited person

- 6.44 An accredited data recipient is permitted to disclose a consumer’s CDR data to an accredited person in accordance with an ‘AP disclosure consent’.⁵⁸

⁵¹ For further information regarding the CDR data de-identification process, see [Chapter 12 \(Privacy Safeguard 12\)](#). CDR Rules, paragraph 7.5(1)(b).

⁵² CDR Rules, subrule 1.7(1).

⁵³ Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020* at [21].

⁵⁴ A ‘de-identification consent’ is defined in paragraph 1.10A(1)(e) of the CDR Rules. It must be sought in accordance with the requirements in Division 4.3 of the CDR Rules. For further information, see [Chapter C \(Consent\)](#).

⁵⁵ CDR Rules, paragraph 4.11(3)(e) and rule 4.15. For further information, see [Chapter C \(Consent\)](#).

⁵⁶ CDR Rules, paragraph 7.5(1)(c).

⁵⁷ CDR Rules, paragraph 7.5(1)(d).

⁵⁸ CDR Rules, paragraphs 7.5(1)(e) and 7.5(1)(i). Note that while paragraph 7.5(1)(e) of the CDR Rules refers to a current ‘disclosure consent’, an AP disclosure consent is a form of ‘disclosure consent’ and is a relevant category of consent for the purposes of paragraph 7.5(1)(e).

- 6.45 An ‘AP disclosure consent’ is a consent given by the consumer for an accredited data recipient to disclose their CDR data to an accredited person in response to a consumer data request.⁵⁹
- 6.46 For further information on ‘AP disclosure consents’ and consumer data requests, see [Chapter C Consent](#)).

Disclosing CDR data to a trusted adviser

- 6.47 An accredited data recipient is permitted to disclose a consumer’s CDR data to a ‘trusted adviser’ in accordance with a ‘TA disclosure consent’.⁶⁰
- 6.48 A ‘TA disclosure consent’ is a consent given by the consumer for an accredited data recipient to disclose their CDR data to a trusted adviser to enable the consumer to receive advice or a service from that adviser.⁶¹
- 6.49 Trusted advisers must belong to one of the following specified classes:⁶²
- qualified accountants within the meaning of the [Corporations Act 2001](#)⁶³
 - people admitted to the legal profession that hold a current practising certificate
 - registered tax agents, BAS agents and tax (financial) advisers within the meaning of the [Tax Agent Services Act 2009](#)
 - financial counselling agencies within the meaning of the [ASIC Corporations \(Financial Counselling Agencies\) Instrument 2017/792](#)
 - financial advisers that are relevant providers under the *Corporations Act 2001*, other than provisional and limited-service time-share advisers, and
 - mortgage brokers within the meaning of the [National Consumer Credit Protection Act 2009](#).
- 6.50 A person is taken to be a member of a class of trusted adviser if the accredited data recipient has taken ‘reasonable steps’ to confirm that the person is, and remains, a member of that class.⁶⁴ For more information on reasonable steps, see [Chapter B \(Key concepts\)](#).
- 6.51 Where an accredited data recipient discloses CDR data to someone who is not a member of a trusted adviser class the disclosure would contravene subrule 7.6(1) of the CDR Rules, unless the person took reasonable steps to confirm the person belonged to the class.
- 6.52 Trusted advisers are not CDR participants and are therefore not subject to the privacy safeguards or other obligations that apply under the CDR system. This means that the CDR data will no longer be subject to the protections of the CDR system. An accredited data recipient must explain this to the consumer at the time of disclosure in accordance with the

⁵⁹ CDR Rules, paragraph 1.10A(1)(c)(i). For further information, see [Chapter C \(Consent\)](#).

⁶⁰ CDR Rules, paragraph 7.5(1)(e). Note that while paragraph 7.5(1)(e) refers to a current ‘disclosure consent’, a TA disclosure consent is a form of ‘disclosure consent’ and is a relevant category of consent for the purposes of paragraph 7.5(1)(e).

⁶¹ CDR Rules, paragraph 1.10A(1)(c)(iii).

⁶² CDR Rules, subrule 1.10C(2).

⁶³ Section 88B of the *Corporations Act 2001* states that ASIC may declare in writing persons who are qualified accountants for the purposes of that Act. ASIC’s qualified accountant declaration instrument can be accessed here: <https://asic.gov.au/regulatory-resources/financial-services/financial-product-disclosure/certificates-issued-by-a-qualified-accountant/>.

⁶⁴ CDR Rules, subrule 1.10C(3)).

relevant data standard.⁶⁵ The classes of trusted advisers are professions subject to existing regulatory frameworks, including consumer protection mechanisms.

6.53 For further information on ‘TA disclosure consents’ and consumer data requests, see [Chapter C \(Consent\)](#).

Disclosing a CDR insight to a specified person

6.54 An accredited data recipient is permitted to disclose a CDR insight in accordance with an ‘insight disclosure consent’.⁶⁶

6.55 ‘CDR insights’ are insights based on a consumer’s CDR data. CDR insights remain CDR data. These insights are intended to allow accredited data recipients to disclose CDR data outside the CDR system to either confirm, deny, or provide simple information to a person selected by the consumer, where this is for a limited, permitted purpose.

6.56 An ‘insight disclosure consent’ is a consent given by the consumer for an accredited data recipient to disclose CDR insights outside the CDR system for these limited purposes:⁶⁷

- to verify the consumer’s identity
- to verify the consumer’s account balance, or
- to verify the details of credits to, and debits from, the consumer’s accounts.⁶⁸

6.57 CDR insights can be disclosed to any person, provided the consumer has given valid consent.

6.58 This means that, unless the insight is disclosed to an accredited person, the CDR data will no longer be subject to the protections and safeguards of the CDR system. An accredited data recipient must explain this to the consumer at the time of disclosure in accordance with the relevant data standard.⁶⁹

6.59 For further information on ‘insight disclosure consents’ and consumer data requests, see [Chapter C \(Consent\)](#).

Disclosing CDR data under a business consumer disclosure consent

6.60 An accredited data recipient is permitted to disclose a CDR business consumer’s CDR data to a specified person in accordance with a ‘business consumer disclosure consent’ if the consumer has also given a business consumer statement.⁷⁰

⁶⁵ CDR Rules, paragraph 8.11(1)(c)(iv). See section on ‘Disclosure Consent: Non-Accredited Person Disclosure Notification’ in the Consumer Data Standards, available at: <https://consumerdatastandards.gov.au/consumer-data-standards/current-reference>.

⁶⁶ CDR Rules, paragraph 7.5(1)(e). Note that while paragraph 7.5(1)(e) refers to a current ‘disclosure consent’, an insight disclosure consent is a form of ‘disclosure consent’ and is a relevant category of consent for the purposes of paragraph 7.5(1)(e).

⁶⁷ CDR Rules, subrule 1.10A(3).

⁶⁸ CDR Rules, paragraph 1.10A(3)(a)(i)-(iii).

⁶⁹ CDR Rules, paragraph 8.11(1A)(b). See section on ‘Disclosure Consent: Non-Accredited Person Disclosure Notification’ in the Consumer Data Standards, available at: <https://consumerdatastandards.gov.au/consumer-data-standards/current-reference>.

⁷⁰ CDR Rules, paragraph 1.10A(1)(c)(v), subrule 1.10A(10) and paragraph 7.5(1)(e). Note that while paragraph 7.5(1)(e) of the CDR Rules refers to a current ‘disclosure consent’, a business consumer disclosure consent is a form of ‘disclosure consent’ and is a relevant category of consent for the purposes of paragraph 7.5(1)(e).

6.61 For further information on ‘business consumer disclosure consents’ and consumer data requests, see [Chapter C \(Consent\)](#).

Disclosing CDR data to an OSP

6.62 An accredited data recipient is permitted to disclose the consumer’s CDR data to their direct or indirect OSP for the purpose of:

- using the consumer’s CDR data to provide goods or services requested by the consumer, including by directly or indirectly deriving CDR data from the CDR data
- disclosing, to the consumer, any of their CDR data for the purpose of providing the existing goods or services, or
- disclosing CDR data in accordance with a current disclosure consent, to the extent reasonably needed to do those things.⁷¹

Example

BrightSpark Pty Ltd is an accredited data recipient for Zachary’s CDR data and provides Zachary with electricity savings tips through its mobile electricity usage application.

BrightSpark provided the information required by paragraph 4.11(3)(f) of the CDR Rules to Zachary when it asked him to give the relevant consent. BrightSpark includes information about OSPs in its CDR policy (per subrule 7.2(4) of the CDR Rules).

BrightSpark engages SaveEnergy Pty Ltd to analyse consumers’ data and report on consumers’ electricity usage trends, so that BrightSpark can provide tailored electricity savings advice to consumers.

BrightSpark discloses Zachary’s account and electricity usage data to SaveEnergy. However, BrightSpark did not first consider whether SaveEnergy needs both electricity usage and account data for this purpose.

If SaveEnergy does not need to analyse Zachary’s account data in order to report on his electricity usage trends, BrightSpark may have disclosed Zachary’s CDR data to an OSP beyond the extent reasonably needed to provide the service requested by Zachary. The disclosure by BrightSpark may therefore not be a permitted disclosure under paragraph 7.5(1)(f) of the CDR Rules.

6.63 The consumer’s CDR data includes data collected from a data holder or accredited data recipient in response to the consumer’s request. The consumer’s CDR data also includes data that has been directly and/or indirectly derived from their CDR data.

6.64 Disclosure of a consumer’s CDR data by an accredited data recipient to an OSP for the purpose outlined in paragraph 6.62 is a permitted disclosure under subrule 7.5(1) of the CDR Rules that does not require the consent of the consumer.⁷²

6.65 Any use or disclosure by a direct or indirect OSP of an accredited data recipient (or of a CDR representative of an accredited data recipient) of CDR data disclosed under a CDR

⁷¹ CDR Rules, paragraph 7.5(1)(f).

⁷² However, the accredited data recipient must ensure it has complied with the requirements set out in paragraph 6.62.

outsourcing arrangement will be taken to have been a use or disclosure by the accredited data recipient. This occurs regardless of whether the use or disclosure is in accordance with the arrangement.⁷³

6.66 When disclosing CDR data to an OSP located outside of Australia, an accredited data recipient must also have regard to the requirements for disclosure of CDR data to an overseas recipient under Privacy Safeguard 8.⁷⁴ See [Chapter 8 \(Privacy Safeguard 8\)](#) for more information.

6.67 For further information, see [Chapter B \(Key Concepts\)](#), ‘Outsourced service providers’.

Disclosing CDR data to the other party in a sponsorship arrangement

6.68 A party to a sponsorship arrangement is permitted to disclose the consumer’s CDR data to the other party to the arrangement for the purpose of:

- using the consumer’s CDR data to provide goods or services requested by the consumer, including by directly or indirectly deriving CDR data from the CDR data
- de-identifying CDR data to use for general research and/or to disclose (including by selling) the de-identified data, in accordance with a current de-identification consent
- disclosing, to the consumer, any of their CDR data for the purpose of providing the existing goods or services
- disclosing CDR data in accordance with a current disclosure consent

to the extent reasonably needed to do those things.⁷⁵

Disclosures of CDR data by an accredited OSP

6.69 Where an accredited data recipient has collected CDR data on behalf of another accredited person in its capacity as a direct or indirect OSP of the person under a CDR outsourcing arrangement, the accredited data recipient is permitted to use or disclose that CDR data in accordance with the arrangement.⁷⁶

6.70 Disclosure of CDR data in relation to a CDR outsourcing arrangement by an accredited data recipient to the relevant principal is a permitted disclosure under subrule 7.5(1) of the CDR Rules that does not require the consent of the consumer.

⁷³ CDR Rules, subrule 7.6(2). See also section 56AU of the Competition and Consumer Act, regarding the application to acts done by or in relation to agents of CDR entities.

⁷⁴ An accredited person must also include certain information in its CDR policy about OSPs located overseas: CDR Rules, paragraph 7.2(4)(d). See [Chapter 1 \(Privacy Safeguard 1\)](#) for further information.

⁷⁵ CDR Rules, paragraph 7.5(1)(f).

⁷⁶ CDR Rules, paragraph 7.5(1)(h)—this rule only applies to OSPs who are accredited. More broadly, all OSPs must only use and disclose data in accordance with their CDR outsourcing arrangement with their OSP principal.

Disclosing service data to a CDR representative in a CDR representative arrangement

6.71 A CDR representative principal may disclose CDR data it collected on behalf of its CDR representative to that CDR representative for purposes of the CDR representative:

- using the CDR data to provide goods or services (in accordance with a use consent, and the data minimisation principal)
- in accordance with a de-identification consent, de-identifying the data to use for general research or to disclose (including by sale)
- directly or indirectly deriving CDR data from the collected CDR data in order to use the data for the 2 purposes outlined above
- disclosing to the CDR consumer any of their own CDR data, to provide the consumer with the requested good or services
- disclosing the consumer's CDR data in accordance with a current disclosure consent
- disclosing a CDR consumer's CDR data to a direct or indirect OSP for the purpose of:
 - using the consumer's CDR data to provide goods or services requested by the consumer, including by directly or indirectly deriving CDR data from the CDR data, or
 - disclosing, to the consumer, any of their CDR data for the purpose of providing the existing goods or services,
 - disclosing CDR data in accordance with a current disclosure consent,
 to the extent reasonably needed to do those things
- disclosing (by sale or otherwise) to any person, CDR data that has been de-identified in accordance with the CDR data de-identification process on the data becoming redundant data, and
- disclosing CDR data to an accredited person if the CDR consumer has provided the accredited person and accredited data recipient the appropriate consents.⁷⁷

6.72 Any use or disclosure of service data by a CDR representative is taken to have been by the CDR representative principal, whether or not the use or disclosure is in accordance with the CDR representative arrangement.⁷⁸

Use or disclosure under Australian law or a court/tribunal order

6.73 An accredited data recipient may use or disclose CDR data if that use or disclosure is required or authorised by or under an Australian law or a court/tribunal order, and the entity makes a written note of the use or disclosure.⁷⁹

⁷⁷ CDR Rules, paragraph 7.5(1)(j).

⁷⁸ CDR Rules, subrule 7.6(4).

⁷⁹ Competition and Consumer Act, paragraph 56E(1)(c).

- 6.74 For the purposes of Privacy Safeguard 6, an Australian law does not include the APPs under the Privacy Act.⁸⁰
- 6.75 ‘Australian law’ and ‘court/tribunal order’ are discussed in [Chapter B \(Key concepts\)](#).
- 6.76 The accredited data recipient must keep a written note of any uses or disclosures made on this ground.
- 6.77 A written note should include the following details:
- the date of the use or disclosure
 - details of the CDR data that was used or disclosed
 - the relevant Australian law or court/tribunal order that required or authorised the use or disclosure
 - if the accredited data recipient used the CDR data, how the CDR data was used by the accredited data recipient, and
 - if the accredited data recipient disclosed the CDR data, to whom the CDR data was disclosed.

Interaction with other Privacy Safeguards

- 6.78 The restrictions on using or disclosing CDR data in Privacy Safeguard 6 are additional to those in Privacy Safeguards 7 (see [Chapter 7 \(Privacy Safeguard 7\)](#)), 8 (see [Chapter 8 \(Privacy Safeguard 8\)](#)) and 9 (see [Chapter 9 \(Privacy Safeguard 9\)](#)).
- 6.79 Privacy Safeguard 7 prohibits accredited data recipients and designated gateways from using or disclosing CDR data for direct marketing unless the use or disclosure is required or authorised under the CDR Rules and in accordance with a valid consent.
- 6.80 Privacy Safeguard 8 prohibits an accredited data recipient from disclosing CDR data to an overseas recipient unless an exception applies.
- 6.81 Privacy Safeguard 9 prohibits an accredited data recipient of CDR data that contains a government related identifier from adopting, using or disclosing that identifier, unless an exception applies.
- 6.82 Privacy Safeguard 7 operates to the exclusion of Privacy Safeguard 6⁸¹ (which means that direct marketing uses or disclosures cannot be authorised under Privacy Safeguard 6), while Privacy Safeguards 8 and 9 operate as restrictions in addition to Privacy Safeguard 6.⁸²

⁸⁰ Competition and Consumer Act, subsection 56EI(1) (Note 3) and paragraph 56EC(4)(a).

⁸¹ Competition and Consumer Act, subsection 56E(3).

⁸² See Competition and Consumer Act, Note 2 of section 56EK and Note 2 of section 56EL.

Chapter 7:

Privacy Safeguard 7 —

Use or disclosure of CDR data for direct marketing by accredited data recipients or designated gateways

Version 5.0, November 2023

Contents

Key points	3
What does Privacy Safeguard 7 say?	3
Accredited data recipients	3
Designated gateways	3
Who does Privacy Safeguard 7 apply to?	4
How Privacy Safeguard 7 interacts with the Privacy Act	5
What is direct marketing?	6
When is direct marketing allowed?	7
Information about upgraded or alternative goods or services	8
Offer to renew existing goods or services	9
Information about the benefits of existing goods or services	10
Information about other goods or services provided by another accredited person	10
Disclosure to another accredited person to enable provision of promoted goods and services	10
Using the CDR data as reasonably needed, in accordance with the data minimisation principle	11
Disclosure to an outsourced service provider	11
Disclosure to a CDR representative	12
Interaction with other privacy safeguards	13
Interaction with other legislation	13

Key points

- Privacy Safeguard 7¹ prohibits accredited data recipients of CDR data from using or disclosing the CDR data for direct marketing, unless the consumer consents and such use or disclosure is required or authorised under the consumer data rules (CDR Rules).²
- Direct marketing in the CDR context involves the use or disclosure of CDR data to promote goods and services directly to a consumer.
- The CDR Rules permit accredited data recipients of CDR data to engage in certain direct marketing activities in relation to particular goods or services, if consent has been received to do so.
- An accredited data recipient of CDR data must comply with the data minimisation principle when using the CDR data for direct marketing.

What does Privacy Safeguard 7 say?

Accredited data recipients

- 7.1 Privacy Safeguard 7 prohibits accredited data recipients of CDR data from using or disclosing the CDR data for direct marketing, unless:
- the disclosure is required under the CDR Rules in response to a valid request from the CDR consumer, or
 - the use or disclosure is authorised under the CDR Rules in accordance with a valid consent from the CDR consumer.³
- 7.2 Rule 7.8 and subrule 7.5(3) of the CDR Rules authorise certain direct marketing related uses or disclosures by accredited data recipients (in accordance with the consumer's consent).

Designated gateways

- 7.3 Privacy Safeguard 7 prohibits designated gateways for CDR data from using or disclosing the CDR data for direct marketing unless:
- the disclosure is required or authorised under the CDR Rules, or
 - the use is authorised under the CDR Rules.⁴

¹ Competition and Consumer Act, section 56EJ.

² Privacy Safeguard 7 also prohibits designated gateways from using or disclosing the CDR data for direct marketing, unless the use or disclosure is authorised, or the disclosure is required, under the CDR Rules. However, there are currently no designated gateways in the banking or energy sector, and no CDR Rules for the use or disclosure of CDR data by designated gateways.

³ Competition and Consumer Act, subsection 56EJ(1).

⁴ Competition and Consumer Act, subsection 56EJ(2).

- 7.4 While Privacy Safeguard 7 applies to designated gateways, there are currently no designated gateways in the banking or energy sector.⁵ There are also currently no CDR Rules for the use or disclosure of CDR data by designated gateways.⁶

Why is it important?

- 7.5 To provide a positive consumer experience and ensure consumer control over their data, consumers should not be subjected to unwanted direct marketing.
- 7.6 Direct marketing is addressed separately to other uses and disclosures (see [under Privacy Safeguard 6](#)) to ensure that direct marketing under the CDR accords with the particular wishes of the CDR consumer.

Who does Privacy Safeguard 7 apply to?

- 7.7 Privacy Safeguard 7 applies to accredited data recipients of CDR data and designated gateways for CDR data. It does not apply to data holders.
- 7.8 Data holders must ensure that they adhere to their obligations under the *Privacy Act 1988* (the Privacy Act) and the APPs, including APP 7 in respect of direct marketing.
- 7.9 As a non-accredited entity, a CDR representative is not directly bound by Privacy Safeguard 7. However, under the terms of the CDR representative arrangement with their CDR representative principal,⁷ a CDR representative is required to comply with Privacy Safeguard 7 as though it were the CDR representative principal.⁸ It also must not use or disclose the service data unless doing so would be in accordance with the CDR representative arrangement, and a permitted use or disclosure under certain provisions in CDR Rules, rule 7.5.⁹ Further, any use or disclosure of service data by the CDR representative is taken to have been a use or disclosure by their CDR representative principal (regardless of whether the CDR representative's actions accord with the CDR representative arrangement).¹⁰
- 7.10 Where they are a non-accredited entity, an outsourced service provider (OSP) is not directly bound by Privacy Safeguard 7. However, under the terms of the CDR outsourcing

⁵ For the banking sector, see the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019. For the energy sector, the energy designation specifies AEMO as a gateway for certain information: Consumer Data Right (Energy Sector) Designation 2020, subsection 6(4). However, at the time of publication, AEMO is not a designated gateway for any CDR data because under current CDR Rules, no CDR data is (or is to be) disclosed to AEMO because of the reasons in paragraph 56AL(2)(c) of the Competition and Consumer Act.

There are also no designated gateways in the telecommunications sector, although unlike the banking and energy sectors at the date of publication of these guidelines, there are no rules allowing for the sharing of designated telecommunications data under the CDR system: Consumer Data Right (Telecommunications Sector) Designation 2022.

⁶ CDR Rule 7.7, which relates to Privacy Safeguard 6, only applies accredited data recipients.

⁷ A CDR representative arrangement is a written contract between a CDR representative and their CDR representative principal. The requirements for this arrangement are outlined in CDR Rules, rule 1.10AA.

⁸ CDR rules, subrule 1.10AA(4)(a)(iib).

⁹ CDR Rules, paragraphs 1.10AA(4)(c) and (d).

¹⁰ CDR Rules, subrule 7.6(4). See also rule 1.16A in relation to a CDR representative principal's obligations and liability.

arrangement with their OSP principal,¹¹ an OSP is required to comply with Privacy Safeguard 7 in its handling of service data as if it were the OSP principal.¹² It also must not use or disclose the service data unless doing so would be in accordance with the CDR outsourcing arrangement.¹³ Further, any use or disclosure of service data by the OSP is taken to have been a use or disclosure by their OSP principal (regardless of whether the OSP's actions accord with the CDR outsourcing arrangement).¹⁴

How Privacy Safeguard 7 interacts with the Privacy Act

7.11 It is important to understand how Privacy Safeguard 7 interacts with the Privacy Act and the APPs.¹⁵

7.12 APP 7 sets out when an APP entity is prohibited from using or disclosing personal information for the purpose of direct marketing.

CDR entity	Privacy protections that apply in the CDR context
Accredited data recipient	<p>Privacy Safeguard 7</p> <p>For accredited data recipients of a consumer's CDR data, Privacy Safeguard 7 applies to any uses or disclosures of that CDR data for direct marketing.¹⁶</p> <p>APP 7 does not apply in relation to that CDR data.¹⁷</p>
Designated gateway	Privacy Safeguard 7

¹¹ A CDR outsourcing arrangement is a written contract between an OSP principal and their provider that meets the minimum requirements listed in CDR Rules, subrule 1.10(3).

¹² CDR Rules, paragraph 1.10(3)(b)(i)(D),

¹³ CDR Rules, paragraph 1.10(3)(b)(iv).

¹⁴ CDR Rules, subrule 7.6(5). See also rule 1.16 in relation to an OSP principal's obligations and liability.

¹⁵ The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies (APP entities).

¹⁶ Privacy Safeguard 7 applies from the point when the accredited person becomes an accredited data recipient of the CDR data. An accredited person becomes an accredited data recipient for CDR data when:

- CDR data is held by (or on behalf of) the person
- the CDR data, or any other CDR data from which it was directly or indirectly derived, was disclosed to the person under the consumer data rules, and
- the person is neither a data holder, nor a designated gateway, for the first mentioned CDR data. See Competition and Consumer Act, section 56EK.

¹⁷ The APPs do not apply to an accredited data recipient of CDR data, in relation to that CDR data: Competition and Consumer Act, paragraph 56EC(4)(a). However, subsection 56EC(4) does not affect how the APPs apply to accredited persons and accredited data recipients who are APP entities, in relation to the handling of personal information outside the CDR system. (Note: Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See Privacy Act, subsection 6E(1D).) Subsection 56EC(4) also does not affect how the APPs apply to an accredited person who does not become an accredited data recipient of the CDR data (other than for Privacy Safeguards 1 – 4). See Competition and Consumer Act, paragraph 56EC(5)(aa).

CDR entity	Privacy protections that apply in the CDR context
	For designated gateways for CDR data, Privacy Safeguard 7 applies to the use and disclosure of the CDR data for direct marketing. ¹⁸ APP 7 does not apply in relation to that CDR data. ¹⁹
Data holder²⁰	APP 7 Privacy Safeguard 7 does not apply to a data holder.

What is direct marketing?

- 7.13 ‘Direct marketing’ is not defined in the *Competition and Consumer Act 2010* (Competition and Consumer Act). The term is also used in APP 7 but is not defined in the Privacy Act.²¹
- 7.14 For the purpose of Privacy Safeguard 7, ‘direct marketing’ takes its ordinary meaning, and involves an entity’s use or disclosure of CDR data to communicate directly with a consumer to promote goods and services.
- 7.15 An example of direct marketing by an entity includes sending an email to a consumer promoting financial products using the consumer’s CDR data.²²
- 7.16 ‘Direct marketing’ is distinct from the situation where:
- a consumer has requested a good or service
 - the accredited data recipient has obtained the consumer’s consent to collect and use the consumer’s CDR data to provide this good or service, and
 - the requested good or service is to provide the consumer with offers about suitable products (for example, a service offered by a comparison site).²³

This is illustrated in the following examples.

Example 1 – comparison site

Kwok wishes to obtain suitable offers from multiple providers for electricity plans and provides Tang and Co Pty Ltd, an accredited person, with a valid request to collect his CDR data from the relevant data holders of his CDR data for this purpose.

¹⁸ Competition and Consumer Act, subsection 56EJ(2).

¹⁹ The APPs do not apply to designated gateways for CDR data in relation to that CDR data: Competition and Consumer Act, paragraph 56EC(4)(d). However, subsection 56EC(4) does not affect how the APPs apply to designated gateways who are APP entities, in relation to the handling of personal information outside the CDR system. See Competition and Consumer Act, paragraph 56EC(5)(b).

²⁰ In this chapter, references to data holders include AEMO. See [Chapter B \(Key concepts\)](#) for further information about how the privacy safeguards apply to AEMO.

²¹ For the purposes of APP 7, the phrase has been interpreted to take its ordinary meaning of marketing addressed directly to individuals (*Shahin Enterprises Pty Ltd v BP Australia Pty Ltd* [2019] SASC 12 [113] (Blue J)). It involves the use or disclosure of personal information to communicate directly with an individual to promote goods and services (Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 81).

²² For information regarding ‘valid requests’, see [Chapter 3 \(Privacy Safeguard 3\)](#).

²³ Explanatory Statement to the CDR Rules.

Tang and Co provides Kwok with offers for electricity plans as requested, using Kwok's CDR data that it has collected in accordance with the CDR Rules.

Example 2 – switching banking providers

Guy is considering switching banking providers for his credit card and provides McCarthy Bank, an accredited person, with a valid request to collect his CDR data from his existing bank for the purpose of providing suitable offers in relation to credit cards.

McCarthy Bank provides Guy with the offers for credit card products as requested, using Guy's CDR data it has collected in accordance with the CDR Rules.

In both examples, the uses of the consumer's CDR data by the accredited person (Tang and Co/McCarthy Bank) would not be 'direct marketing' and Privacy Safeguard 7 would not apply. The accredited person's use of the consumer's CDR data would be a permitted use under Privacy Safeguard 6 as the CDR data would be used for the purpose of providing the service requested by the consumer (Kwok/Guy).

However, if Tang and Co or McCarthy Bank were to use Kwok or Guy's CDR data to provide offers about other products not requested by the consumer, this would likely be 'direct marketing' and if so would be permitted only if this was authorised under the CDR Rules.²⁴

When is direct marketing allowed?

7.17 Generally, an entity is not permitted to engage in direct marketing under the CDR system.

7.18 However, the CDR Rules permit an accredited data recipient of CDR data to engage in certain specific direct marketing activities in accordance with a 'direct marketing consent', in relation to:

- the 'existing goods or services' being provided to the consumer, or
- other goods or services provided by another accredited person.²⁵

7.19 The 'existing goods or services' refer to the goods or services requested by the consumer.²⁶

7.20 A 'direct marketing consent' is a consent provided by a consumer under the CDR Rules for an accredited data recipient to use or disclose CDR data for the purposes of direct marketing.²⁷ An accredited person must ask for the consumer's express consent in accordance with Division 4.3 of the CDR Rules for any direct marketing they intend to undertake.²⁸

7.21 Subrule 7.5(3) of the CDR Rules allows an accredited data recipient to use or disclose CDR data for the following permitted direct marketing activities:

- in accordance with a consumer's direct marketing consent:

²⁴ This would be 'direct marketing' even where the offers were about other products related to the requested product.

²⁵ CDR Rules, rule 7.8 and subrule 7.5(3). Examples of existing goods or services include the services provided by Tang and Co to Kwok, and McCarthy Bank to Guy, in the examples under paragraph 7.16.

²⁶ CDR Rules, paragraph 7.5(1)(a).

²⁷ CDR Rules, subrule 1.10A(1)(d). See Chapter B (Key concepts) for further information on direct marketing consents.

²⁸ See especially CDR Rules, paragraphs 4.11(1)(a)(ii) and 4.11(1)(c) and subrule 4.11(2). For guidance regarding the requirements for seeking direct marketing consents, see [Chapter C \(Consent\)](#).

- sending the consumer information about upgraded or alternative goods or services to the existing goods or services
- sending the consumer an offer to renew existing goods or services when they expire
- sending the consumer information about the benefits of existing goods or services
- sending the consumer information about other goods and services provided by another accredited person if the accredited data recipient reasonably believes the consumer might benefit from these other goods or services, and only sends such information on a reasonable number of occasions, and
- disclosing the consumer's CDR data to an accredited person so that the accredited person may provide the goods or services referred to in the dot point above, but only where the consumer has provided a relevant collection, use and disclosure consent
- using CDR data in a way and to the extent that is reasonably needed in order to send the consumer something permitted by the paragraph above (including by analysing the CDR data to identify the appropriate information to send)
- disclosing the consumer's CDR data to a direct or indirect OSP:
 - for the purpose of doing the things referred to in the above 2 paragraphs, and
 - to the extent reasonably needed to do those things, and
- where the accredited data recipient is a CDR representative principal – disclosing CDR data to a CDR representative under a CDR representative arrangement for the purposes of specified direct marketing-related uses or disclosures by the CDR representative.²⁹

Information about upgraded or alternative goods or services

7.22 Sending the consumer information about upgraded³⁰ or alternative³¹ goods or services is direct marketing.³² An accredited data recipient of CDR data may only engage in this form of direct marketing if it has obtained a direct marketing consent (which is still current) from the consumer under Division 4.3 of the CDR Rules.³³

Example

Loan Tracker Pty Ltd is an accredited person that offers products and services to assist consumers to monitor and repay their loans.

²⁹ CDR Rules, paragraph 7.5(3)(e). See paragraph 7.42 - 7.43 for more information on the specified uses or disclosures by CDR representatives.

³⁰ A good or service will be an 'upgraded' good or service if the good or service is an improved version of the existing good or service.

³¹ A good or service will be an 'alternative' good or service if a consumer could choose between that good or service and the existing good or service in order to achieve a similar outcome.

³² CDR Rules, paragraph 7.5(3)(a)(i).

³³ See especially CDR Rules, paragraphs 4.11(1)(a)(ii) and 4.11(1)(c) and subrule 4.11(2). For guidance regarding the requirements for seeking direct marketing consents, see [Chapter C \(Consent\)](#).

Loan Tracker asks its customers for their consent to receive direct marketing information about upgraded or alternative goods or services when seeking their consent to collect and use their CDR data to provide the requested service.

Through the ‘Show Me My Money’ service offered by Loan Tracker, monthly emails are sent to consumers setting out their current aggregate loan balances, the amount required to be repaid over the month, and estimating the consumer’s disposable income for that month after repayments and living expenses are taken into account.

Loan Tracker also wishes to include in its monthly emails links to information about other products and services offered by Loan Tracker which it considers might be useful to the consumer.

If Loan Tracker includes these links to information about other products and services, this may constitute using consumers’ CDR data to directly market its other products and services.

Loan Tracker may only use the CDR data to engage in the direct marketing activities if it:

- *has obtained a direct marketing consent (which is still current) for the purpose of sending information about upgraded or alternative goods or services, and*
- *is able to show that the other products and services marketed are truly ‘upgraded’ or ‘alternative’ services to the ‘Show Me My Money’ service.*

Offer to renew existing goods or services

7.23 Sending the consumer an offer to renew the existing goods or services is direct marketing.³⁴ An accredited data recipient may only engage in this form of direct marketing if it has obtained a direct marketing consent (which is still current) from the consumer under Division 4.3 of the CDR Rules.³⁵

7.24 If the consumer wishes to ‘renew’ the existing goods or services, the accredited data recipient must once again seek the consumer’s consent to the collection, use and (if applicable) disclosure of their CDR data for the relevant good or service. This is because an accredited person may seek to collect CDR data only in response to a valid request from the consumer.³⁶

7.25 An accredited data recipient may, in certain cases, invite a consumer to amend the duration of a consent (including a direct marketing consent), for example by extending its duration.³⁷ Where an accredited data recipient wishes to issue such an invitation, they should first consider whether the invitation would constitute an offer to renew the existing goods or services under paragraph 7.5(3)(a)(ii) of the CDR Rules (in which case a direct marketing consent would be required).

³⁴ CDR Rules, paragraph 7.5(3)(a)(ii).

³⁵ See especially CDR Rules, paragraphs 4.11(1)(a)(ii) and 4.11(1)(c) and subrule 4.11(2). For guidance regarding the requirements for seeking direct marketing consents, see [Chapter C \(Consent\)](#).

³⁶ The consumer’s consent to the collection and use of their CDR data for an accredited person to provide goods or services is required for a ‘valid request’: CDR Rules, rule 4.3. For information regarding valid requests and the requirements for seeking consent, see [Chapter C \(Consent\)](#).

³⁷ CDR Rules, rule 4.12B. For further information about the requirements for asking a consumer to amend their consent, see CDR Rules, rule 4.12C and [Chapter C \(Consent\)](#).

Information about the benefits of existing goods or services

7.26 Sending the consumer information about the benefits of the existing goods or services being used by the consumer is direct marketing.³⁸ An accredited data recipient may only engage in this form of direct marketing if it has obtained a direct marketing consent (which is still current) from the consumer under Division 4.3 of the CDR Rules.³⁹

Information about other goods or services provided by another accredited person

7.27 Sending the consumer information about other goods or services provided by another accredited person is direct marketing. An accredited data recipient may only engage in this form of direct marketing if it:

- has obtained a direct marketing consent from the consumer under Division 4.3 of the CDR Rules⁴⁰
- reasonably believes that the consumer might benefit from the goods or services offered by the other accredited person, and
- sends such information to the consumer on no more than a reasonable number of occasions.⁴¹

Disclosure to another accredited person to enable provision of promoted goods and services

7.28 An accredited data recipient of CDR data is permitted to disclose a consumer's CDR data to another accredited person for the purposes of enabling that accredited person to provide the goods or services outlined in paragraph 7.27.⁴²

7.29 An accredited data recipient may only disclose CDR data to another accredited person if the consumer has provided both a direct marketing consent and a disclosure consent to the accredited data recipient in accordance with Division 4.3 of the CDR Rules, and has also provided a collection consent and a use consent to the accredited person who will receive the data.⁴³

³⁸ CDR Rules, paragraph 7.5(3)(a)(iii).

³⁹ See especially CDR Rules, paragraphs 4.11(1)(a)(ii) and 4.11(1)(c) and subrule 4.11(2). For guidance regarding the requirements for seeking direct marketing consents, see [Chapter C \(Consent\)](#).

⁴⁰ See especially CDR Rules, paragraphs 4.11(1)(a)(ii) and 4.11(1)(c) and subrule 4.11(2). For guidance regarding the requirements for seeking direct marketing consents, see [Chapter C \(Consent\)](#).

⁴¹ CDR Rules, paragraph 7.5(3)(a)(iv).

⁴² CDR Rules, paragraph 7.5(3)(b).

⁴³ For information regarding direct marketing consents and disclosure consents, see [Chapter C \(Consent\)](#).

Using the CDR data as reasonably needed, in accordance with the data minimisation principle

- 7.30 Using CDR data for the purpose of sending the information or renewal offer outlined above in paragraphs 7.22, 7.23, 7.26, 7.27 and 7.28, including by analysing the data to decide what, if any, information will be sent, is direct marketing.⁴⁴
- 7.31 In order to use the CDR data for this purpose, the underlying direct marketing consent for the sending of information or renewal offers must be current.
- 7.32 An accredited data recipient must comply with the data minimisation principle when using the CDR data for these direct marketing purposes. This means that the CDR data, and any CDR data derived from it, must only be used as reasonably needed to fulfil the relevant direct marketing purpose.
- 7.33 For further information on the data minimisation principle, see [Chapter B \(Key concepts\)](#).

Privacy tip: An accredited data recipient must allow a consumer to withdraw their direct marketing consent by:⁴⁵

- using their dashboard, or
- through a ‘simple alternative method of communication’ made available for that purpose, such as an embedded link in an email communication through which they may notify the accredited data recipient of their intention to ‘opt out’.

For further information regarding withdrawal of consent, see [Chapter C \(Consent\)](#).

Disclosure to an outsourced service provider

- 7.34 An accredited data recipient is permitted to disclose CDR data to a direct or indirect OSP for the purpose of sending the information or renewal offer (outlined above in paragraphs 7.22, 7.23, 7.26, 7.27 and 7.28), or to use the CDR data (as outlined above in paragraph 7.30).⁴⁶
- 7.35 An accredited data recipient may only disclose CDR data to the extent reasonably needed to do those things.⁴⁷
- 7.36 Under this permitted disclosure, accredited persons may engage third parties (who fall within the meaning of ‘OSP’)⁴⁸ to undertake direct marketing activities on their behalf, where such activities are permitted under subrule 7.5(3) of the CDR Rules.
- 7.37 In order to disclose the CDR data for this purpose, the underlying direct marketing consent to send information or renewal offers must be current. In addition, the accredited person must:

⁴⁴ CDR Rules, paragraph 7.5(3)(c).

⁴⁵ CDR Rules, subrule 4.13(1).

⁴⁶ CDR Rules, paragraph 7.5(3)(d)(i).

⁴⁷ CDR Rules, paragraph 7.5(3)(d)(ii).

⁴⁸ See CDR Rules, rule 1.10. ‘Outsourced service provider’ is discussed in [Chapter B \(Key concepts\)](#).

- provide the information required by paragraph 4.11(3)(f) of the CDR Rules to the consumer at the time of seeking the consumer’s consent to collect and use the consumer’s CDR data, and
 - include certain information about OSPs in its CDR policy.⁴⁹
- 7.38 An accredited data recipient who discloses CDR data to an OSP must ensure that the provider complies with its requirements under the CDR outsourcing arrangement.⁵⁰
- 7.39 For the purposes of this permitted disclosure, an OSP is a person to whom an accredited data recipient discloses⁵¹ CDR data under a CDR outsourcing arrangement.⁵²
- 7.40 If the disclosure is proposed to be made to an overseas OSP, Privacy Safeguard 8 will apply in addition to Privacy Safeguard 7 (see [Chapter 8 \(Privacy Safeguard 8\)](#)).
- 7.41 For further information, see [Chapter B \(Key Concepts\)](#), ‘Outsourced service providers’. For further guidance regarding an accredited data recipient’s obligations in relation to OSPs, see [Chapter 6 \(Privacy Safeguard 6\)](#).

Disclosure to a CDR representative

- 7.42 Where an accredited data recipient is a CDR representative principal, they are permitted to disclose CDR data to a CDR representative under a CDR representative arrangement for the purposes of the CDR representative:⁵³
- in accordance with a direct marketing consent, sending to the CDR consumer:
 - information about upgraded or alternative goods or services
 - offers to renew existing goods or services
 - information about the benefits of existing goods or services, or
 - information about other goods or services provided by another accredited person, where the CDR representative reasonably believes the consumer might benefit from those other goods or services, and sends such information to the consumer on no more than a reasonable number of occasions, or
 - using the CDR data as reasonably needed to send the above information to the CDR consumer (including by analysing the CDR data to identify the appropriate information to send)
 - disclosing the CDR consumer’s CDR data to a direct or indirect OSP of the CDR representative for the purpose of specified direct marketing activities, and to the extent reasonably needed to do those things.
- 7.43 See paragraphs 7.22 -7.27 and 7.30 - 7.33 for more information on these permitted purposes.

⁴⁹ CDR Rules, subrule 7.2(4). See [Chapter 1 \(Privacy Safeguard 1\)](#).

⁵⁰ CDR Rules, rule 1.16.

⁵¹ Data will be ‘disclosed’ under the CDR system where it is made accessible or visible to others outside the entity. Whether an accredited data recipient retains effective control over the data does not affect whether data is ‘disclosed’.

⁵² CDR Rules, rule 1.10. A CDR outsourcing arrangement is a written contract between the accredited data recipient and OSP which meets the requirements set out in subrule 1.10(3) of the CDR Rules, and under which the provider will provide goods or services to the accredited data recipient. For further information, see [Chapter B \(Key Concepts\)](#).

⁵³ CDR Rules, paragraph 7.5(3)(e).

Risk point: As soon as the customer’s direct marketing consent is no longer current (i.e. because it expires or is withdrawn), the accredited data recipient can no longer engage in the permitted uses or disclosure relating to direct marketing under the CDR Rules.

Privacy tip: Accredited data recipients should have processes and systems in place to promptly inform any OSPs engaging in direct marketing activities of the expiry of a consumer’s direct marketing consent.⁵⁴

Interaction with other privacy safeguards

- 7.44 The prohibition against direct marketing in Privacy Safeguard 7 is complemented by Privacy Safeguards 6 (see [Chapter 6 \(Privacy Safeguard 6\)](#)), 8 (see [Chapter 8 \(Privacy Safeguard 8\)](#)) and 9 (see [Chapter 9 \(Privacy Safeguard 9\)](#)).
- 7.45 Privacy Safeguard 6 prohibits an accredited data recipient of CDR data from using or disclosing CDR data unless required or authorised under the CDR Rules or another Australian law or court or tribunal order.
- 7.46 Privacy Safeguard 8 restricts disclosures of CDR data made to recipients located overseas.
- 7.47 Privacy Safeguard 9 prohibits an accredited data recipient of CDR data that contains a government related identifier from adopting, using or disclosing that identifier, unless an exception applies.

Interaction with other legislation

- 7.48 Under the Privacy Act, APP 7 does not apply to the extent that the *Do Not Call Register Act 2006*, the *Spam Act 2003* or any other legislation prescribed by the regulations applies (APP 7.8). There is no corresponding exemption under Privacy Safeguard 7.
- 7.49 This means that if an accredited data recipient or designated gateway engages in a form of direct marketing that may be permitted under another Act,⁵⁵ and the entity uses or discloses CDR data for that purpose, the entity will be in breach of Privacy Safeguard 7 unless that use or disclosure is required or authorised under the CDR Rules.
- 7.50 Similarly, this means that if an accredited data recipient or designated gateway engages in a form of direct marketing permitted under Privacy Safeguard 7 and the CDR Rules, the entity may nevertheless be in breach of another Act if the requirements relating to marketing communications under that Act are not also satisfied.

⁵⁴ This will assist the accredited data recipient in directing an OSP under paragraph 1.10(3)(b)(v) of the CDR Rules.

⁵⁵ For instance, a person may make telemarketing calls to a number registered on the Do Not Call Register if the relevant account holder has consented to the making of the call: *Do Not Call Register Act 2006*, subsection 11(2).

Chapter 8:

Privacy Safeguard 8 —

Overseas disclosure of CDR data by accredited data recipients

Version 5.0, November 2023



Contents

Key points	3
What does Privacy Safeguard 8 say?	3
Why is this important?	4
Who does Privacy Safeguard 8 apply to?	4
How Privacy Safeguard 8 interacts with the Privacy Act	5
Meaning of disclosure	6
What is an overseas recipient?	6
When can CDR data be disclosed to an overseas recipient?	6
Exception 1 — Disclosing CDR data to an overseas recipient who is an accredited person	9
Exception 2 — Disclosing CDR data after taking ‘reasonable steps’ to ensure an overseas recipient does not breach the privacy safeguards	9
Exception 3 — Disclosing CDR data where overseas recipient is subject to a relevant law or binding scheme	11
When is an accredited data recipient accountable for the breaches by an overseas recipient?	13
How does Privacy Safeguard 8 interact with the other privacy safeguards?	14
Privacy Safeguard 6	14
Privacy Safeguard 7	14
Privacy Safeguard 9	14

Key points

- Privacy Safeguard 8¹ sets out the circumstances in which an accredited data recipient of a consumer's CDR data can disclose that data to a recipient located overseas.
- Under Privacy Safeguard 8, an accredited data recipient of a consumer's CDR data must not disclose that data to a recipient located overseas (other than the CDR consumer) unless one of the following exceptions applies:
 - the overseas recipient is also an accredited person
 - the accredited data recipient takes reasonable steps to ensure the overseas recipient will not breach privacy safeguard penalty provisions (noting that, for this exception, the accredited data recipient remains accountable for any breach of the relevant privacy safeguards by the overseas recipient), or
 - the accredited data recipient reasonably believes the overseas recipient is subject to a law or a binding scheme equivalent to the privacy safeguards and there are mechanisms available to the consumer to enforce that protection.
- These requirements are in addition to the other disclosure restrictions set out in Privacy Safeguards 6, 7 and 9 and the consumer data rules (CDR Rules).

What does Privacy Safeguard 8 say?

- 8.1 In addition to the disclosure restrictions set out in Privacy Safeguards 6, 7 and 9, and the CDR Rules, an accredited data recipient of a consumer's CDR data must not disclose that data to a person located overseas unless one of the following 4 exceptions applies:
- a. the overseas recipient is an accredited person
 - b. the accredited data recipient takes reasonable steps to ensure the overseas recipient does not breach the relevant privacy safeguards² and the overseas recipient has a CDR policy in place in relation to the CDR data
 - c. the accredited data recipient reasonably believes the overseas recipient is bound by a law or binding scheme that provides substantially similar protection for the CDR data as the privacy safeguards provide in relation to accredited data recipients, and a consumer will be able to enforce that law or scheme in relation to the CDR data, or
 - d. conditions specified in the CDR Rules for overseas disclosure are met. As there are currently no CDR Rules made for the purposes of this exception, an accredited data recipient cannot rely on this exception.
- 8.2 Where the overseas recipient is not accredited or subject to a similar law or binding scheme to the privacy safeguards, even if an accredited data recipient takes reasonable steps to ensure the overseas recipient does not breach the privacy safeguards, but the overseas

¹ Competition and Consumer Act, section 56EK.

² The relevant privacy safeguards are the privacy safeguard penalty provisions as defined in section 56EU of the Competition and Consumer Act (Privacy Safeguards 3–13 inclusive, and the requirement to have a CDR policy in Privacy Safeguard 1).

recipient nevertheless breaches a relevant privacy safeguard, the accredited data recipient remains accountable for that breach.

- 8.3 For the purposes of a CDR outsourcing arrangement, an accredited data recipient must also comply with the CDR Rules that relate to CDR outsourcing arrangements.³

Why is this important?

- 8.4 As an overarching objective of the CDR system, consumers should be able to trust that an accredited data recipient will manage CDR data appropriately and in compliance with the privacy safeguards, including when CDR data is disclosed overseas.
- 8.5 It is also important that entities are aware of and understand the obligations on them to protect CDR data where they seek to make a disclosure of CDR data to an overseas recipient.

Who does Privacy Safeguard 8 apply to?

- 8.6 Privacy Safeguard 8 applies to accredited data recipients of CDR data. It does not apply to data holders or designated gateways.
- 8.7 Data holders and designated gateways should ensure that they adhere to their obligations under the *Privacy Act 1988* (Privacy Act) and the APPs, including APP 8, when disclosing personal information to an overseas recipient.
- 8.8 As a non-accredited entity, a CDR representative is not directly bound by Privacy Safeguard 8. However, under the terms of the CDR representative arrangement with their CDR representative principal,⁴ a CDR representative is required to comply with Privacy Safeguard 8 as if it were an accredited data recipient.^{5,6} A CDR representative principal breaches subrule 7.8A(1) of the CDR Rules if its CDR representative fails to comply with Privacy Safeguard 8 in relation to service data as if it were an accredited data recipient of the service data.⁷
- 8.9 Where they are a non-accredited entity, an outsourced service provider (OSP) is not directly bound by Privacy Safeguard 8. However, under the terms of the CDR outsourcing arrangement with their OSP principal,⁸ an OSP is required to comply with Privacy Safeguard 8 in its handling of service data as if it were the OSP principal.⁹ An accredited person breaches subrule 7.8B(1) of the CDR Rules if a direct or indirect OSP of the accredited

³ CDR Rules, rule 1.10, subrule 1.16, paragraph 7.5(1)(f) and rule 7.6. For more information on CDR outsourcing arrangements, please refer to [Chapter B \(Key concepts\)](#).

⁴ A CDR representative arrangement is a written contract between a CDR representative and their CDR representative principal. The requirements for this arrangement are outlined in CDR Rules, rule 1.10AA.

⁵ CDR Rules, paragraph 1.10AA(4)(g).

⁶ See [Chapter B \(Key concepts\)](#) for more information on 'CDR representative principal', 'CDR representative', 'CDR representative arrangement' and 'service data'.

⁷ CDR Rules, subrule 7.8A(1). See also rule 1.16A in relation to a CDR representative principal's obligations and liability.

⁸ A CDR outsourcing arrangement is a written contract between an OSP principal and their provider that meets the minimum requirements listed in CDR Rules, subrule 1.10(3).

⁹ CDR Rules, rule 1.10(3)(b)(i)(E).

person or of their CDR representative, fails to comply with Privacy Safeguard 8 as if it were an accredited data recipient of that service data.¹⁰

How Privacy Safeguard 8 interacts with the Privacy Act

8.10 It is important to understand how Privacy Safeguard 8 interacts with the Privacy Act and the APPs.¹¹

8.11 APP 8 outlines when an APP entity may disclose personal information about an individual to an overseas recipient (see APP Guidelines, [Chapter 8 \(APP 8\)](#)).

CDR entity	Privacy protections that apply in the CDR context
Accredited data recipient	<p>Privacy Safeguard 8</p> <p>For accredited data recipients of a consumer’s CDR data, Privacy Safeguard 8 applies to any overseas disclosures of that CDR data.¹²</p> <p>APP 8 does not apply in relation to that CDR data.¹³</p>
Designated gateway	<p>APP 8</p> <p>Privacy Safeguard 8 does not apply to a designated gateway.</p>
Data holder¹⁴	<p>APP 8</p> <p>Privacy Safeguard 8 does not apply to a data holder.</p>

¹⁰ CDR Rules, rule 7.8B(1). See also rule 1.16 in relation to an OSP principal’s obligations and liability.

¹¹ The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies (APP entities).

¹² Privacy Safeguard 8 applies from the point when the accredited person becomes an accredited data recipient of the CDR data. An accredited person becomes an accredited data recipient for CDR data when:

- CDR data is held by (or on behalf of) the person
- the CDR data, or any other CDR data from which it was directly or indirectly derived, was disclosed to the person under the consumer data rules, and
- the person is neither a data holder, nor a designated gateway, for the first mentioned CDR data. See section 56EK of the Competition and Consumer Act.

¹³ The APPs do not apply to an accredited data recipient of CDR data, in relation to that CDR data: Competition and Consumer Act, paragraph 56EC(4)(a). However, subsection 56EC(4) does not affect how the APPs apply to accredited persons and accredited data recipients who are APP entities, in relation to the handling of personal information outside the CDR system. (Note: Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See Privacy Act, subsection 6E(1D).) Subsection 56EC(4) also does not affect how the APPs apply to an accredited person who does not become an accredited data recipient of the CDR data (other than for Privacy Safeguards 1 – 4). See Competition and Consumer Act, paragraph 56EC(5)(aa).

¹⁴ In this chapter, references to data holders include AEMO. See [Chapter B \(Key concepts\)](#) for further information about how the privacy safeguards apply to AEMO.

Meaning of disclosure

- 8.12 The term ‘disclose’ is not defined in the *Competition and Consumer Act 2010* (Competition and Consumer Act). It is discussed in [Chapter B \(Key concepts\)](#).
- 8.13 An accredited data recipient discloses CDR data when it makes it accessible or visible to others outside the entity.¹⁵
- 8.14 The release of the information may be a release in accordance with the CDR Rules, an accidental release or an unauthorised release.
- 8.15 This focuses on the act done by the disclosing party. The state of mind or intentions of the recipient does not affect the fact of disclosure. Further, there will be a disclosure even where the information is already known to the overseas recipient.
- 8.16 Where an accredited data recipient engages a third party to perform services on its behalf, the provision of CDR data to that provider will in most circumstances be a disclosure. However, in limited circumstances, providing CDR data to a third party to perform services on behalf of the entity may be a use, rather than a disclosure. See ‘disclosure’ and ‘use’ in [Chapter B \(Key concepts\)](#) for guidance on how to determine whether providing CDR data to a third party constitutes a use or disclosure.

What is an overseas recipient?

- 8.17 Under Privacy Safeguard 8, an overseas recipient is a person,¹⁶ who receives CDR data from an accredited data recipient, who is not:
- in Australia or in an external Territory, and
 - a consumer for the CDR data.¹⁷

When can CDR data be disclosed to an overseas recipient?

- 8.18 When making an overseas disclosure of CDR data, an accredited data recipient must comply with Privacy Safeguard 8 in addition to each of the other privacy safeguards and CDR Rules that relate to disclosure of CDR data (to the extent they are applicable to the relevant disclosure).¹⁸

¹⁵ Whether an accredited data recipient retains effective control over the data does not affect whether data is ‘disclosed’.

¹⁶ Being a body corporate, body politic or individual.

¹⁷ Competition and Consumer Act, paragraph 56EK(1)(b).

¹⁸ This includes Privacy Safeguard 6 and the CDR Rules relating to permitted disclosures (CDR Rules, subrules 7.5(1) and 7.5(2), and rules 7.5A, 7.6 and 7.7); Privacy Safeguard 7 and the CDR Rules relating to disclosure of CDR data for direct marketing (CDR Rules, subrule 7.5(3), and rules 7.6 and 7.8); Privacy Safeguard 9 relating to disclosure of government related identifiers; CDR Rules relating to AP disclosure consents (e.g. CDR Rules, rule 4.7B, paragraph 7.5(1)(e) and 7.5(1)(i) and subrule 7.5A(1); CDR Rules relating to TA disclosure consents (e.g. CDR Rules, paragraph 7.5(1)(e) and subrule 7.5A(2)); CDR Rules relating to insight disclosures (e.g. CDR Rules, paragraph 7.5(1)(e) and subrule 7.5A(3) and (4)); CDR rules relating to business consumer disclosures (e.g. paragraph 7.5(1)(e) and subrule 7.5A(5) and CDR Rules relating to OSPs and CDR outsourcing arrangements (e.g. CDR Rules paragraph 7.5(1)(f) and (h) and rule 7.6).

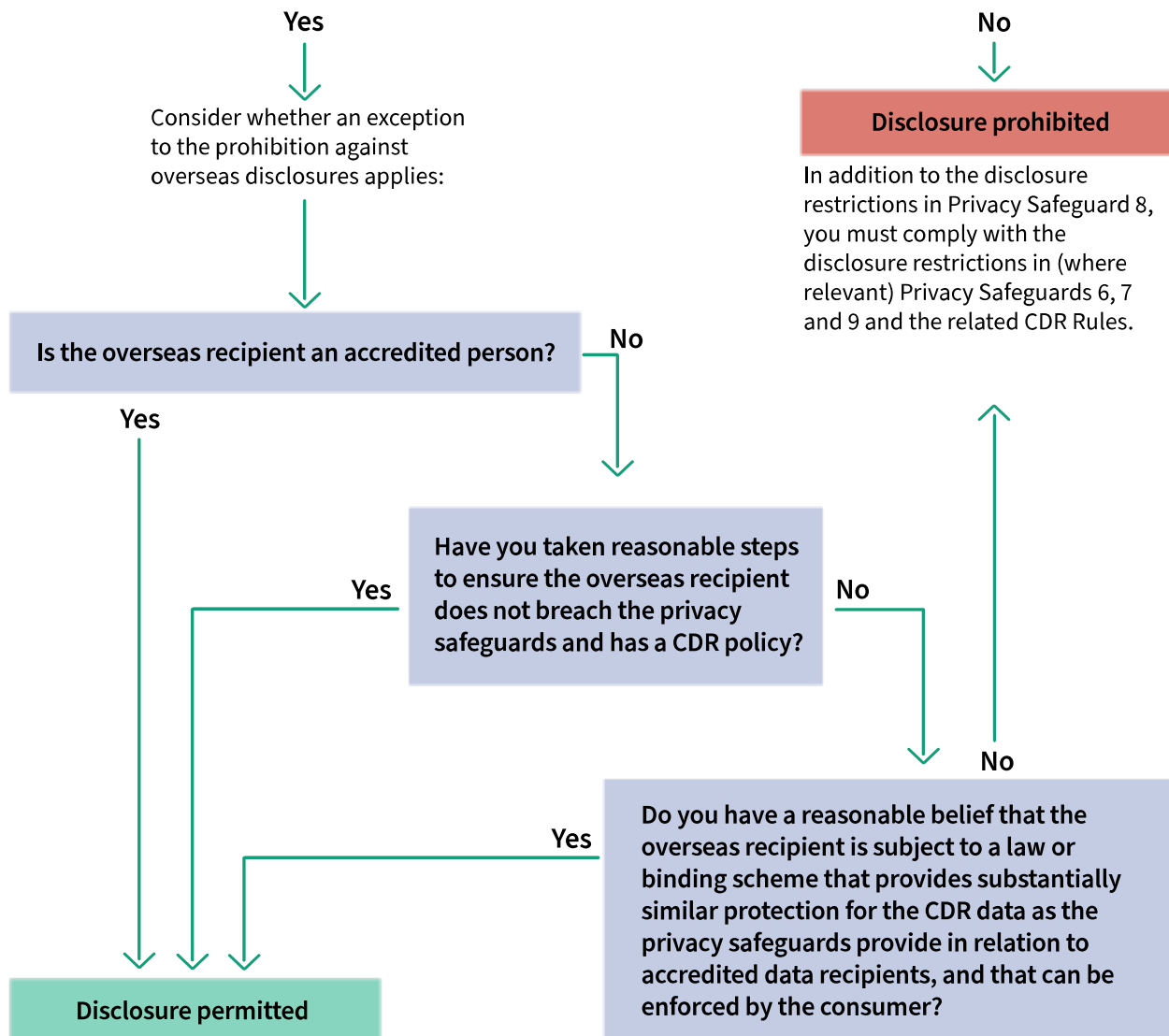
- 8.19 Privacy Safeguard 8 provides that an accredited data recipient must not disclose CDR data to a person located overseas unless one of the following 4 exceptions applies:
- the overseas recipient is an accredited person
 - the accredited data recipient takes reasonable steps to ensure the overseas recipient does not breach the relevant privacy safeguards¹⁹ and that the overseas recipient has a CDR policy in place in relation to the CDR data
 - the accredited data recipient reasonably believes the overseas recipient is bound by a law or binding scheme that provides substantially similar protection for the CDR data as the privacy safeguards provide in relation to accredited data recipients, and can be enforced by the consumer, or
 - conditions specified in the CDR Rules for overseas disclosure are met. As there are currently no CDR Rules in relation to Privacy Safeguard 8 which specify conditions for overseas disclosure, an accredited data recipient cannot currently rely on this exception.
- 8.20 The flow chart following outlines at a high level when an accredited data recipient may disclose CDR data to an overseas recipient, including by demonstrating the point at which the entity must consider other relevant privacy safeguards and CDR Rules, and relevant exceptions under Privacy Safeguard 8.

¹⁹ The relevant privacy safeguards are the privacy safeguard penalty provisions defined in section 56EU of the Competition and Consumer Act (Privacy Safeguards 3–13 inclusive, and the requirement to have a CDR policy in Privacy Safeguard 1).

When can an accredited data recipient disclose CDR data to an overseas recipient?

Have you complied with the general disclosure requirements and restrictions (where relevant) in:

- Privacy Safeguard 6 (for permitted disclosures of CDR data)?
- Privacy Safeguard 7 (for direct marketing)?
- Privacy Safeguard 9 (for disclosure of government related identifiers)?



Exception 1 — Disclosing CDR data to an overseas recipient who is an accredited person

- 8.21 An accredited data recipient may disclose CDR data to an overseas recipient if the person is an accredited person.²⁰
- 8.22 This exception may be relied upon only where the accredited data recipient has obtained a disclosure consent from the consumer to disclose CDR data to the accredited overseas recipient.²¹
- 8.23 The term ‘accredited person’ is discussed in [Chapter B \(Key concepts\)](#).
- 8.24 The CDR Rules require that an individual or company must apply to be an accredited person under the Competition and Consumer Act. An accreditation takes effect when the person is included in the Register of Accredited Persons.²²
- 8.25 The CDR Rules and the ACCC’s Accreditation Guidelines provide more information about the requirements and process for accreditation.
- 8.26 Accreditation is considered sufficient protection to ensure compliance with the privacy safeguards.²³

Exception 2 — Disclosing CDR data after taking ‘reasonable steps’ to ensure an overseas recipient does not breach the privacy safeguards

- 8.27 An accredited data recipient may disclose CDR data to an overseas recipient if the accredited data recipient takes reasonable steps to ensure that any act or omission by (or on behalf of) the overseas recipient will not breach privacy safeguard penalty provisions.²⁴
- 8.28 Any acts or omissions of the overseas recipient (or those who acted on behalf the overseas recipient) are also considered to be acts or omissions of the accredited data recipient who disclosed the CDR data.²⁵
- 8.29 Examples for persons acting on behalf of the overseas recipient could include employees, directors, officers, or subcontractors.

²⁰ Competition and Consumer Act, paragraph 56EK(1)(c).

²¹ Under the CDR Rules, an accredited data recipient may only disclose CDR data to an accredited person where they have a ‘disclosure consent’ from the consumer: see CDR Rules, rule 1.10A. A disclosure consent is a consent given by a consumer for the accredited data recipient to disclose CDR data to an accredited person: in response to consumer data request (an ‘AP disclosure consent’), or for the purposes of direct marketing: CDR Rules, paragraph 1.10A(1)(c). For further information on disclosure consents, see [Chapter C \(Consent\)](#).

²² CDR Rules, rule 5.8.

²³ Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019, section 1.351.

²⁴ Competition and Consumer Act, paragraph 56EK(1)(d).

²⁵ Competition and Consumer Act, subsections 56EK(2) and 56EK(3). See also Competition and Consumer Act, section 56AU.

What are ‘reasonable steps’?

8.30 Reasonable steps would generally involve, at a minimum, that an accredited data recipient enters into an enforceable contractual arrangement with the overseas recipient that requires the overseas recipient to handle the CDR data in accordance with:

- the relevant privacy safeguards, and
- the CDR Rules that relate to CDR outsourcing arrangements.²⁶

8.31 Whether an accredited data recipient has taken reasonable steps to ensure the overseas recipient can comply with the CDR system may include consideration of the following factors:

- the terms of the contract between the accredited data recipient and the overseas recipient
- steps taken by the accredited data recipient to monitor compliance with the contract
- the accredited data recipient’s relationship with the overseas recipient. More rigorous steps may be required when an entity discloses CDR data to an overseas recipient for the first time
- the nature of the overseas recipient, including the maturity of its processes and systems, and familiarity with CDR legislation (which may be derived from previous engagements with other CDR entities)
- the possible adverse consequences for a consumer if the CDR data is mishandled by the overseas recipient. More rigorous steps may be required as the risk of adversity increases
- the nature of the CDR data being disclosed. Where CDR data is sensitive in nature (and could, for example, cause financial or physical harm to a consumer if mishandled), it should be subject to more rigorous protections in the contractual arrangements
- existing technical and operational protections implemented by the overseas recipient to protect the CDR data (where these are not equivalent to the security requirements set out in Privacy Safeguard 12 and in Schedule 2 of the CDR Rules), and
- the practicability of taking protective steps, including time and cost involved. However, a CDR entity is not excused from ensuring that an overseas recipient is compliant with CDR legislation by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take particular steps will depend on whether the burden is excessive in all the circumstances.

Example

YC Pty Ltd is an accredited person that provides banking services and products to customers. YC Pty Ltd seeks to engage a contractor located overseas, Analysed Data Services, in order to offer certain data analytics services to its customers using their payments transactions data.

²⁶ CDR Rules, rule 1.10, subrule 1.16(1), paragraph 7.5(1)(f) and rule 7.6. For more information on CDR outsourcing arrangements, please refer to [Chapter B \(Key concepts\)](#).

YC Pty Ltd considers whether an exception under Privacy Safeguard 8 relating to overseas disclosures will apply.

Analysed Data Services is not an accredited person and is not subject to a law or scheme similar to that of the CDR system.

Before disclosing CDR data to Analysed Data Services, YC Pty Ltd must therefore take reasonable steps to ensure Analysed Data Services complies with the relevant privacy safeguards and has a CDR policy in place in relation to the CDR data.

YC Pty Ltd will remain accountable if Analysed Data Services mishandles the CDR data.

Exception 3 — Disclosing CDR data where overseas recipient is subject to a relevant law or binding scheme

8.32 An accredited data recipient may disclose CDR data to an overseas recipient if they reasonably believe:

- the overseas recipient is bound by a law or binding scheme that provides substantially similar protection for the CDR data as the privacy safeguards provide in relation to accredited data recipients, and
- this law or binding scheme can be enforced by the consumer.²⁷

What is ‘reasonable belief’?

8.33 To rely on this exception, an accredited data recipient must have a reasonable belief that an overseas recipient is subject to a law, or binding scheme that provides substantially similar protection for the CDR data as the privacy safeguards provide in relation to accredited data recipients, and that a consumer will be able to enforce the protections provided by that law or binding scheme.

8.34 An accredited data recipient must have a reasonable basis for the belief, which is an objective test and not merely a genuinely held subjective belief. It is the responsibility of the entity to be able to justify its reasonable belief.

What is a ‘law or binding scheme’?

8.35 An overseas recipient may be subject to a law or binding scheme, where, for example, it is:

- bound by a consumer data protection law that applies in the jurisdiction of the overseas recipient
- required to comply with another law that imposes comparable obligations to the CDR system, or
- subject to an industry scheme or code that is enforceable, irrespective of whether the overseas recipient was obliged or volunteered to participate or subscribe to the scheme or code.

²⁷ Competition and Consumer Act, paragraph 56EK(1)(e).

8.36 However, an overseas recipient may not be subject to a law or binding scheme where, for example:

- the overseas recipient is exempt from complying, or is authorised not to comply, with part, or all, of the consumer data protection law in the jurisdiction, or
- the overseas recipient can opt out of the binding scheme without notice and without returning or destroying the data.

What is meant by ‘substantially similar’?

8.37 A law or binding scheme would provide substantially similar protection for the CDR data if it would provide a comparable, or a higher level of privacy protection for the CDR data to that provided by the privacy safeguards in relation to accredited data recipients. Each provision of the law or scheme is not required to correspond directly to an equivalent privacy safeguard. Rather, the overall effect of the law or scheme is of central importance.

8.38 Whether there is substantially similar protection is a question of fact. Factors that may indicate that the overall effect is substantially similar, include:

- the law or scheme regulates the collection of consumer data in a comparable way
- the law or scheme requires the recipient to notify individuals about the collection of their consumer data
- the law or scheme requires the recipient to only use or disclose the consumer data for authorised purposes
- the law or scheme includes comparable data quality and data security standards, and
- the law or scheme includes a right to seek correction of consumer data.

When can a consumer enforce the protections?

8.39 A consumer will be able to enforce the protections when it has access to a mechanism to allow for the enforcement of a law or binding scheme that provides substantially similar protection to the CDR system.

8.40 A range of mechanisms may satisfy those requirements, ranging from a regulatory body similar to the Office of the Australian Information Commissioner (OAIC), to an accredited dispute resolution scheme, an independent tribunal, or a court with judicial functions and powers.

8.41 Factors that may be relevant in deciding whether the enforcement mechanism is accessible and effective include whether the mechanism:

- is independent of the overseas recipient that is required by the law or binding scheme to comply with the consumer data protections
- is a body with authority to consider a breach of any of the consumer data protections in the law or binding scheme
- is accessible to an individual, for example, the existence of the scheme is publicly known, and can be accessed by individuals directly and without payment of any unreasonable charge
- has the power to make a finding that the overseas recipient is in breach of the law or binding scheme and to provide a remedy to the individual, and

- is required to operate according to principles of procedural fairness.

When is an accredited data recipient accountable for the breaches by an overseas recipient?

- 8.42 Privacy Safeguard 8 provides that an accredited data recipient is also accountable for the acts or omissions of an overseas recipient where it discloses CDR data to an overseas recipient and:
- the overseas recipient is not an accredited person
 - the accredited data recipient does not reasonably believe that the overseas recipient is bound by a law or scheme that provides substantially similar protection for the CDR data as the privacy safeguards provide in relation to accredited data recipients, and that a consumer will be able to enforce protections provided by that law or scheme, or
 - the overseas recipient (or a person acting on behalf of the overseas recipient) breaches the relevant privacy safeguards²⁸ and/or does not have a CDR policy.²⁹
- 8.43 In these circumstances, for the purposes of Privacy Safeguard 8, the act or omission is also taken to have been done by the accredited data recipient. The accredited data recipient is taken to have breached the privacy safeguard.
- 8.44 Where an accredited data recipient takes reasonable steps to ensure the overseas recipient complies with the privacy safeguards, but the overseas recipient nevertheless breaches a relevant privacy safeguard, the accredited data recipient is also accountable for that breach.³⁰

Risk point: An accredited data recipient will be accountable under the CDR system for the acts and omissions of an overseas recipient under Privacy Safeguard 8 in the circumstances set out above at 8.42 - 8.44.

Privacy tip: Accredited data recipients should maintain strong governance mechanisms, policies and procedures in relation to overseas disclosures of CDR data, including outsourcing arrangements. An accredited person should ensure that all contracts that aim to ensure compliance with the 'reasonable steps' exception in Privacy Safeguard 8 contain enforceable provisions that extend to the acts or omissions of subcontractors. Disclosing CDR data to overseas participants who are either accredited persons or bound by a law, or binding scheme that provides substantially similar protection for the CDR data as the privacy safeguards provide in relation to accredited data recipients will reduce the risk profile for an accredited data recipient.

²⁸ The relevant privacy safeguards are those privacy safeguard penalty provisions in defined in s 56EU of the Competition and Consumer Act (privacy safeguards 3–13 inclusive, and the requirement to have a CDR policy in Privacy Safeguard 1).

²⁹ Competition and Consumer Act, subsection 56EK(2).

³⁰ Competition and Consumer Act, subsections 56EK(2) and (3). See also Competition and Consumer Act, section 56AU.

- 8.45 There are also other conditions in the CDR regulatory framework that affect when an accredited data recipient is liable when making an overseas disclosure:
- Subsection 56AU(2) of the Competition and Consumer Act provides that acts done by or in relation to another person who is acting on behalf of a CDR entity, within the person's actual or apparent authority, are taken to have also been done in relation to the CDR entity,³¹ and
 - In relation to the use of CDR outsourcing arrangements:
 - subrule 7.8B(1) of the CDR Rules provides that an accredited person breaches that Rule if a direct or indirect OSP of the accredited person, or of their CDR representative, fails to comply with Privacy Safeguard 8 as if they were an accredited data recipient of the service data
 - subrule 7.6(2) of the CDR Rules provides that an accredited data recipient will be liable for any use or disclosure of CDR data by any of its direct or indirect OSP, or a direct or indirect OSP of its CDR representatives
 - subrule 7.6(5) of the CDR Rules provides that an accredited data recipient will be liable for the handling of any CDR data collected by its direct or indirect OSP.

How does Privacy Safeguard 8 interact with the other privacy safeguards?

Privacy Safeguard 6

- 8.46 In addition to Privacy Safeguard 8, an accredited data recipient should consider Privacy Safeguard 6 when determining whether to disclose CDR data to an overseas recipient.
- 8.47 This includes whether the disclosure is a permitted disclosure for the purposes of Privacy Safeguard 6 and also whether the accredited data recipient will need to comply with CDR outsourcing arrangements relating to OSPs. See [Chapter 6 \(Privacy Safeguard 6\)](#).

Privacy Safeguard 7

- 8.48 In addition to Privacy Safeguard 8, an accredited data recipient should consider Privacy Safeguard 7 where they are seeking to disclose CDR data to engage in permitted direct marketing activities. See [Chapter 7 \(Privacy Safeguard 7\)](#).

Privacy Safeguard 9

- 8.49 In addition to Privacy Safeguard 8, an accredited data recipient should also consider Privacy Safeguard 9 where CDR data it is seeking to disclose to an overseas recipient contains government identifiers. See [Chapter 9 \(Privacy Safeguard 9\)](#).

³¹ See also Competition and Consumer Act, subsection 56AU(1), which provides that the conduct of agents of a CDR entity are attributable to the CDR entity.

Chapter 9:

Privacy Safeguard 9 —

Adoption or disclosure of government related identifiers by accredited data recipients

Version 5.0, November 2023

Contents

Key points	3
What does Privacy Safeguard 9 say?	3
Why is it important?	3
Who does Privacy Safeguard 9 apply to?	4
How Privacy Safeguard 9 interacts with the Privacy Act	4
Meaning of government related identifier	5
'Identifiers'	6
'Government related identifier'	6
Adopting, using or disclosing a government related identifier	7
'Adopt'	7
'Use'	7
'Disclose'	8
Exceptions	8
Interaction with other privacy safeguards	9
Privacy Safeguards 3 and 4	9

Key points

- Privacy Safeguard 9¹ sets out a prohibition on accredited data recipients of CDR data from adopting, using or disclosing government related identifiers unless required or authorised:
 - under another Australian law other than the consumer data rules (CDR Rules) or a court/tribunal order, or
 - as prescribed by regulations made under the *Privacy Act 1988* (Privacy Act).
- A government related identifier is a number, letter or symbol, or a combination of any or all of those things, that has been assigned by certain government entities and is used to identify the individual or to verify the identity of the individual.
- Privacy Safeguard 9 only concerns government related identifiers of a consumer who is an individual.
- An individual cannot consent to the adoption, use or disclosure of their government related identifier.

What does Privacy Safeguard 9 say?

9.1 Where CDR data includes a government related identifier, Privacy Safeguard 9 prohibits an accredited data recipient of CDR data from:

- adopting the government related identifier as its own identifier of the consumer, or otherwise using the government related identifier, or
- disclosing CDR data which includes the government related identifier,

unless authorised or required by or under:

- an Australian law other than the CDR Rules or in a court/tribunal order, or
- APP 9.3, which allows an entity to adopt, use or disclose a government related identifier of an individual as prescribed by regulations made under the Privacy Act.

9.2 Privacy Safeguard 9 only concerns government related identifiers of a consumer of the CDR data who is an individual.

9.3 In this Chapter, a government related identifier of a CDR consumer included with the consumer's CDR data is referred to as a 'CDR consumer government related identifier'.

Why is it important?

9.4 The objective of Privacy Safeguard 9 is to restrict use of government related identifiers so that they do not become universal identifiers, which could jeopardise privacy by enabling CDR data from different sources to be matched and linked in ways that a consumer may not agree with or expect.

¹ Competition and Consumer Act, section 56EL.

Who does Privacy Safeguard 9 apply to?

- 9.5 Privacy Safeguard 9 applies to accredited data recipients of CDR data. It does not apply to data holders or designated gateways.
- 9.6 However, data holders and designated gateways must ensure that they are adhering to their obligations under the Privacy Act and APP 9 in relation to government related identifiers of individuals.
- 9.7 As a non-accredited entity, a CDR representative is not directly bound by Privacy Safeguard 9.² However, under the terms of the CDR representative arrangement with their CDR representative principal,³ a CDR representative is required to comply with Privacy Safeguard 9 as if it were an accredited data recipient.^{4,5} A CDR representative principal breaches subrule 7.8A(2) of the CDR Rules if its CDR representative fails to comply with Privacy Safeguard 9 in relation to service data as if it were an accredited data recipient of the service data.⁶
- 9.8 Where they are a non-accredited entity, an outsourced service provider (OSP) is not directly bound by Privacy Safeguard 9. However, under the terms of the CDR outsourcing arrangement with their OSP principal,⁷ an OSP is required to comply with Privacy Safeguard 9 in its handling of service data as if it were the OSP principal.⁸ An accredited person breaches subrule 7.8B(2) of the CDR Rules if a direct or indirect OSP of the accredited person or of their CDR representative, fails to comply with Privacy Safeguard 9 as if it were an accredited data recipient of that service data.⁹

How Privacy Safeguard 9 interacts with the Privacy Act

- 9.9 It is important to understand how Privacy Safeguard 9 interacts with the Privacy Act and the APPs.¹⁰
- 9.10 APP 9 prohibits an APP entity from adopting, using or disclosing a government related identifier unless an exception applies.

² Note that a CDR representative will also have obligations under APP 9 (adoption, use or disclosure of government related identifiers) if they are an APP entity.

³ A CDR representative arrangement is a written contract between a CDR representative and their CDR representative principal. The requirements for this arrangement are outlined in CDR Rules, rule 1.10AA.

⁴ CDR Rules, paragraph 1.10AA(4)(g).

⁵ See [Chapter B \(Key concepts\)](#) for more information on 'CDR representative principal', 'CDR representative', 'CDR representative arrangement' and 'service data'.

⁶ CDR Rules, subrule 7.8A(2). See also rule 1.16A in relation to a CDR representative principal's obligations and liability.

⁷ A CDR outsourcing arrangement is a written contract between an OSP principal and their provider that meets the minimum requirements listed in CDR Rules, subrule 1.10(3).

⁸ CDR Rules, rule 1.10(3)(b)(i)(F),

⁹ CDR Rules, rule 7.8B(2). See also rule 1.16 in relation to an OSP principal's obligations and liability.

¹⁰ The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies.

CDR entity	Privacy protections that apply in the CDR context
Accredited data recipient	<p>Privacy Safeguard 9</p> <p>For accredited data recipients of a consumer's CDR data, Privacy Safeguard 9 applies to the handling of government related identifiers contained in that CDR data.¹¹</p> <p>APP 9 does not apply in relation to that CDR data, except as applied by paragraphs 56EL(1)(d) and (2)(d) of the <i>Competition and Consumer Act 2010</i> (Competition and Consumer Act).¹²</p>
Designated gateway	<p>APP 9</p> <p>Privacy Safeguard 9 does not apply to a designated gateway.</p>
Data holder¹³	<p>APP 9</p> <p>Privacy Safeguard 9 does not apply to a data holder.</p>

Meaning of government related identifier

- 9.11 'Government related identifier' has the meaning given to it in the Privacy Act.¹⁴
- 9.12 Privacy Safeguard 9 only concerns government related identifiers of consumers of the CDR data who are individuals.
- 9.13 For example, the Australian Business Number (ABN) of a body corporate would not be subject to Privacy Safeguard 9. (Note that the ABN of an individual is not an 'identifier' under subsection 6(1) of the Privacy Act).
- 9.14 However, government related identifiers of individuals who are sole traders that manage a small business or of partners in a partnership will be captured by Privacy Safeguard 9.

¹¹ Privacy Safeguard 9 applies from the point when the accredited person becomes an accredited data recipient of the CDR data. An accredited person becomes an accredited data recipient for CDR data when:

- CDR data is held by (or on behalf of) the person
- the CDR data, or any other CDR data from which it was directly or indirectly derived, was disclosed to the person under the consumer data rules, and
- the person is neither a data holder, nor a designated gateway, for the first mentioned CDR data. See Competition and Consumer Act, section 56AK.

¹² The APPs do not apply to an accredited data recipient of CDR data, in relation to that CDR data: Competition and Consumer Act, paragraph 56EC(4)(a). However, paragraph 56EC(4)(a) does not apply for the purposes of paragraphs 56EL(1)(d) and (2)(d), which provide that an accredited data recipient may adopt a government related identifier included in CDR data, use the identifier, or include the identifier in a disclosure of CDR data, if subclause 9.3 of APP 9 applies to the adoption, use or disclosure. Subsection 56EC(4) also does not affect how the APPs apply to accredited persons and accredited data recipients who are APP entities, in relation to the handling of personal information outside the CDR system. (Note: Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See s 6E(1D) of the Privacy Act.) Section 56EC(4) also does not affect how the APPs apply to an accredited person who does not become an accredited data recipient of the CDR data (other than for Privacy Safeguards 1 – 4). See s 56EC(5)(aa) of the Competition and Consumer Act.

¹³ In this chapter, references to data holders include AEMO. See [Chapter B \(Key concepts\)](#) for further information about how the privacy safeguards apply to AEMO.

¹⁴ Competition and Consumer Act, paragraphs 56EL(1)(b) and 56EL(2)(b).

‘Identifiers’

9.15 An ‘identifier’ of an individual is defined in subsection 6(1) of the Privacy Act as a number, letter or symbol, or a combination of any or all of those things, that is used to identify the individual or to verify the identity of the individual.

9.16 The following are explicitly excluded from the definition of identifier:

- an individual’s name
- an individual’s ABN, and
- anything else prescribed by the regulations made under the Privacy Act.¹⁵ This provides flexibility to exclude any specified type of identifier from the definition, and therefore the operation of both Privacy Safeguard 9 and APP 9, as required.

‘Government related identifier’

9.17 A ‘government related identifier’ of an individual is defined in subsection 6(1) of the Privacy Act as an identifier that has been assigned by:

- an agency¹⁶
- a State or Territory authority¹⁷
- an agent of an agency, or a State or Territory authority, acting in its capacity as agent, or
- a contracted service provider for a Commonwealth contract,¹⁸ or a State contract,¹⁹ acting in its capacity as contracted service provider for that contract.

9.18 The following are examples of government related identifiers:

- Medicare numbers
- Centrelink reference numbers²⁰
- driver licence numbers issued by State and Territory authorities, and
- Australian passport numbers.

9.19 Some government related identifiers are also regulated by other laws that restrict the way entities can collect, use or disclose the particular identifier and related personal information. Examples include tax file numbers and individual healthcare identifiers.²¹ These other laws

¹⁵ See the Federal Register of Legislation <https://www.legislation.gov.au> for up-to-date versions of the regulations made under the Privacy Act.

¹⁶ ‘Agency’ is defined in Privacy Act, subsection 6(1).

¹⁷ ‘State or Territory authority’ is defined in subsection 6C(3) of the Privacy Act.

¹⁸ ‘Commonwealth contract’ is defined in subsection 6(1) of the Privacy Act to mean a contract, to which the Commonwealth or an agency is or was a party, under which services are to be, or were to be, provided to an agency.

¹⁹ ‘State contract’ is defined in subsection 6(1) of the Privacy Act to mean a contract, to which a State or Territory or State or Territory authority is or was a party, under which services are to be, or were to be, provided to a State or Territory authority.

²⁰ Note that under regulations 17 and 18 of the *Privacy Regulation 2013*, certain prescribed organisations are permitted to use or disclose certain identifiers (including Centrelink reference numbers) in specific circumstances.

²¹ For more information about the legislative regimes, visit the OAIC’s Tax File Numbers page and Healthcare Identifiers page <https://www.oaic.gov.au>.

apply in addition to Privacy Safeguard 9, i.e. a breach of the *Privacy (Tax File Number) Rule 2015* may be both an interference with the privacy of an individual under the Privacy Act and a breach of Privacy Safeguard 9, as well as a potential offence under the *Taxation Administration Act 1953*.

Adopting, using or disclosing a government related identifier

9.20 An accredited data recipient must not adopt a CDR consumer government related identifier as its own identifier of the consumer, or otherwise use a government related identifier, unless an exception applies.²² In addition, an accredited data recipient must not include the government related identifier when it discloses CDR data unless an exception applies.

‘Adopt’

9.21 The term ‘adopt’ is not defined in the Competition and Consumer Act and so it is appropriate to refer to its ordinary meaning.

9.22 An accredited data recipient ‘adopts’ a CDR consumer government related identifier if it collects CDR data that includes a government related identifier of the consumer and organises the CDR data that it holds about that consumer with reference to that identifier.

Example

Stephanie, an accountant and accredited person, receives a consumer’s driver licence number when it is disclosed to Stephanie in response to a consumer data request. Stephanie then uses the identifier to refer to that consumer in her own identification system.

As Stephanie has adopted a CDR consumer government related identifier, she may be in breach of Privacy Safeguard 9.

‘Use’

9.23 The term ‘use’ is discussed in [Chapter B \(Key concepts\)](#).

9.24 Generally, an entity uses CDR data when it handles and manages that information within its effective control. Examples include:

- the entity accessing and reading the CDR data

²² Competition and Consumer Act, subsection 56EL(1). Note: The principal difference between Privacy Safeguard 9 and APP 9 is that the exceptions to the prohibition on using or disclosing government related identifiers in Privacy Safeguard 9 are much narrower than in APP 9. Only the exceptions under APP 9.1 for adopting, and APP 9.2(c) and (f) for using or disclosing, a government related identifier are carried across to Privacy Safeguard 9:

- The common exceptions between Privacy Safeguard 9 and APP 9 are where the adoption, use or disclosure of the government related identifier is authorised or required by an Australian law or court/tribunal order, or where regulations under APP 9.3 prescribe the adoption, use or disclosure.
- The exceptions in APP 9.2 for using or disclosing government related identifiers for verification purposes, fulfilling obligations to agencies or State or Territory authorities, for ‘permitted general situations’ or for enforcement related activities of enforcement bodies do not apply to Privacy Safeguard 9.

- the entity searching records for the CDR data
- the entity making a decision based on the CDR data, and
- the entity passing the CDR data from one part of the entity to another.

‘Disclose’

9.25 The term ‘disclose’ is discussed in [Chapter B \(Key concepts\)](#).

9.26 An accredited data recipient ‘discloses’ CDR data when it makes it accessible or visible to others outside the entity.²³

Exceptions

Required or authorised by or under an Australian law or court/tribunal order

9.27 An accredited data recipient may use a CDR consumer government related identifier, adopt it as its own identifier or include it when disclosing CDR data if this is required or authorised by or under an Australian law or a court/tribunal order.²⁴

9.28 The meaning of ‘required or authorised by or under an Australian law or a court/tribunal order’ is discussed in [Chapter B \(Key concepts\)](#).

9.29 The Australian law or court/tribunal order should specify:

- a particular government related identifier
- the entities or classes of entities permitted to adopt, use or disclose it, and
- the particular circumstances in which they may adopt, use or disclose it.

Prescribed by regulations

9.30 An accredited data recipient may use a CDR consumer government related identifier, adopt it as its own identifier of the consumer, or include it when disclosing CDR data if:

- the identifier is prescribed by regulations
- the entity is an organisation, or belongs to a class of organisations, prescribed by regulations, and
- the adoption or use occurs in the circumstances prescribed by the regulations.²⁵

9.31 Regulations may be made under the Privacy Act to prescribe these matters.²⁶

²³ Information will be ‘disclosed’ under the CDR system regardless of whether an entity retains effective control over the data.

²⁴ Competition and Consumer Act, paragraph 56EL(1)(c).

²⁵ Competition and Consumer Act, paragraphs 56EL(1)(d) and (2)(d) and APP 9.3.

²⁶ See the Federal Register of Legislation <https://www.legislation.gov.au> for up-to-date versions of regulations made under the Privacy Act.

Interaction with other privacy safeguards

Privacy Safeguards 3 and 4

9.32 Privacy Safeguard 9 applies to the adoption, use and disclosure of government related identifiers. It does not specifically address the *collection* of government related identifiers. However, if an accredited person collects a government related identifier that is considered to be CDR data, they must comply with other privacy safeguards, including [Privacy Safeguard 3](#) and [Privacy Safeguard 4](#). These privacy safeguards are discussed in Chapters 3 and 4 respectively.

Chapter 10:

Privacy Safeguard 10 —

Notifying of the disclosure of CDR data

Version 5.0, November 2023



Contents

Key points	3
What does Privacy Safeguard 10 say?	3
Why is it important?	4
Who does Privacy Safeguard 10 apply to?	4
How Privacy Safeguard 10 interacts with the Privacy Act	5
Who must be notified?	5
How must notification be given?	6
When must notification be given?	8
What matters must be included in the notification?	8
What CDR data was disclosed	10
When the CDR data was disclosed	10
To whom the CDR data was disclosed	11
Other notification requirements under the CDR Rules	12
Disclosure to a designated gateway	13
Interaction with other Privacy Safeguards	13

Key points

- Where a data holder of a consumer's CDR data discloses that data to an accredited person as a result of a consumer data request, the data holder must notify the consumer by updating each consumer dashboard that relates to the request.¹
- Where an accredited data recipient of a consumer's CDR data discloses that data to an accredited person or a trusted adviser, or discloses a CDR insight or a CDR business consumer's CDR data to a specified person, they must notify the consumer by updating each consumer dashboard that relates to the request.²
- The consumer data rules (CDR Rules) set out the matters that must be included in, and the timing of, these notifications.
- The Australian Energy Market Operator Limited (AEMO) is not subject to Privacy Safeguard 10 in its capacity as a data holder.³ Accordingly, unless otherwise indicated, references in this Chapter to data holders exclude AEMO.

What does Privacy Safeguard 10 say?

- 10.1 Where a data holder is required or authorised under the CDR Rules to disclose CDR data, they must notify the consumer by taking the steps identified in the CDR Rules.⁴
- 10.2 Where an accredited data recipient of a consumer's CDR data discloses CDR data, they must notify that consumer by taking the steps identified in the CDR Rules.⁵
- 10.3 The notification must:
- be given to those consumers that the CDR Rules require to be notified
 - cover the matters set out in the CDR Rules, and
 - be given at or before the time specified in the CDR Rules.
- 10.4 Under rule 7.9 in the CDR Rules, data holders and accredited data recipients of a consumer's CDR data must notify the consumer by updating each relevant consumer dashboard to include certain matters as set out in that Rule as soon as practicable after CDR data is disclosed.⁶

¹ *Competition and Consumer Act 2010* (Competition and Consumer Act), subsection 56EM(1) and CDR Rules, subrule 7.9(1).

² *Competition and Consumer Act*, subsection 56EM(2) and CDR Rules, subrule 7.9(2)-(4).

³ *Competition and Consumer Regulations*, paragraph 28RA(2)(b). For information about how Privacy Safeguard 10 applies to retailers who receive CDR data from AEMO, see paragraph 10.10.

⁴ *Competition and Consumer Act*, subsection 56EM(1). For further information on 'required or authorised to use or disclose CDR data under the CDR Rules', refer to [Chapter B \(Key concepts\)](#).

⁵ *Competition and Consumer Act*, subsections 56EM(2), (3) and (4).

⁶ A CDR consumer in the energy sector may elect not to have a data holder dashboard: CDR Rules, clause 2.3 of Schedule 4. In these circumstances, as there is no data holder dashboard that relates to the consumer data request, the data holder would not be able to update any dashboard for the purposes of rule 7.9 in the CDR Rules.

Why is it important?

- 10.5 Notification of disclosure of CDR data is an integral element of the CDR system, as it provides confirmation to consumers that their CDR data has been disclosed in response to a consumer data request.
- 10.6 This ensures consumers are informed when their CDR data is disclosed and builds trust between consumers, data holders and accredited data recipients.

Who does Privacy Safeguard 10 apply to?

- 10.7 Privacy Safeguard 10 applies to data holders and accredited data recipients of CDR data. It does not apply to designated gateways.
- 10.8 Where an accredited data recipient is a CDR representative principal under a CDR representative arrangement, a disclosure of service data by a CDR representative (or by a direct or indirect outsourced service provider (OSP) of the CDR representative) is taken to be a disclosure by the CDR representative principal.⁷ This means that, where a CDR representative (or their direct or indirect OSP) discloses a consumer's CDR data, the CDR representative principal must notify that consumer of the disclosure under Privacy Safeguard 10, although it may arrange for its CDR representative to do so on its behalf.⁸
- 10.9 If an accredited person who is a direct or indirect OSP discloses CDR data that was collected on behalf of another accredited person (the 'OSP principal') under a CDR outsourcing arrangement, only the OSP principal is required to notify the relevant consumer/s of the disclosure for the purposes of Privacy Safeguard 10.⁹ Similarly, where an unaccredited person who is a direct or indirect OSP discloses CDR data under a CDR outsourcing arrangement, the OSP principal is required to notify the relevant consumer/s of the disclosure for the purposes of Privacy Safeguard 10.¹⁰
- 10.10 Privacy Safeguard 10 does not apply to AEMO in its capacity as a data holder.¹¹ Instead, data holders that are retailers in the energy sector (primary data holders)¹² must comply with Privacy Safeguard 10 in relation to AEMO data that they disclose (in addition to having Privacy Safeguard 10 obligations with respect to their own data holdings).¹³

⁷ CDR Rules, subrule 7.9(5).

⁸ CDR Rules, subrule 4.19(2).

⁹ CDR Rules, subrule 1.16(5) and rule 7.9.

¹⁰ CDR Rules, subrule 7.6(2) and rule 7.9.

¹¹ Competition and Consumer Regulations, paragraph 28RA(2)(b).

¹² See [Chapter B \(Key concepts\)](#) for further information about primary data holders.

¹³ Competition and Consumer Regulations, paragraph 28RA(3)(b).

How Privacy Safeguard 10 interacts with the Privacy Act

For data holders

- 10.11 Data holders must comply with Privacy Safeguard 10 when they are required or authorised to disclose CDR data (including SR data)¹⁴ under the CDR Rules.
- 10.12 There is no corresponding obligation under the *Privacy Act 1988* (the Privacy Act) or the APPs to notify an individual of the disclosure of their personal information.
- 10.13 However, APP 5 will continue to apply in relation to the notification of the collection of CDR data that is also personal information.¹⁵

For accredited data recipients

- 10.14 For an accredited data recipient of a consumer's CDR data, Privacy Safeguard 10 applies whenever they disclose that consumer's data.
- 10.15 The APPs do not apply to an accredited data recipient of CDR data, in relation to that CDR data.¹⁶

Who must be notified?

For data holders

- 10.16 The data holder must notify the consumer(s) for the disclosed CDR data by updating each consumer dashboard that relates to the request.¹⁷
- 10.17 There may be more than one consumer for the CDR data with a dashboard that relates to the request. A key example is CDR data relating to a joint account. In this case, the data holder must notify each of the requesting and non-requesting joint account holders. However, a data holder is not liable for a failure to notify the non-requesting joint account holder/s where the data holder considers this necessary to prevent physical, psychological or financial harm or abuse.¹⁸

¹⁴ For further information on SR data, see [Chapter B \(Key concepts\)](#). In the energy sector, AEMO data in relation to a CDR consumer is SR data: CDR Rules, clause 4.3 of Schedule 4.

¹⁵ For example, the obligations in APP 5.2 (f), (i) and (j) to notify individuals of the situations in which their personal information may be disclosed in future.

¹⁶ Competition and Consumer Act, paragraph 56EC(4)(a). However, subsection 56EC(4) does not affect how the APPs apply to accredited persons and accredited data recipients who are APP entities, in relation to the handling of personal information outside the CDR system. (Note: Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See Privacy Act, subsection 6E(1D).) Subsection 56EC(4) also does not affect how the APPs apply to an accredited person who does not become an accredited data recipient of the CDR data (other than for Privacy Safeguards 1 – 4). See Competition and Consumer Act, paragraph 56EC(5)(aa).

¹⁷ Competition and Consumer Act, paragraph 56EM(1)(b) and CDR Rules, subrule 7.9(1). See paragraph 10.24 for information about situations where there is no dashboard that relates to the request.

¹⁸ Rule 4A.15 in the CDR Rules provides that the data holder is not liable under the CDR Rules for failure to comply with Part 4A (including the requirement to provide and update a dashboard) if the data holder considers that the relevant act or omission was necessary in order to prevent physical, psychological or financial harm or abuse.

- 10.18 This exception to notification is to accommodate existing procedures a data holder may have to protect consumers, for example particular arrangements relating to consumers that may be experiencing family violence.
- 10.19 Where the CDR data disclosed relates to an account with a secondary user¹⁹ and the secondary user has a consumer dashboard that relates to the request,²⁰ the data holder must notify both the account holder and secondary user.²¹
- 10.20 Where the CDR data disclosed relates to a non-individual consumer or is in relation to a partnership account, the data holder must notify the relevant nominated representative.²²

For accredited data recipients

- 10.21 The accredited data recipient must notify the consumer who provided the disclosure consent.²³

How must notification be given?

For data holders

- 10.22 A data holder must provide the notification by updating each consumer dashboard that relates to the request (including, if applicable, the dashboard of the other joint account

¹⁹ A person is a secondary user for an account with a data holder if the person has ‘account privileges’ in relation to the account, and the account holder has given the data holder an instruction to treat the person as a secondary user for the purposes of the CDR Rules (CDR Rules, rule 1.7). ‘Account privileges’ for the banking sector are defined in clause 2.2 of Schedule 3 to the CDR Rules. ‘Account privileges’ for the energy sector are defined in clause 2.2 of Schedule 4 to the CDR Rules.

²⁰ A data holder will provide a secondary user with a dashboard when the secondary user is the CDR consumer on whose behalf the accredited person made the consumer data request: CDR Rules, rule 1.15. See footnote 6 regarding when a data holder dashboard will be provided to a CDR consumer in the energy sector.

²¹ The application of CDR Rules relating to secondary users is staged in the banking and energy sectors. For the meaning of staged application, see [Chapter B \(Key concepts\)](#). For staged application of CDR Rules in the banking sector, see CDR Rules, clause 6.7 of Schedule 3. For staged application of CDR Rules in the energy sector, see CDR Rules, clauses 8.16 and 8.6 of Schedule 4. Data holders should carefully review the staged application provisions relevant to each sector when considering their obligations under the Privacy Safeguards.

²² The application of CDR Rules relating to partnerships is staged in the banking and energy sectors. For the meaning of staged application, see [Chapter B \(Key concepts\)](#). For staged application of CDR Rules in the banking sector, see CDR Rules, clause 6.7 of Schedule 3. For staged application of CDR Rules in the energy sector, see CDR Rules, clauses 8.1 and 8.6 of Schedule 4. Data holders should carefully review the staged application provisions relevant to each sector when considering their obligations under the Privacy Safeguards.

A ‘nominated representative’ is the individual nominated by the non-individual consumer under paragraphs 1.13(c)(i) or 1.13(d)(i) in the CDR Rules who is able to give, amend and manage authorisations to disclose CDR data on behalf of the non-individual consumer. There may be more than one nominated representative.

²³ CDR rules, subrules 7.9(2)-(4). A disclosure consent is a consent given by a consumer for the accredited data recipient to disclose CDR data to an accredited person: for example, in response to consumer data request (an ‘AP disclosure consent’, an ‘insight disclosure consent’, a business consumer disclosure consent or a ‘TA disclosure consent’), or for the purposes of direct marketing: CDR Rules, paragraph 1.10A(1)(c). For further information, see Chapter C (Consent).

holder/s)²⁴ to include the matters discussed in paragraphs 10.36 and 10.40 to 10.51 as soon as practicable after CDR data relating to that consumer is disclosed.²⁵

- 10.23 The data holder's consumer dashboard is an online service that must be offered, and in most circumstances must be provided, by a data holder to each consumer (and, if applicable, the other joint account holder/s)²⁶ where a consumer data request has been made on their behalf by an accredited person. Data holders must include within the dashboard certain details of each authorisation to disclose CDR data that has been given by the consumer.²⁷
- 10.24 If a CDR consumer in the energy sector does not have online access to their account, they may elect not to have a data holder dashboard.²⁸ In these circumstances, there will be no dashboard that relates to the consumer data request and the data holder would not be able to update any dashboard for the purposes of subrule 7.9(1) in the CDR Rules.
- 10.25 Further guidance about the data holder's consumer dashboard is set out in [Chapter B \(Key concepts\)](#) and the [Guide to privacy for data holders](#).

For accredited data recipients

- 10.26 An accredited data recipient must provide the notification by updating the consumer dashboard for the consumer who provided the disclosure consent.²⁹
- 10.27 The accredited data recipient's consumer dashboard is an online service that must be provided by an accredited data recipient to each consumer who has provided a consent in relation to their CDR data. Accredited data recipients must include in the dashboard certain details of each consent that has been given by the consumer.³⁰
- 10.28 Where an accredited data recipient disclosed CDR data that was collected on behalf of another accredited person (the 'principal') under a CDR outsourcing arrangement, only the principal needs to notify the relevant consumer/s by updating the relevant dashboard.³¹
- 10.29 Further guidance about the accredited data recipient's consumer dashboard is set out in [Chapter B \(Key concepts\)](#) and [Chapter C \(Consent\)](#).

²⁴ Where the CDR data disclosed relates to a joint account, and either the co-approval or pre-approval option applies to that account, the data holder must provide each relevant account holder with a consumer dashboard, and notify each of the joint account holders by updating their consumer dashboards to include those same matters as soon as practicable after the CDR data is disclosed. However, the data holder may decline to provide a relevant account holder with a consumer dashboard or update the consumer dashboard if the data holder considers it necessary to do either in order to prevent physical, psychological or financial harm or abuse. See CDR Rules, rule 4A.15.

²⁵ CDR Rules, rule 7.9.

²⁶ Where the CDR data disclosed relates to a joint account, and either the co-approval or pre-approval option applies to that account, the data holder must provide each relevant account holder with a consumer dashboard, except where the data holder considers it necessary to decline to provide a relevant account holder with a dashboard in order to prevent physical, psychological or financial harm or abuse. See CDR Rules, rules 4A.13 and 4A.15.

²⁷ The requirements are outlined in rule 1.15 in the CDR Rules, and include requirements to provide details of the CDR data to which the authorisation relates and when the authorisation will expire.

²⁸ CDR Rules, subclause 2.3(2) of Schedule 4.

²⁹ A disclosure consent is a consent given by a consumer for the accredited data recipient to disclose CDR data: for example, an 'AP disclosure consent', an 'insight disclosure consent', a 'business consumer disclosure consent', or a 'TA disclosure consent', or a direct marketing consent: CDR Rules, paragraph 1.10A(1)(c). For further information, see Chapter C (Consent).

³⁰ The requirements are outlined in rule 1.14 in the CDR Rules and include requirements to provide details of the CDR data to which each consent relates and when each consent will expire.

³¹ CDR Rules, paragraph 1.16(5)(a). For information on 'CDR outsourcing arrangements', see [Chapter B \(Key concepts\)](#).

When must notification be given?

- 10.30 Data holders and accredited data recipients must notify the consumer/s as soon as practicable after the CDR data is disclosed.³²
- 10.31 As a matter of best practice, notification should generally occur in as close to real time as possible (for example, in relation to ongoing disclosure, as close to the time of first disclosure as possible). In most cases, notification will occur on the same day as the CDR data is disclosed.
- 10.32 The test of practicability is an objective test. It is the responsibility of the data holder or accredited data recipient to be able to justify any delay in notification.
- 10.33 In determining what is ‘as soon as practicable’, data holders and accredited data recipients may take the following factors into account:
- the time and cost involved, in combination with other factors
 - technical matters, and
 - the individual needs of the consumer (for example, any additional steps required to make the content accessible).
- 10.34 Data holders and accredited data recipients are not excused from providing prompt notification by reason only that it would be inconvenient, time consuming, or costly to do so.
- 10.35 Notifications about disclosure should remain on a consumer’s consumer dashboard, even where the relevant authorisation has expired.³³

What matters must be included in the notification?

- 10.36 The minimum matters that must be included by data holders and accredited data recipients in a notification about disclosure to an accredited person, and provided via the consumer’s dashboard are:
- what CDR data was disclosed
 - when the CDR data was disclosed, and
 - the accredited person to whom the CDR data was disclosed.³⁴

³² CDR Rules, subrules 7.9(1), 7.9(2), 7.9(3), 7.9(3A) and 7.9(4).

³³ CDR Rule 1.14(3)(h) and 1.15(3)(f) provide that the consumer dashboard must include certain information about a consent or authorisation (respectively), including where that consent or authorisation is not current. This includes information about when CDR data was collected or disclosed pursuant to the consent, or disclosed pursuant to the authorisation.

³⁴ CDR Rules, subrules 7.9(1) and 7.9(2). The accredited person needs to be identified in accordance with any entry on the Register of Accredited Persons specified as being for that purpose.

10.37 Where an accredited data recipient discloses CDR data to a person in accordance with a business consumer disclosure consent, the minimum matters that must be included in the notification provided via the consumer's dashboard are:

- what CDR data was disclosed
- when the CDR data was disclosed, and
- the person to whom it was disclosed.³⁵

10.38 Where an accredited data recipient discloses CDR data to a trusted adviser, the minimum matters that must be included in the notification provided via the consumer's dashboard are:

- what CDR data was disclosed,
- when the CDR data was disclosed, and
- the identity of the trusted adviser.³⁶

10.39 Where an accredited data recipient discloses a CDR insight, the minimum matters that must be included in the notification provided via the consumer's dashboard are:

- what CDR data was disclosed
- when the CDR data was disclosed, and
- the person to whom the CDR data was disclosed.³⁷

10.40 Data holders and accredited data recipients should provide information about these matters clearly and simply, but also with enough specificity to be meaningful for the consumer. How much information is required may differ depending on the circumstances.

10.41 Guidance on each of the minimum matters follows.

³⁵ CDR Rules, subrule 7.9(3A).

³⁶ CDR Rules, subrule 7.9(3).

³⁷ CDR Rules, subrule 7.9(4).

Risk point: Consumers may not read or understand a notification if it is complex.

Privacy tip: Data holders and accredited data recipients should ensure that the notification is as simple and easy to understand as possible. To do this, entities should consider a range of factors when formulating a notification, such as:

- the audience
- the language used (including the level of detail), and
- the presentation of the information (e.g. layout, format and any visual aids used). For more complex notifications, entities could consider providing a condensed summary of key matters in the notification and linking to a more comprehensive summary or, where it may assist the consumer, a full log of disclosure.

What CDR data was disclosed

10.42 Data holders and accredited data recipients must notify the consumer of what CDR data was disclosed.

10.43 In doing so, the entity should ensure the CDR data is described in a manner that allows the consumer to easily understand what CDR data was disclosed.

10.44 Data holders and accredited data recipients must use the Data Language Standards when describing what CDR data was disclosed.³⁸ This will aid consumer comprehension by ensuring consistency between how CDR data was described in the authorisation/consent-seeking processes and how CDR data is described in the consumer dashboard.

When the CDR data was disclosed

10.45 Data holders and accredited data recipients must notify the consumer of when the CDR data was disclosed.³⁹

*‘One-off’ disclosure*⁴⁰

10.46 The entity should include the date on which the CDR data was disclosed.

³⁸ The Data Language Standards (<https://consumerdatastandardsaustralia.github.io/standards/#data-language-standards-common>) provide descriptions of the types of data to be used by data holders and accredited data recipients when making and responding to requests. Adherence to the Data Language Standards is mandatory and will help ensure there is a consistent interpretation and description of the consumer data that will be shared in the CDR system. See section 56FA of the Competition and Consumer Act and rule 8.11 in the CDR Rules.

³⁹ CDR Rules, paragraph 7.9(1)(b). Note this requirement refers to dates of disclosure, not the date that authorisation was provided or expired.

⁴⁰ For data holders, this is where the accredited person made a consumer data request on behalf of the consumer for a collection of CDR data on a single occasion. For accredited data recipients, this is where the consumer’s disclosure consent applies for the disclosure of CDR data on a single occasion.

Ongoing disclosure⁴¹

- 10.47 The entity should, at a minimum, include the date range in which CDR data will be disclosed, with the starting date being the date on which the CDR data was first disclosed, and the end date being the date on which the entity will make its final disclosure. This end date might not necessarily be the same as the date that the authorisation (in the case of a data holder) or disclosure consent (in the case of an accredited data recipient) expires.
- 10.48 Where the entity is unsure of the end date they may put the date the authorisation or disclosure consent expires, but must update the end date as soon as practicable after it becomes known.⁴²
- 10.49 If disclosure of particular CDR data stops (for example, because authorisation for that data is withdrawn), but disclosure later recommences under an amended authorisation, then the disclosure is not continuous and 2 separate date ranges should be included.

To whom the CDR data was disclosed

- 10.50 In a notification to the consumer of the disclosure of CDR data to an accredited person, the entity must indicate the accredited person to whom the CDR data was disclosed.
- 10.51 The accredited person must be identified in accordance with any entry on the Register of Accredited Persons specified as being for that purpose.⁴³

Example

Bank Belle, a data holder, receives a consumer data request on 1 July 2022 from Watson and Co, an accredited person, to disclose Zoe's transaction details.

Bank Belle asks Zoe on 1 July 2022 to authorise the disclosure of her transaction details to Watson and Co for the sharing period specified in the consumer data request (i.e. 1 July 2022 to 1 January 2023).

Upon receiving Zoe's authorisation, Bank Belle discloses Zoe's transaction details to Watson and Co on 1 July 2022.

Bank Belle updates Zoe's consumer dashboard on 1 July 2022 to include the following notification statement:

We shared your transaction details with Watson and Co on 01.07.22. We'll continue to share your transaction details with Watson and Co until 01.01.23.

⁴¹ For data holders, this is where the accredited person made a consumer data request on behalf of the consumer for collection of CDR data over a specified period of time. For accredited data recipients, this is where the consumer's disclosure consent applies for the disclosure of CDR data over a specified period of time.

⁴² CDR Rules, rules 4.19 and 4.27 require data holders and accredited data recipients (respectively) to update the consumer dashboard as soon as practicable after the information required to be contained on the dashboard changes.

⁴³ CDR Rules, paragraphs 7.9(1)(c) and (2)(c).

The above statement is an example of how Bank Belle, a data holder, could notify Zoe of the disclosure of her CDR data in accordance with subrule 7.9(1) in the CDR Rules.

10.52 In a notification to the consumer of a disclosure of CDR data to a trusted adviser, the accredited data recipient must indicate the trusted adviser to whom the CDR data was disclosed.⁴⁴

10.53 In a notification to the consumer of the disclosure of a CDR insight, the accredited data recipient must indicate to whom the data was disclosed.⁴⁵

10.54 In a notification to the consumer of a disclosure of CDR data to a specified person in accordance with a business consumer disclosure consent, the accredited data recipient must indicate to whom the CDR data was disclosed.⁴⁶

Other notification requirements under the CDR Rules

For data holders

10.55 In addition to the Privacy Safeguard 10 notification requirements in relation to disclosure, there are other notification requirements that must be complied with by a data holder:

- general obligation to update the consumer dashboard (CDR Rules, rule 4.27)
- notification requirements where authorisations are withdrawn or otherwise expire (CDR Rules, rules 4.26A and 4.28).

For accredited data recipients

10.56 In addition to the Privacy Safeguard 10 notification requirements in relation to disclosure, there are other notification requirements relating to consent and collection that must be complied with by an accredited data recipient:^{47,48}

- providing CDR receipts to the consumer (CDR Rules, rule 4.18)
- notification requirements where certain consents expire or are amended (CDR Rules, rules 4.18AA, 4.18A, 4.18B and 4.18C)
- general obligation to update the consumer dashboard (CDR Rules, rule 4.19)

⁴⁴ CDR Rules, subrule 7.9(3).

⁴⁵ CDR Rules, subrule 7.9(4).

⁴⁶ CDR Rules, subrule 7.9(3A).

⁴⁷ For an accredited data recipient who collected CDR data on behalf of a principal in a CDR outsourcing arrangement, note the effect of subrule 1.7(5) in the CDR Rules which provides that, in the CDR Rules, ‘unless the contrary intention appears, a reference to an accredited person making a consumer data request, collecting CDR data, obtaining consents, providing a consumer dashboard, or using or disclosing CDR data does not include a reference to an accredited person doing those things on behalf of a principal in its capacity as the provider in an OSP arrangement, in accordance with the arrangement’.

For information on ‘CDR outsourcing arrangements’, see [Chapter B \(Key concepts\)](#).

⁴⁸ Under a sponsorship arrangement, where both an affiliate and their sponsor are required to give one of the notices in CDR Rules 4.18 – 4.20, the Rules provide that the sponsor and affiliate may choose which of them will give the notice: CDR Rules, rule 4.20A.

- ongoing notification requirements for consents to collect and use (CDR Rules, rule 4.20), and
- notifying the consumer of the collection of their CDR data under Privacy Safeguard 5 (CDR Rules, rule 7.4).

10.57 For further information regarding the notification requirements for consent, see [Chapter C \(Consent\)](#). For further information regarding the notification requirement for collection, see [Chapter 5 \(Privacy Safeguard 5\)](#).

Disclosure to a designated gateway

10.58 Privacy Safeguard 10 applies where a data holder or accredited data recipient discloses CDR data to a designated gateway as required or authorised under the CDR Rules.⁴⁹

10.59 There are currently no CDR Rules made for this circumstance.

Note: *There are currently no designated gateways in the banking sector or energy sector.⁵⁰ See Chapter B (Key concepts) for the meaning of designated gateway.*

Interaction with other Privacy Safeguards

10.60 Data holders and accredited data recipients must comply with Privacy Safeguard 1 by taking reasonable steps to implement practices, procedures and systems that will ensure they comply with the CDR system, including Privacy Safeguard 10. See [Chapter 1 \(Privacy Safeguard 1\)](#).

10.61 Privacy Safeguard 11 mandates the steps which data holders and accredited data recipients must take to advise a consumer where they have disclosed CDR data that was incorrect. See [Chapter 11 \(Privacy Safeguard 11\)](#).

⁴⁹ CDR Rules may be made in relation to the notification requirements for that disclosure.

⁵⁰ For the banking sector, see the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019. For the energy sector, the energy designation specifies AEMO as a gateway for certain information: subsection 6(4) of the Consumer Data Right (Energy Sector) Designation 2020. However, at the time of publication, AEMO is not a designated gateway for any CDR data because under current CDR Rules, no CDR data is (or is to be) disclosed to AEMO because of the reasons in subsection 56AL(2)(c) of the Competition and Consumer Act.

There are also no designated gateways in the telecommunications sector, although unlike the banking and energy sectors at the date of publication of these guidelines, there are no rules allowing for the sharing of designated telecommunications data under the CDR system: Consumer Data Right (Telecommunications Sector) Designation 2022.

Chapter 11: Privacy Safeguard 11 — Quality of CDR data

Version 5.0, November 2023



Contents

Key points	3
What does Privacy Safeguard 11 say?	3
Why is it important?	4
Who does Privacy Safeguard 11 apply to?	4
How Privacy Safeguard 11 interacts with the Privacy Act	5
What are the quality considerations?	6
Accurate	8
Up to date	8
Complete	9
Taking reasonable steps to ensure the quality of CDR data	9
When must an entity take reasonable steps?	9
What constitutes ‘reasonable steps’?	10
Examples of reasonable steps	11
Advising a consumer when disclosed CDR data is incorrect	11
In what circumstances must an entity disclose corrected CDR data to the original recipient?	15
Record keeping requirements	15
How does Privacy Safeguard 11 interact with the other privacy safeguards?	16
Privacy Safeguard 5	16
Privacy Safeguard 10	16
Privacy Safeguard 12	17
Privacy Safeguard 13	17

Key points

- Privacy Safeguard 11,¹ together with rule 7.10 of the consumer data rules (CDR Rules), sets out obligations for data holders and accredited data recipients of CDR data to:
 - ensure the quality of disclosed consumer data right (CDR) data
 - inform consumers if they become aware they disclosed incorrect CDR data, and
 - disclose corrected CDR data to the original recipient if requested to do so by the affected consumer.
- The Australian Energy Market Operator Limited (AEMO) is not subject to Privacy Safeguard 11 in its capacity as a data holder.² Accordingly, unless otherwise indicated, all references in this Chapter to data holders exclude AEMO.

What does Privacy Safeguard 11 say?

11.1 Privacy Safeguard 11 requires:

- data holders who are required or authorised to disclose CDR data under the CDR Rules,³ and
- accredited data recipients of a consumer's CDR data who are disclosing that consumer's CDR data when required or authorised under the CDR Rules

to:

- take reasonable steps to ensure that the CDR data is, having regard to the purpose for which it is held, accurate, up to date and complete
- advise the consumer in accordance with the CDR Rules if they become aware that the CDR data disclosed was not accurate, up to date and complete when disclosed, and
- where incorrect CDR data was previously disclosed, comply with a request by the consumer to disclose corrected CDR data to the original recipient in accordance with the CDR Rules.⁴

11.2 Privacy Safeguard 11 provides that holding CDR data so that it can be disclosed as required under the CDR Rules is not to be regarded as a purpose when working out the purpose for which the CDR data is or was held.⁵

¹ Competition and Consumer Act, section 56EN.

² Competition and Consumer Regulations, sub-regulation 28RA(4). For further information, see paragraph 11.10.

³ Privacy Safeguard 11 does not apply to AEMO in its capacity as a data holder. Privacy Safeguard 11 does not apply to retailers for data AEMO holds that AEMO has disclosed to the retailer and that the retailer is required or authorised to disclose under the CDR Rules. See the Competition and Consumer Regulations and pages 3–4 of the Explanatory Statement to the Competition and Consumer Amendment (Consumer Data Right) Regulations 2021. For further information, see paragraph 11.10.

⁴ Both the consumer's request, and the actions taken by the CDR participant to correct the data under Privacy Safeguard 11, must be in accordance with the CDR Rules: see Competition and Consumer Act, subsection 56EN(4). Further, the requirement to disclose corrected CDR data to the recipient under Privacy Safeguard 11 does not apply in circumstances specified in the CDR Rules: see Competition and Consumer Act, subsection 56EN(4A)). However, no such Rules have been made as at the date of publication of this Chapter 11.

⁵ See Competition and Consumer Act, subsection 56EN(5). This is applicable to subsections 56EN(1), (2) and (3)(b).

- 11.3 Rule 7.10 of the CDR Rules requires data holders⁶ and accredited data recipients of a consumer's CDR data who have disclosed CDR data that was incorrect at the time of disclosure to provide the consumer with a written notice by electronic means that identifies:
- the accredited person to whom the CDR data was disclosed
 - the CDR data that was incorrect, and
 - the date of the disclosure.
- 11.4 The notice must also advise the consumer that they can request the entity to disclose the corrected data to the accredited person (to whom the incorrect CDR data was previously disclosed). The data holder or accredited data recipient must disclose the corrected data if the consumer requests them to do so.
- 11.5 This notice must be provided to the consumer as soon as practicable, but no more than 5 business days after the data holder or accredited data recipient becomes aware that some or all of the disclosed data was incorrect.

Why is it important?

- 11.6 The objective of Privacy Safeguard 11 is to ensure consumers have trust in and control over the quality of their CDR data disclosed as part of the CDR system.
- 11.7 Privacy Safeguard 11 does this by ensuring entities are disclosing CDR data that is accurate, up to date and complete, and by giving consumers control over their data by allowing them to require entities to disclose corrected data to the relevant accredited person.
- 11.8 This allows consumers to enjoy the benefits of the CDR system, such as receiving competitive offers from other service providers, as the data made available to sector participants can be relied on.

Who does Privacy Safeguard 11 apply to?

- 11.9 Privacy Safeguard 11 applies to data holders and accredited data recipients of CDR data.
- 11.10 Privacy Safeguard 11 does not apply to designated gateways or AEMO. Data holders that are retailers in the energy sector also do not have Privacy Safeguard 11 obligations in relation to CDR data held by AEMO that AEMO has disclosed to them.⁷ Retailers must comply with Privacy Safeguard 11 in respect to their own data holdings.
- 11.11 As a non-accredited entity, a CDR representative is not directly bound by Privacy Safeguard 11. However, under the terms of the CDR representative arrangement with their CDR representative principal,⁸ a CDR representative is required to comply with Privacy Safeguard

⁶ Privacy Safeguard 11 does not apply to AEMO in its capacity as a data holder. Privacy Safeguard 11 does not apply to retailers for data AEMO holds that AEMO has disclosed to the retailer and that the retailer is required or authorised to disclose under the CDR Rules. See the Competition and Consumer Regulations and pages 3–4 of the Explanatory Statement to the Competition and Consumer Amendment (Consumer Data Right) Regulations 2021. For further information, see paragraph 11.10.

⁷ See the Competition and Consumer Regulations and pages 3–4 of the Explanatory Statement to the Competition and Consumer Amendment (Consumer Data Right) Regulations 2021.

⁸ A CDR representative arrangement is a written contract between a CDR representative and their CDR representative principal that meets the minimum requirements listed in subrules 1.10AA(1), (3) and (4) in the CDR Rules.

11 in its handling of service data as if it were the CDR representative principal.^{9,10} A CDR representative principal breaches subrule 7.10A(1) in the CDR Rules if its CDR representative fails to comply with Privacy Safeguard 11 (subsection 56EN(2)) as if it were an accredited person (regardless of whether the CDR representative's actions accord with the CDR representative arrangement).¹¹

How Privacy Safeguard 11 interacts with the Privacy Act

- 11.12 It is important to understand how Privacy Safeguard 11 interacts with the *Privacy Act 1988* (the Privacy Act) and APPs.¹²
- 11.13 APP 10 requires APP entities to take reasonable steps to ensure the quality of personal information in certain circumstances.
- 11.14 APP 10 requires an APP entity to take reasonable steps to ensure the quality of personal information at the time of the *collection* and *use* as well as the *disclosure* of the information.
- 11.15 Although Privacy Safeguard 11 applies only in relation to the *disclosure* of CDR data, good practices and procedures by data holders that ensure the quality of personal information collected, used and disclosed under APP 10 will also help to ensure the quality of CDR data that is *disclosed* under the CDR system.
- 11.16 Data holders (including AEMO) should also be aware that APP 13 (correction of personal information) obligations under the Privacy Act continue to apply in certain circumstances. For example, where the data holder becomes aware of incorrect CDR data, but the data holder has not disclosed that data to an accredited data recipient, the data holder must continue to comply with APP 13 and take steps that are reasonable to correct CDR data.¹³

CDR entity	Privacy protections that apply in the CDR context
Accredited data recipient	Privacy Safeguard 11 For accredited data recipients of a consumer's CDR data, Privacy Safeguard 11 applies to the disclosure of CDR data and the disclosure of corrected CDR data. ¹⁴

⁹ CDR Rules, paragraph 1.10AA(4)(a)(iii).

¹⁰ See [Chapter B \(Key concepts\)](#) for more information on 'CDR representative principal', 'CDR representative', 'CDR representative arrangement' and 'service data'.

¹¹ CDR Rules, rule 7.10A. See also rule 1.16A in relation to a CDR representative principal's obligations and liability.

¹² The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies (APP entities).

¹³ See [Chapter 13 \(APP 13\)](#) of the OAIC's APP Guidelines for further information.

¹⁴ Privacy Safeguard 11 applies from the point when the accredited person becomes an accredited data recipient of the CDR data. An accredited person becomes an accredited data recipient for CDR data when:

- CDR data is held by (or on behalf of) the person
- the CDR data, or any other CDR data from which it was directly or indirectly derived, was disclosed to the person under the consumer data rules, and
- the person is neither a data holder, nor a designated gateway, for the first mentioned CDR data.

See Competition and Consumer Act, section 56AK.

CDR entity	Privacy protections that apply in the CDR context
	The APPs do not apply to accredited data recipients in relation to that CDR data. ¹⁵
Data holder (other than AEMO)	<p>Privacy Safeguard 11, APP 10 and APP 13</p> <p>Privacy Safeguard 11 applies instead of APP 10 to <i>disclosures</i> of CDR data that are required or authorised under the CDR Rules.</p> <p>APP 10 continues to apply to CDR data that is also personal information in all other circumstances, including:</p> <ul style="list-style-type: none"> • the collection and use of CDR data, and • disclosures of CDR data outside the CDR system. <p>Note: APP 13 continues to apply when the data holder becomes aware of incorrect CDR data, but the data has not been disclosed to an accredited data recipient.¹⁶</p>
Data Holder (AEMO)	<p>APP 10 and APP 13</p> <p>Privacy Safeguard 11 does not apply to AEMO as a data holder.</p>
Designated gateway	<p>APP 10 and APP 13</p> <p>Privacy Safeguard 11 does not apply to a designated gateway.</p>

What are the quality considerations?

11.17 The 3 quality considerations under Privacy Safeguard 11 are that data should be ‘accurate, up to date and complete’. Whether or not CDR data is accurate, up to date and complete must be determined with regard to the purpose for which it is held. ‘Held’ is discussed in [Chapter B \(Key concepts\)](#).

11.18 When working out the purpose for which the CDR data is or was held, entities must disregard the purpose of holding the CDR data so that it can be disclosed as required under the CDR Rules.

11.19 For example, a data holder that is an authorised deposit-taking institution collects transaction data for the purpose of providing a banking service to its customer. It does not hold transaction data for the purpose of being required to disclose the data under the CDR system. ‘Purpose’ is discussed further in [Chapter B \(Key concepts\)](#).

¹⁵ The APPs do not apply to an accredited data recipient of CDR data, in relation to that CDR data: Competition and Consumer Act, paragraph 56EC(4)(a). However, subsection 56EC(4) does not affect how the APPs apply to accredited persons and accredited data recipients who are APP entities, in relation to the handling of personal information outside the CDR system. (Note: Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data: see Privacy Act, subsection 6E(1D)). Subsection 56EC(4) of the Competition and Consumer Act also does not affect how the APPs apply to an accredited person who does not become an accredited data recipient of the CDR data (other than for Privacy Safeguards 1 – 4). See Competition and Consumer Act, paragraph 56EC(5)(aa).

¹⁶ APP 13 requires that APP entities must take reasonable steps to correct personal information where the entity is satisfied, independently of any request, that personal information it holds is inaccurate, out of date, incomplete, irrelevant or misleading.

Example 1 – data holder (banking sector)

Bright Bank is a data holder and is regularly required or authorised to disclose consumers' CDR data under the CDR Rules.

Bright Bank receives a consumer data request from Leighton, requesting that Bright Bank share their account balance and details with Innobank.

Bright Bank holds this data for the purposes of providing a bank account service to Leighton.

When Bright Bank is required or authorised to disclose Leighton's CDR data under the CDR Rules to Innobank, Privacy Safeguard 11 requires Bright Bank to take reasonable steps to ensure the data is accurate, up to date and complete having regard to this purpose.

Example 2 – data holder (energy sector)

Eager Energy is a retailer and a data holder in the energy sector.

Eager Energy receives a consumer data request from Mustafa, requesting that Eager Energy share Mustafa's billing and metering information with OliveCompare.¹⁷ Eager Energy follows the process in the CDR Rules to obtain the metering data for Mustafa's account from AEMO.¹⁸

When Eager Energy is required or authorised to disclose Mustafa's CDR data to OliveCompare under the CDR Rules, Privacy Safeguard 11 requires Eager Energy to take reasonable steps to ensure the billing data is accurate, up to date and complete having regard to its purpose. However, Eager Energy does not have to comply with Privacy Safeguard 11 with respect to the metering data it obtained from AEMO.¹⁹

Example 3 – accredited data recipient

Vikingforce is an accredited data recipient that collects and uses Hamish's CDR data to provide him with a product comparison service and recommendations about suitable products. With Hamish's consent, Vikingforce transfers Hamish's CDR data to Turtledoors so he can acquire the recommended product.

Vikingforce holds Hamish's CDR data for the purpose of providing Hamish with a product comparison service and product recommendations, and must take reasonable steps to ensure the data is accurate, up to date and complete having regard to this purpose.

Vikingforce does not hold Hamish's CDR data for the purpose of transferring it to Turtledoors for Hamish to acquire a product, and must disregard this purpose when taking reasonable steps to ensure the data is accurate, up to date and complete under Privacy Safeguard 11.

11.20 The 3 terms listed in Privacy Safeguard 11, 'accurate', 'up to date', and 'complete', are not defined in the Competition and Consumer Act 2010 (Competition and Consumer Act) or the Privacy Act.²⁰

¹⁷ Metering data is a type of AEMO data: CDR Rules, clause 1.2 of Schedule 4.

¹⁸ AEMO data is specified as SR data for the energy sector: see CDR Rules, clause 4.3 of Schedule 4. For the application of rules in relation to SR data, see Division 1.5 of Part 1 of the CDR Rules.

¹⁹ Regulation 28RA(4) of the Competition and Consumer Regulations; pages 3–4 of the Explanatory Statement to the Competition and Consumer Amendment (Consumer Data Right) Regulations 2021.

²⁰ These terms are also used in Privacy Safeguard 13 in respect of the requirement for a data holder, as an alternative to correcting the CDR data, to include a statement with CDR Data to ensure that it is accurate, up to date, complete and not misleading, after receiving a request from the consumer to correct the CDR data (see [Chapter 13 \(Privacy Safeguard 13\)](#)).

11.21 The following analysis of each term draws on the ordinary meaning of the terms and the APP Guidelines.²¹ As the analysis indicates, there is overlap in the meaning of the terms.

Accurate

11.22 CDR data is inaccurate if it contains an error or defect or is misleading. An example is factual information about a consumer's contact details, account, income, assets, payment or repayment history or employment status which is incorrect having regard to the purpose for which it is held.

11.23 CDR data that is derived from other CDR data is not inaccurate by reason only that the consumer disagrees with the method or result of the derivation.²² For the purposes of Privacy Safeguard 11, derived data may be 'accurate' if it is presented as such and accurately records the method of derivation (if appropriate).

11.24 For instance, an accredited data recipient may use the existing information it holds about a consumer to predict their income over a certain period of time. If the data is presented as the estimated future income for the consumer for that period, and states the basis for that estimation (that is, it is based on the consumer's income over previous financial years), this would not be inaccurate solely because the consumer believes their income will be higher or lower during the projected period.

11.25 CDR data may be inaccurate even if it is consistent with a consumer's instructions or if the inaccuracy is attributable to the consumer. For example, if a consumer has provided an incorrect mobile number which is held by the data holder for the purpose of being able to contact the consumer, and the data holder discloses this, the CDR data may be inaccurate and the data holder may later become aware of this inaccuracy.

Up to date

11.26 CDR data is not up to date if it contains information that is no longer current at, or during, the time that the data holder is required or authorised to disclose the CDR data. An example is a statement that a consumer has an active account with a certain entity, where the consumer has closed that account before the time that the data disclosure occurred. Another example is an assessment that a consumer has the ability to meet a loan repayment obligation, where in fact the consumer's ability to do so changed in the period before the data disclosure was required or authorised.²³

11.27 CDR data about a past event may have been up to date at the time it was recorded but has been overtaken by a later development. Whether that data is up to date at the time it is disclosed will depend on the purpose for which it is held. For example, if a consumer has had a second child but their CDR data records them as having only one child, the CDR data will still be up to date if that data is held for the purpose of recording whether the consumer is a parent.

11.28 In a similar manner to accuracy, CDR data may not be up to date even if it is consistent with a consumer's instructions or if the inaccuracy is attributable to the consumer.

²¹ See APP Guidelines, [Chapter 10 \(APP 10\)](#).

²² Data derived from CDR data continues to be 'CDR data': see Competition and Consumer Act, section 56AI.

²³ Such an assessment will likely be 'materially enhanced information' under section 10 of the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019, or section 11 of the Consumer Data Right (Energy Sector) Designation 2020, and therefore not 'required consumer data' under the CDR Rules.

Complete

11.29 CDR data is incomplete if it presents a partial or misleading picture of a matter of relevance, rather than a true or full picture.

11.30 An example is data from which it can be inferred that a consumer owes a debt, which in fact has been repaid. The CDR data will be incomplete under Privacy Safeguard 11 if the data is held, for instance, for the purpose of determining the borrowing capacity of the consumer. Where the CDR data is held for a different purpose for which the debt is irrelevant, the fact that the debt has been repaid may not of itself render the CDR data incomplete. If, however, the accredited person has requested a consumer's CDR data for a specific period, and in that period the consumer owed a debt which is recorded in the CDR data, and that debt was repaid in a later period, the CDR data will still be 'complete' in respect of that specific period.

Taking reasonable steps to ensure the quality of CDR data

When must an entity take reasonable steps?

11.31 Privacy Safeguard 11 requires an entity to take reasonable steps to ensure the quality of CDR data at the following points in time:

- **for data holders:** at the time the entity is required or authorised, or throughout the period in which the entity is required or authorised, to disclose CDR data under the CDR Rules. This includes when a data holder discloses CDR data:
 - to accredited data recipients under rule 4.6 in the CDR Rules, and
 - to consumers under rule 3.4 in the CDR Rules
- **for accredited data recipients:** at the time the entity discloses CDR data when required or authorised under the CDR Rules. This includes (but is not limited to) when an accredited data recipient discloses CDR data to:
 - an accredited data recipient under paragraph 7.5(1)(i) in the CDR Rules²⁴
 - the consumer under paragraph 7.5(1)(d) in the CDR Rules
 - an outsourced service provider (OSP) under paragraph 7.5(1)(f) in the CDR Rules
 - a sponsor or affiliate under paragraph 7.5(1)(f) in the CDR Rules
 - a trusted adviser under paragraph 7.5(1)(e) in the CDR Rules
 - a specified person (in the case of a CDR insight) under paragraph 7.5(1)(e) in the CDR Rules
 - a specified person (in the case of a business consumer disclosure) under paragraph 7.5(1)(e) in the CDR Rules, or
 - a CDR representative under paragraph 7.5(1)(j) in the CDR Rules.

²⁴ Disclosure of CDR data to an accredited person under an 'AP disclosure consent' has been permitted since 1 July 2021: CDR Rules, subrule 7.5A(1).

- 11.32 At other times, regular reviews of the quality of CDR data held by the entity may also assist to ensure the CDR data is accurate, up-to-date and complete at the time it is disclosed.
- 11.33 Entities should also be aware that Privacy Safeguard 11 only requires accredited data recipients to take reasonable steps when disclosing CDR data *under the CDR Rules*. It does not apply in relation to other disclosures of CDR data, for example where an accredited data recipient is required or authorised under another Australian law or court/tribunal order to disclose CDR data. The concept, ‘required or authorised to use or disclose CDR data under the CDR Rules’ is discussed in [Chapter B \(Key concepts\)](#).

Risk point: If a data holder does not have systems in place to maintain data quality, and takes steps to ensure the quality of CDR data only at the time of the disclosure or authorisation, there is a greater risk that the data will be incorrect at that time. There is also a greater risk that the consumer will later request that the data holder correct CDR data it disclosed, meaning the data holder will also need to follow the process in Privacy Safeguard 13.²⁵

Privacy tip: While the obligation to ensure the quality of CDR data under Privacy Safeguard 11 applies only at the time a data holder is required or authorised to disclose the data, data holders should have processes and procedures in place to periodically update and confirm the accuracy of the CDR data that they hold, during periods in which they are not required or authorised to disclose the data. As CDR data that falls under the privacy safeguards is also personal information, data holders should already have in place such processes and procedures to ensure the accuracy of personal information they collect, use and disclose for the purposes of APP 10.

What constitutes ‘reasonable steps’?

11.34 The requirement to ensure the quality of CDR data is subject to a ‘reasonable steps’ test.

11.35 This test requires an objective assessment of what is considered reasonable, having regard to the purpose for which the information is held, which could include:

- **The nature of the entity.** The size of the entity, its resources, the complexity of its operations and its business model are all relevant to determining what steps would be reasonable for the entity to take to ensure the quality of the CDR data it is authorised or required to disclose.
- **The sensitivity of the CDR data held and adverse consequences for the consumer if the quality of CDR data is not ensured.** An entity should consider the sensitivity of the data and possible adverse consequences for the consumer concerned if the CDR data is not correct for the purpose it is held. For example, a data holder should take more extensive steps to ensure the quality of highly sensitive data that it might be required or authorised to disclose. More rigorous steps may be required as the risk of adversity increases.
- **Whether the CDR data has been inferred.** Entities may be required to take more rigorous steps to ensure the quality of CDR data that has been created, generated or inferred through analytics processes.

²⁵ For further information, see paragraphs 11.66 to 11.68 and [Chapter 13 \(Privacy Safeguard 13\)](#).

- **The practicability of taking action, including time and cost involved.** A ‘reasonable steps’ test recognises that privacy protection must be viewed in the context of the practical options available to entities. The time, cost and resources involved in ensuring the quality of CDR data are relevant considerations. However, an entity is not excused from taking certain steps by reason only that it would be inconvenient, time-consuming, or impose some cost to do so. Whether these factors make it unreasonable to take a particular step will depend on whether the burden is excessive in all the circumstances.

11.36 In some circumstances, it will be reasonable for an accredited data recipient to take no steps to ensure the quality of CDR data. For example, where an accredited data recipient collects CDR data from a data holder known to be reliable, and the accredited data recipient has not created, generated, or inferred any further CDR data, it may be reasonable to take no steps to ensure the quality of that data. It is the responsibility of the accredited data recipient in this example to be able to justify that this is reasonable.

Examples of reasonable steps

11.37 The following are given as examples of reasonable steps that an entity should consider:

- Implementing internal practices, procedures and systems to verify, audit, monitor, identify and correct poor-quality CDR data to ensure that CDR data is accurate, up to date and complete at the point of disclosure.
- Ensuring internal practices, procedures and systems are commensurate with other reasonable steps the entity is taking to ensure the quality of CDR data the entity is authorised or required to disclose.
- Ensuring updated or new CDR data is promptly added to the relevant existing records as appropriate.²⁶
- For a data holder, implementing protocols to ensure that the CDR data is accurate, up to date and complete both before and once it has been converted to the format required by the Data Standards.
- For an accredited data recipient, ensuring that any analytic processes used are operating appropriately and are fit for purpose, and not creating inaccurate or unjustified results. This is because data derived from CDR data collected by an accredited data recipient continues to be ‘CDR data’.²⁷

Advising a consumer when disclosed CDR data is incorrect

11.38 Under Privacy Safeguard 11, if a data holder or accredited data recipient becomes aware that disclosed CDR data was not accurate, up to date and complete, they must advise the consumer in accordance with the CDR Rules.²⁸

²⁶ Compliance with Privacy Safeguard 13 (correction of CDR data) and where relevant, APP 13 (correction of personal information) for data holders, can also support this example for taking reasonable steps to ensure quality of CDR data.

²⁷ See Competition and Consumer Act, section 56AI.

²⁸ See Competition and Consumer Act, subsection 56EN(3).

11.39 Rule 7.10 in the CDR Rules sets out the requirements for notifying the consumer where a data holder or accredited data recipient becomes aware that disclosed CDR data was not accurate, up to date and complete. These requirements are summarised below.

In what circumstances must a consumer be advised that disclosed CDR data was incorrect?

11.40 Data holders and accredited data recipients must advise a consumer that some or all of the CDR data was incorrect if the entity:²⁹

- has disclosed CDR data after being required or authorised to do so under the CDR Rules, and
- later becomes aware that some or all of the CDR data, when disclosed, was not accurate, up to date and complete, having regard to the purpose for which the data was held.

11.41 Data holders and accredited data recipients may later ‘become aware’ of inaccuracies in CDR data that was previously disclosed if they discover an inconsistency during normal business practices. Examples include but are not limited to circumstances where:

- information provided by the consumer is inconsistent with CDR data previously disclosed, or
- the entity is notified by the consumer or another entity that the CDR data is incorrect (this may include a data holder providing corrected data to an accredited data recipient),³⁰ or
- a practice, procedure or system that the entity has implemented to ensure compliance with the privacy safeguards (such as a periodic audit or monitoring program) indicates that the CDR data previously disclosed was incorrect.

11.42 The obligation to notify the consumer that disclosed CDR data was incorrect is not affected by whether the entity took reasonable steps to ensure the quality of the data. Privacy Safeguard 11 and rule 7.10 of the CDR Rules require the consumer to be notified when, in fact, the CDR data was not accurate, up to date and complete when disclosed, regardless of the reason for the incorrect data.

What information must be provided to the consumer when incorrect CDR data has been disclosed?

11.43 Rule 7.10 of the CDR Rules requires a data holder or accredited data recipient that has disclosed incorrect CDR data to an accredited person to provide the consumer, via electronic means, with a written notice that:

- identifies the accredited person to whom the incorrect CDR data was disclosed
- states the date of the disclosure

²⁹ Competition and Consumer Act, subsection 56EN(3).

³⁰ If a consumer notifies a data holder or accredited data recipient that the CDR data it disclosed was incorrect, the consumer may also request that the entity correct that CDR data. When this happens, Privacy Safeguard 13 will also apply to the data holder or accredited data recipient. For further information see paragraphs 11.66 to 11.68 and [Chapter 13 \(Privacy Safeguard 13\)](#).

- identifies which CDR data was incorrect, and
- states that the data holder or accredited data recipient must disclose the corrected data to that accredited person if the consumer requests that they do so.

11.44 Where the data holder or accredited data recipient disclosed the incorrect CDR data to an accredited person who was collecting that CDR data on behalf of another accredited person (the ‘OSP principal’) as a direct or indirect OSP under a CDR outsourcing arrangement, the data holder or accredited data recipient only needs to identify in the notice the OSP principal accredited person on whose behalf the data was collected.³¹

11.45 A notice may deal with one or more disclosures of incorrect CDR data.

How must a notice be provided?

11.46 Rule 7.10 of the CDR Rules requires a data holder or accredited data recipient to notify the consumer in writing by electronic means after disclosing incorrect data.

11.47 The requirement for this notice to be given by electronic means will be satisfied if, for example, the notice is given over email or over the consumer’s dashboard.

11.48 The written notice may, for instance, be in the body of an email or in an electronic file attached to an email.

Privacy tip: In selecting an ‘electronic means’ for the notice, the data holder or accredited data recipient should consider the consumer’s chosen method for receiving communications from the entity (if applicable) and whether the consumer is likely to receive the notice in a timely manner through a given ‘electronic means’. For example, if a consumer has elected to receive communications from the entity by email, it may be most appropriate to deliver the notice through that means.

How quickly must the consumer be notified?

11.49 Data holders and accredited data recipients must provide notices to the consumer as soon as practicable, but no more than 5 business days after the entity becomes aware that some or all of the disclosed data was incorrect.

11.50 The test of practicability is an objective test. The entity should be able to justify that it is not practicable to give notification more quickly than 5 days after becoming aware of the disclosure of incorrect CDR data.³²

11.51 In adopting a timetable that is ‘practicable’, an entity can take technical and resource considerations into account. However, it is the responsibility of the entity to justify any delay in providing the notice.

11.52 The maximum time of 5 business days will rarely be an appropriate period of time before a notice is given. This maximum period would only be appropriate in circumstances such as

³¹ CDR Rules, paragraph 1.16(5)(b). For information on ‘CDR outsourcing arrangements’, see [Chapter B \(Key concepts\)](#).

³² Options for providing early notification should, so far as practicable, be built into the entity’s processes and systems. For example, processes and systems should be in place to promptly notify a consumer that incorrect CDR data has been disclosed if the entity corrects CDR data (such as in response to a consumer’s correction request) that it had disclosed prior to it being corrected.

where a system error has caused a data holder to disclose incorrect data to a large number of accredited persons in respect of a large number of consumers.

11.53 The 5 business day period commences on the day after the entity becomes aware that some or all of the disclosed data was incorrect.³³ For example, if the entity becomes aware on 2 August, the 5 business day period begins on 3 August.

11.54 A ‘business day’ is a day that is not Saturday, Sunday or a public holiday in the place concerned.³⁴

Example

Blue Book Ltd is a data holder for a large number of consumers. Hazel authorises Blue Book to disclose her CDR data to an accredited person, Credibility Pty Ltd. Soon after the data is disclosed on 1 July, Credibility queries whether Hazel’s account data is correct.

Blue Book then becomes aware that some of the data was incorrect when disclosed because it showed the incorrect address for Hazel. Hazel’s address was inaccurate for the purpose for which Blue Book held the information (contacting Hazel). Within a number of hours, Blue Book is able to provide a notice to Hazel over her consumer dashboard which states that:

- incorrect CDR data was given to Credibility on 1 July
- the account data was incorrect due to a mistake in Hazel’s address, and
- Blue Book will be required to disclose the corrected data to Credibility if Hazel requests that they do so.

Blue Book has provided Hazel with the notice required under Rule 7.10 in the CDR Rules and Privacy Safeguard 11, as soon as practicable. (Blue Book also ensures that it updates its own data holdings promptly upon becoming aware of the inaccuracy. Ensuring that known errors are corrected promptly, regardless of how they are identified, is a reasonable step required by subsection 56EN(1) of the Competition and Consumer Act (i.e. Privacy Safeguard 11).

Blue Book then realises that the error is systemic and has caused it to disclose incorrect CDR data in respect of all similar disclosures to accredited persons.

Blue Book hires experts to undertake an urgent review of its CDR disclosures and determine the extent of the error. It takes Blue Book almost 5 business days before it is in a position to send all affected CDR consumers a notice similar to the one given to Hazel.

Blue Book would need to be able to demonstrate that it has sent the affected consumers the required notices as soon as practicable, to ensure compliance with Rule 7.10 in the CDR Rules and Privacy Safeguard 11.

³³ See *Acts Interpretation Act 1901*, section 36.

³⁴ *Acts Interpretation Act 1901*, section 2B.

In what circumstances must an entity disclose corrected CDR data to the original recipient?

11.55 Privacy Safeguard 11 requires data holders and accredited data recipients to disclose corrected CDR data, in accordance with the CDR Rules, to the original recipient³⁵ of the disclosure if:³⁶

- the entity has advised the consumer that some or all of the CDR data was incorrect when the entity disclosed it, and
- the consumer requests, in accordance with the CDR rules, the entity to disclose the corrected CDR data.

11.56 The obligation to disclose corrected CDR data applies regardless of whether the entity failed to take reasonable steps to ensure the quality of the CDR data disclosed.

11.57 The term ‘corrected CDR data’ is not defined in the Competition and Consumer Act. For the purposes of the obligation to disclose corrected CDR data under Privacy Safeguard 11, ‘corrected CDR data’ includes:

- CDR data which has been corrected in accordance with paragraph 56EP(3)(a)(i) of the Competition and Consumer Act, and
- CDR data for which a qualifying statement has been included in accordance with paragraph 56EP(3)(a)(ii) of the Competition and Consumer Act.³⁷

Record keeping requirements

11.58 If an entity discloses corrected CDR data in accordance with Privacy Safeguard 11,³⁸ the entity (and, if the data is disclosed to an accredited person, the recipient) must comply with the record keeping requirements under rule 9.3 in the CDR Rules.

11.59 For data holders, subrule 9.3(1) of the CDR Rules requires the entity to keep and maintain various records relating to CDR data, including records of disclosures of CDR data made in response to consumer data requests.³⁹ If corrected data is disclosed, the data holder must keep and maintain a record of both the initial disclosure in which incorrect CDR data was disclosed, and the subsequent disclosure in which the corrected CDR data was disclosed. This is because both disclosures are made in response to the original consumer data request. There is no requirement, however, to record the disclosure as either ‘correct’ or ‘incorrect’.

11.60 For accredited data recipients, subrule 9.3(2) of the CDR Rules requires the recipient to keep and maintain various records relating to CDR data, including records of collections of CDR data under the CDR Rules.⁴⁰ This means that, similarly to data holders, accredited data

³⁵ The original recipient may be the consumer where the data holder disclosed the CDR data to the consumer in response to a valid consumer request in accordance with subrules 3.4(2) or (3) in the CDR Rules.

³⁶ Competition and Consumer Act, subsection 56EN(4).

³⁷ See [Chapter 13 \(Privacy Safeguard 13\)](#).

³⁸ Competition and Consumer Act, subsection 56EN(4).

³⁹ CDR Rules, paragraph 9.3(1)(d). For further information on record keeping requirements for data holders, see the [Guide to privacy for data holders](#).

⁴⁰ CDR Rules, paragraph 9.3(2)(e).

recipients must keep and maintain a record of both the initial collection of the incorrect CDR data and the subsequent collection of the corrected CDR data, in circumstances where corrected CDR data is disclosed under subsection 56EN(4) of the Competition and Consumer Act.

How does Privacy Safeguard 11 interact with the other privacy safeguards?

Privacy Safeguard 5

- 11.61 Privacy Safeguard 5 requires an accredited data recipient to notify a consumer of the collection of their CDR data by updating the consumer's dashboard.
- 11.62 Where an accredited data recipient has collected CDR data, and then collects corrected CDR data after the data holder complies with the consumer's request to correct and disclose corrected data under Privacy Safeguards 11 and 13, the accredited data recipient must notify that consumer under Privacy Safeguard 5 in respect of both collections.

Privacy Safeguard 10

- 11.63 Privacy Safeguard 10 requires data holders to notify a consumer of the disclosure of their CDR data by updating the consumer's dashboard.
- 11.64 Where a data holder has disclosed CDR data, and then discloses corrected CDR data as a result of the consumer's request to correct and disclose corrected CDR data under Privacy Safeguards 11 and 13, the data holder must notify that consumer under Privacy Safeguard 10 in respect of both disclosures.

Example

McCarthy Bank Ltd, a data holder, discloses Satoko's CDR data to accredited person, Watson and Co, in response to a consumer data request made on Satoko's behalf.

McCarthy Bank updates Satoko's consumer dashboard under Privacy Safeguard 10 and rule 7.9 in the CDR Rules, and Watson and Co updates Satoko's consumer dashboard under Privacy Safeguard 5 and rule 7.4 in the CDR Rules.

However, Satoko realises that the CDR data disclosed by McCarthy Bank is not accurate, and asks McCarthy Bank to correct the data.

McCarthy Bank corrects the CDR data in accordance with Privacy Safeguard 13 and rule 7.15 in the CDR Rules. McCarthy Bank also takes reasonable steps to correct its own data holdings as required by Privacy Safeguard 11, as it is made aware of inaccuracies through Satoko's request.

In accordance with Privacy Safeguard 11, McCarthy Bank then advises Satoko that Satoko may request that the corrected data be disclosed to Watson and Co. Satoko makes this request, and McCarthy Bank complies. Both Watson and Co and McCarthy Bank update Satoko's consumer dashboards accordingly.

Privacy Safeguard 12

11.65 Where an accredited data recipient amends CDR data to comply with Privacy Safeguard 11, it should consider whether it needs to take action under Privacy Safeguard 12 to destroy or de-identify the original data.

Privacy Safeguard 13

11.66 As set out in [Chapter 13 \(Correction of CDR data\)](#), a correction request made under Privacy Safeguard 13 may trigger the obligations under Privacy Safeguard 11.

11.67 Privacy Safeguard 13 applies where a consumer requests that a data holder or accredited data recipient correct their CDR data, where that data has previously been disclosed under the CDR Rules. In most circumstances, Privacy Safeguard 13 requires the data holder or accredited data recipient to respond to the consumer's request by either correcting the CDR data, including a qualifying statement with the CDR data to ensure it is accurate, up to date, complete and not misleading (having regard to the purpose for which it is held), or stating why a correction is unnecessary or inappropriate.⁴¹

11.68 Where a data holder corrects CDR data or includes a qualifying statement with the data in accordance with Privacy Safeguard 13, they should be aware that this may trigger Privacy Safeguard 11, meaning the consumer must be advised of any previous disclosures of the CDR data where the data may have been incorrect when it was disclosed. In such circumstances, the data holder will be on notice that the CDR data was likely incorrect when disclosed.

⁴¹ Competition and Consumer Act, paragraph 56EP(3)(a); CDR Rules, rule 7.15. Privacy Safeguard 13 does not apply to AEMO: Competition and Consumer Regulations, paragraph 28RA(2)(a)(iii). Different obligations apply to retailers who receive a Privacy Safeguard request that relates to AEMO data: clause 6.1 of Schedule 4 to the CDR Rules. For further information, see [Chapter 13 \(Correction of CDR data\)](#).

Chapter 12:

Privacy Safeguard 12 —

Security of CDR data, and destruction or de-identification of redundant data

Version 5.0, November 2023



Contents

Key points	3
What does Privacy Safeguard 12 say?	3
Why is it important?	4
Who does Privacy Safeguard 12 apply to?	4
Accreditation guidelines on information security	5
How Privacy Safeguard 12 interacts with the Privacy Act	6
PART A: Security of CDR data	7
What do security measures need to protect against?	7
What steps does an entity need to take to secure CDR data?	8
Additional conditions on sponsors to ensure CDR data is secure	18
Notifiable Data Breach (NDB) scheme	19
PART B: Treatment of redundant data (destruction and de-identification)	20
Overview of the process for treating redundant data	20
What is 'redundant data'?	22
Deciding how to deal with redundant data	23
Steps to destroy redundant data	26
Steps to de-identify redundant data	28
Other relevant security obligations	29
Privacy safeguards	29
Other CDR de-identification processes	30

Key points

- Securing CDR data is an integral element of the consumer data right (CDR) system.
- Privacy Safeguard 12¹ places requirements on accredited data recipients of CDR data and designated gateways to ensure CDR data is protected from misuse, interference and loss, as well as from unauthorised access, modification or disclosure. The specific steps that these entities must take to protect CDR data are in the consumer data rules (CDR Rules).
- In addition, if an accredited data recipient of CDR data or a designated gateway no longer needs the CDR data for purposes permitted by the privacy safeguards or the CDR Rules, then the data is considered 'redundant data' and will need to be destroyed (or deleted) or de-identified unless an exception applies.
- An applicant for accreditation must demonstrate compliance with the information security requirements in Privacy Safeguard 12 in order to gain and maintain accreditation under the CDR system.

What does Privacy Safeguard 12 say?

- 12.1 Accredited data recipients of CDR data and designated gateways must take the steps in the CDR Rules to protect CDR data from misuse, interference and loss, as well as unauthorised access, modification and disclosure.
- 12.2 Accredited data recipients of CDR data and designated gateways must also take the steps set out in the CDR Rules to destroy or de-identify any CDR data that is no longer needed for:
- the purposes permitted under the CDR Rules, or
 - any purpose for which the information may be used or disclosed under the privacy safeguards.
- 12.3 Consumers can request that their CDR data be deleted once it is no longer needed.² Accredited data recipients of CDR data and designated gateways must delete CDR data that is subject to a deletion request unless an exception applies.
- 12.4 These requirements apply except where:
- the accredited data recipient or designated gateway is required by an Australian law or a court/tribunal order to keep the CDR data, or
 - the CDR data relates to current or anticipated legal or dispute resolution proceedings to which the accredited data recipient, designated gateway or consumer is a party.

¹ Competition and Consumer Act, section 56EO.

² CDR Rules, rule 4.16.

Why is it important?

- 12.5 Poor information security can leave systems and services at risk and may cause harm and distress to individuals, whether to their well-being, finances, or reputation. Some examples of harm include:
- financial fraud, including unauthorised credit card transactions or credit fraud
 - identity theft causing financial loss or emotional and psychological harm
 - family violence, and
 - physical harm or intimidation.
- 12.6 Poor information security practices negatively impact an entity’s reputation and undermine its commercial interests. As shown in the OAI’s long-running [Australian community attitudes to privacy survey](#), privacy protection contributes to an individual’s trust in an entity. If an entity is perceived to be handling data contrary to community expectations, individuals may seek out alternative products and services.
- 12.7 In addition, accredited data recipients are entrusted with CDR data under the CDR system to allow them to provide products and services to consumers. Privacy Safeguard 12 ensures that accredited data recipients are taking steps to ensure a consistent, high standard of security under the CDR Rules to ensure this data is protected. This helps to build public trust and confidence in the security practices of accredited data recipients.
- 12.8 Deleting or de-identifying redundant data also minimises the risk profile of an accredited data recipient as they are not holding unnecessary CDR data.

Who does Privacy Safeguard 12 apply to?

- 12.9 Privacy Safeguard 12 applies to accredited data recipients of CDR data and designated gateways for CDR data. It does not apply to data holders. However, data holders must ensure that they are adhering to their obligations under the *Privacy Act 1988* (the Privacy Act) and the APPs, including APP 11, in relation to the security of personal information.
- 12.10 As a non-accredited entity, a CDR representative is not directly bound by Privacy Safeguard 12. However, under the terms of the CDR representative arrangement with their CDR representative principal,³ a CDR representative is required to comply with Privacy Safeguard 12 in its handling of service data as if it were the CDR representative principal.^{4,5} A CDR representative is also required to take the steps in Schedule 2 of the CDR Rules to protect the service data as if it were the CDR representative principal.⁶ A failure by the CDR

³ A CDR representative arrangement is a written contract between a person with unrestricted accreditation (the CDR representative principal) and a person without accreditation (the CDR representative). The requirements for this arrangement are outlined in CDR Rules, rule 1.10AA.

⁴ CDR Rules, paragraph 1.10AA(4)(a)(iv).

⁵ See [Chapter B \(Key concepts\)](#) for more information on ‘CDR representative principal’, ‘CDR representative’, ‘CDR representative arrangement’ and ‘service data’.

⁶ CDR Rules, paragraph 1.10AA(4)(b).

representative to comply with Privacy Safeguard 12 or Schedule 2 is taken to be a failure by the CDR representative principal.⁷

12.11 Where they are a non-accredited entity, an outsourced service provider (OSP) is not directly bound by Privacy Safeguard 12. However, under the terms of the CDR outsourcing arrangement with their OSP principal,⁸ an OSP is required to take the steps in Schedule 2 of the CDR Rules to protect the service data as if it were an accredited data recipient.⁹ An OSP is also required to comply with the OSP principal's CDR policy as it relates to deletion and de-identification of CDR data and the treatment of redundant or de-identified CDR data as if it were the OSP principal.¹⁰ For an accredited OSP chain principal, a failure to comply with Schedule 2 in relation to service data by their direct or indirect OSP is taken to be a failure by the OSP chain principal.¹¹

Note: *There are no designated gateways in the banking sector or energy sector.¹² See Chapter B (Key concepts) for the meaning of designated gateway.*

Accreditation guidelines on information security

12.12 This chapter provides guidance on the steps for securing CDR data and managing redundant data in compliance with Privacy Safeguard 12.

12.13 An applicant for accreditation must demonstrate compliance with information security requirements in Privacy Safeguard 12 in order to gain and maintain accreditation under the CDR system.

12.14 Accredited persons should refer to the Supplementary accreditation guidelines: information security by the Australian Competition and Consumer Commission (ACCC)¹³ for specific guidance on the:

⁷ CDR Rules, subrules 7.11(3) and 7.12(3). A failure by any direct or indirect OSP of the CDR representative to comply with Schedule 2 is also taken to be a failure by the CDR representative principal. See also rule 1.16A in relation to a CDR representative principal's obligations and liability.

⁸ A CDR outsourcing arrangement is a written contract between an OSP principal and their provider that meets the minimum requirements listed in CDR Rules, subrule 1.10(3).

⁹ CDR Rules, subrule 1.10(3)(b)(ii).

¹⁰ CDR Rules, paragraph 1.10(3)(b)(i)(A).

¹¹ CDR Rules, subrule 7.11(2). See also rule 1.16 in relation to an OSP principal's obligations and liability.

¹² For the banking sector, see the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019. For the energy sector, the energy designation specifies AEMO as a gateway for certain information: Consumer Data Right (Energy Sector) Designation 2020, subsection 6(4). However, at the time of publication, AEMO is not a designated gateway for any CDR data because under current CDR Rules, no CDR data is (or is to be) disclosed to AEMO because of the reasons in subsection 56AL(2)(c) of the Competition and Consumer Act.

There are also no designated gateways in the telecommunications sector (Consumer Data Right (Telecommunications Sector) Designation 2022) or non-bank lending sector (Consumer Data Right (Non-Bank Lenders) Designation 2022), although unlike the banking and energy sectors, at the date of publication of these guidelines, there are no rules allowing for the sharing of designated telecommunications data or non-bank lending data under the CDR system.

¹³ <https://www.cdr.gov.au/resources/guides/accreditation-guidelines>.

- information security obligations under Privacy Safeguard 12 that applicants must satisfy for accreditation under the CDR system, and
- ongoing information security and reporting obligations under Privacy Safeguard 12, including preparing attestation and assurance reports.

How Privacy Safeguard 12 interacts with the Privacy Act

12.15 It is important to understand how Privacy Safeguard 12 interacts with the Privacy Act and the APPs.¹⁴

12.16 APP 11 requires APP entities to take measures to ensure the security of personal information they hold and to consider whether they are permitted to retain this personal information (see APP Guidelines, [Chapter 11 \(APP 11\)](#)).

CDR entity	Privacy protections that apply in the CDR context
Accredited data recipient	<p>Privacy Safeguard 12</p> <p>For accredited data recipients of a consumer’s CDR data, Privacy Safeguard 12 applies to the security of that CDR data.¹⁵</p> <p>APP 11 does not apply in relation to that CDR data.¹⁶</p> <p>Note: Accredited persons must also demonstrate compliance with the information security requirements in Privacy Safeguard 12 to maintain accreditation.¹⁷</p>
Designated gateways	Privacy Safeguard 12

¹⁴ The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies (APP entities). See also APP Guidelines, [Chapter B \(Key concepts\)](#).

¹⁵ Privacy Safeguard 12 applies from the point when the accredited person becomes an accredited data recipient of the CDR data. An accredited person becomes an accredited data recipient for CDR data when:

- CDR data is held by (or on behalf of) the person
- the CDR data, or any other CDR data from which it was directly or indirectly derived, was disclosed to the person under the consumer data rules, and
- the person is neither a data holder, nor a designated gateway, for the first mentioned CDR data. See Competition and Consumer Act, section 56AK.

¹⁶ The APPs do not apply to an accredited data recipient of CDR data, in relation to that CDR data: Competition and Consumer Act, paragraph 56EC(4)(a). However, subsection 56EC(4) does not affect how the APPs apply to accredited persons and accredited data recipients who are APP entities, in relation to the handling of personal information outside the CDR system. (Note: Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See Privacy Act, subsection 6E(1D).) Subsection 56EC(4) also does not affect how the APPs apply to an accredited person who does not become an accredited data recipient of the CDR data (other than for Privacy Safeguards 1 – 4). See Competition and Consumer Act, paragraph 56EC(5)(aa).

¹⁷ See the ACCC’s Supplementary accreditation guidelines: information security for more information.

For designated gateways for CDR data, Privacy Safeguard 12 applies to the security of the CDR data.¹⁸

APP 11 does not apply in relation to that CDR data.¹⁹

Data holders²⁰

APP 11

Privacy Safeguard 12 does not apply to data holders.

PART A: Security of CDR data

What do security measures need to protect against?

12.17 An accredited data recipient is required to put in place information security measures specified in the CDR Rules to protect the CDR data they receive from misuse, interference and loss, as well as unauthorised access, modification and disclosure.

12.18 A designated gateway of CDR data is required to put in place information security measures specified in the CDR Rules to protect that CDR data from misuse, interference and loss, as well as unauthorised access, modification and disclosure.

12.19 The terms ‘misuse’, ‘interference’, ‘loss’, ‘unauthorised access’, ‘unauthorised modification’ and ‘unauthorised disclosure’ are not defined in the *Competition and Consumer Act 2010* (Competition and Consumer Act). The following discussion represents the OAIC’s interpretation of these terms based on their ordinary meaning. However, given that information security is an evolving concept, the discussion below is not intended as an exhaustive list of examples.

- **Misuse:** occurs where CDR data is used for a purpose not permitted by the CDR Rules. For example, misuse would occur if an employee of a CDR entity browses consumer statements to discover information about someone they know.²¹
- **Interference:** occurs when there is an attack on CDR data that interferes with the CDR data but does not necessarily modify its content. For example, interference would occur if there is a ransomware attack that leads to the data being locked down and ransomed.
- **Loss:** refers to the accidental or inadvertent loss of CDR data where the data is no longer accessible and usable for its purpose, or in circumstances where it is likely to result in authorised access or disclosure. Examples of loss include physical loss by

¹⁸ Competition and Consumer Act, subsection 56EO(1).

¹⁹ The APPs do not apply to designated gateways for CDR data in relation to that CDR data: Competition and Consumer Act, paragraph 56EC(4)(d). However, subsection 56EC(4) does not affect how the APPs apply to designated gateways who are APP entities, in relation to the handling of personal information outside the CDR system. See Competition and Consumer Act, paragraph 56EC(5)(b).

²⁰ In this chapter, references to data holders include AEMO. See [Chapter B \(Key concepts\)](#) for further information about how the privacy safeguards apply to AEMO.

²¹ Privacy Safeguard 6 sets out when an accredited data recipient of CDR data or a designated gateway for CDR data is permitted to use that CDR data (see [Chapter 6 \(Privacy Safeguard 6\)](#)). Privacy Safeguards 7 and 9 also contain requirements relating to an entity’s use of CDR data for the purpose of direct marketing and use of government related identifiers respectively (see [Chapters 7 \(Privacy Safeguard 7\)](#) and [9 \(Privacy Safeguard 9\)](#)).

leaving data in a public place, failing to keep adequate backups in the event of systems failure or as a result of natural disasters.²²

- **Unauthorised access:** occurs where CDR data is accessed by someone who is not permitted to do so. This includes unauthorised access by an employee of the accredited data recipient or designated gateway, or an independent contractor, as well as unauthorised access by an external third party. For example, unauthorised access would occur if a computer network is compromised by an external attacker resulting in CDR data being accessed without authority.
- **Unauthorised modification:** occurs where CDR data is altered by someone who is not permitted to do so, or where the data is altered in a way that is not permitted. For example, unauthorised modification would occur if an employee of an accredited data recipient or designated gateway altered a consumer's savings account information to offer a more favourable deal.
- **Unauthorised disclosure:** occurs where an accredited data recipient or designated gateway, whether intentionally or unintentionally, makes CDR data accessible or visible to others outside the entity. For example, unauthorised disclosure includes 'human error', such as an email sent to the wrong person. It can also include disclosure of CDR data to a scammer as a result of inadequate identity verification procedures.

12.20 Information security not only covers cybersecurity (the protection of networks and information systems from cyber-attack), but also physical and organisational security measures.

What steps does an entity need to take to secure CDR data?

12.21 Privacy Safeguard 12 requires accredited data recipients and designated gateways to take the steps in the CDR Rules to protect the CDR data from misuse, interference and loss, as well as unauthorised access, modification and disclosure. These steps are detailed in Schedule 2 of the CDR Rules.

12.22 The CDR Rules provide obligations for accredited data recipients to have governance requirements in place, understand their data environment and risk posture, and implement minimum security controls.²³ Additional conditions also apply to an accredited person who proposes, under a sponsorship arrangement, to become the sponsor of a person who has sponsored accreditation (the affiliate).²⁴ These conditions relate to the affiliate's information security capabilities, and are outlined below at paragraph 12.76. For more information on the sponsorship model, see Chapter B key concepts.

12.23 Broadly, the steps accredited data recipients must take to manage the information security of CDR data are:

- **Step 1:** define and implement security governance in relation to CDR data.

²² Loss does not apply to intentional destruction or de-identification of CDR data undertaken in accordance with the CDR Rules.

²³ The CDR Rules currently do not detail steps for how designated gateways must comply with Privacy Safeguard 12.

²⁴ CDR Rules, clause 2.2 of Schedule 1.

- **Step 2:** define the boundaries of the CDR data environment.²⁵
- **Step 3:** have and maintain an information security capability (including the minimum security controls set out in Part 2 of Schedule 2 to the CDR Rules).
- **Step 4:** implement a formal controls assessment program.
- **Step 5:** manage and report security incidents.

12.24 This section summarises what is required by these steps and provides guidance on how accredited data recipients may implement them.

12.25 The 5 steps are not sequential and do not have to be undertaken in order. They should be understood as the minimum processes, policies and procedures that must be put in place to ensure security of CDR data. As such, these steps may occur in parallel and may be repeated iteratively as required.

Step 1: Define and implement security governance in relation to CDR data

Information security governance framework

12.26 The CDR Rules require an accredited data recipient to establish and maintain a formal governance framework²⁶ for managing information security risks relating to CDR data.

12.27 An accredited data recipient may leverage their existing information security governance structure and extend it to their CDR data environment.²⁷ An accredited data recipient may also utilise existing frameworks, requirements and models in developing their information security governance framework and defining security areas.²⁸

12.28 Complying with an existing framework or model does not, of itself, mean that the entity will be compliant with all information security obligations under Privacy Safeguard 12.

12.29 When deciding whether to adopt, apply or modify a standard information security governance framework or model, an accredited data recipient should ensure that the framework or model:

- is appropriate for CDR data and the CDR sector(s) in which the accredited data recipient is operating
- is current and up to date
- takes into account what internal or external auditing is undertaken, and
- is underpinned by a risk profile comparable to the risk profile of the accredited data recipient's CDR data environment.

²⁵ 'CDR data environment' means the information technology systems used for, and processes that relate to, the management of CDR data: CDR Rules, subclause 1.2 of Schedule 2.

²⁶ A formal governance framework refers to policies, processes, roles and responsibilities required to facilitate the oversight and management of information security.

²⁷ For further information, see the ACCC's Supplementary accreditation guidelines: information security.

²⁸ The ACCC's Supplementary accreditation guidelines: information security provide examples of frameworks, requirements and models that might be used in this regard, namely ISO 27001, NIST CSF, PCI DSS and CPS 234.

12.30 Accredited persons are subject to ongoing reporting and audit requirements set out in the CDR Rules (Schedule 1, Part 2). Further information regarding the reporting requirements is contained within the ACCC's Supplementary accreditation guidelines: information security. Accredited data recipients should ensure that any information security governance framework or model takes these requirements into account.

Privacy tip: An accredited data recipient should consider conducting a security risk assessment (which may be part of a broader risk assessment to identify other risks including data mismanagement and quality) before establishing and maintaining a formal governance framework. This ensures the accredited data recipient is aware of their security risk profile and vulnerabilities so that the formal governance framework matches the privacy risks and is fit for purpose.

Documenting practices and procedures relating to information security and management of CDR data

- 12.31 Accredited data recipients must clearly document their practices and procedures relating to information security and management of CDR data, including the specific responsibilities of senior management.²⁹
- 12.32 Accredited data recipients may choose to document these practices and procedures as part of the information security policy required by the CDR Rules, (see paragraphs 12.36–12.40) or as a separate document.
- 12.33 Senior management will have ultimate responsibility for the management of information security.³⁰ Senior management should implement the necessary practices, procedures, resources and training to allow the accredited data recipient to effectively discharge its responsibilities under the CDR Rules.³¹
- 12.34 An accredited data recipient should establish formal information security governance structures, such as committees and forums, to oversee the security of CDR data.³² These committees or forums should include membership from across key business areas, particularly where the entity's CDR data environment is large or complex, so information security is an integrated component of the accredited data recipient's entire business and not left to the compliance or the information and communications technology area alone.
- 12.35 An accredited data recipient's formal information security governance structures should have clear procedures for oversight and accountability, and clear lines of authority for decisions regarding the security of CDR data.

²⁹ CDR Rules, subclause 1.3(2) of Schedule 2.

³⁰ Senior management, of an accredited data recipient that is a body corporate, means: (a) the accredited data recipient's directors; and (b) any person who makes or participates in making decisions that affect the management of CDR data by the accredited data recipient: CDR Rules, clause 1.2 of Schedule 2.

³¹ The ACCC's Supplementary accreditation guidelines: information security.

³² The ACCC's Supplementary accreditation guidelines: information security.

Risk point: Accredited data recipients that view security as a box-ticking exercise or treat it in isolation from broader organisational frameworks can expose CDR data to security risks.

Privacy tip: Accredited data recipients should foster a security-aware culture amongst staff. When establishing procedures for oversight, accountability and lines of authority for decisions regarding CDR security, it is expected that:

- privacy and personal information security steps and strategies are supported by senior management
- senior management should promote a privacy culture that values and protects CDR data and supports the integration of privacy practices, procedures and systems into broader organisational frameworks
- it is clear to staff who holds key security roles, including who is responsible for the overall operational oversight and strategic direction of secure CDR data handling, and
- if there are several areas or teams responsible for information security and privacy, or if the organisation's CDR data environment is large or complex, there should be governance arrangements in place to ensure that key business areas work together (for example, committees and forums).

Information security policy

12.36 An accredited data recipient must have and maintain an information security policy that governs information security across their organisation.³³

12.37 The information security policy must include information about:³⁴

- its information security risk posture (that is, the exposure and potential harm to the entity's information assets, including CDR data, from security threats)
- how the entity plans to address those risks
- the exposure and potential harm from security threats, and
- how its information security practices and procedures and its information security controls, are designed, implemented and operated to mitigate those risks.

12.38 The information security policy should be internally and externally enforceable. Compliance with the policy should also be monitored.³⁵

12.39 An accredited data recipient may choose to address CDR data security in a single policy or across multiple policies (for example, to account for different business areas). While a specific information security policy for CDR data is preferred, it is not required.

³³ CDR Rules, subclause 1.3(3) of Schedule 2.

³⁴ CDR Rules, subclause 1.3(3) of Schedule 2.

³⁵ The term 'enforceable' is defined in the ACCC's Supplementary accreditation guidelines: information security as both internally and externally enforceable, and as including provisions to deal with breaches of the policy. 'Internally' refers to the policy being enforceable against an accredited person's employees and internal departments. 'Externally' refers to the policy, or parts thereof, being enforceable against the accredited person's third parties and vendors through mechanisms such as contractual requirements and ongoing third-party monitoring processes.

12.40 Entities should ensure relevant staff are aware of the information security policy and are trained in their responsibilities. The information security policy should be easily accessible to all relevant staff.

Risk point: Failing to ensure that employees are aware of their information security obligations risks non-compliance with the CDR information security requirements.

Privacy tip: Relevant employees should be aware of, and have access to, the information security policy. The information security policy should include provisions to deal with breaches of the policy by employees and ongoing monitoring of compliance.

Review of appropriateness

12.41 The accredited data recipient must review and update the formal governance framework for appropriateness:

- in response to material changes to both the extent and nature of threats to its CDR data environment and its operating environment, or
- where no such material changes occur — at least annually.³⁶

What is a material change?

A material change is one that significantly changes the CDR data environment, such as the introduction of a new system, the migration of data onto new infrastructure, introduction of a new OSP or CDR representative, or a change to the terms and conditions of the services provided by an existing OSP.³⁷

Step 2: Define the boundaries of the CDR data environment

12.42 An accredited data recipient must assess, define and document its CDR data environment.³⁸ To define and document the CDR data environment, accredited data recipients should identify the people, processes and technology that manage, secure, store or otherwise interact with CDR data. This includes infrastructure, which may be owned and/or managed by an OSP or third-party.³⁹

12.43 Mapping the CDR data environment will ensure an accredited data recipient is fully aware of the CDR data it handles, where the data is kept, who has access to it, and the risks associated with that data before applying security capability controls in Step 3. It will also help to ensure that an accredited data recipient's practices, procedures and systems are up to date.

³⁶ CDR Rules, subclause 1.3(4) of Schedule 2.

³⁷ See the ACCC's Supplementary accreditation guidelines: information security.

³⁸ See the footnote to paragraph 12.23 for the definition of 'CDR data environment'.

³⁹ See the ACCC's Supplementary accreditation guidelines: information security.

Factors to consider as part of the documented CDR data environment analysis

‘CDR data environment’ refers to the systems, technology and processes that relate to the management of CDR data, including CDR data collected by or disclosed to OSPs or CDR representatives. The documented analysis should generally include information about:

People: Who will have access to CDR data? Who will authorise access?

Technology: Such as information systems, storage systems (including whether data is stored overseas, with a cloud service provider, or other third-party), data security systems, authentication systems.

Processes: The entity’s CDR information handling practices, such as how it collects, uses and stores personal information, including whether CDR data handling practices are outsourced to third parties.

Other factors to consider: What other data exists in the data environment, and how does it overlap or connect with the CDR data? This is important to know in order to identify which datasets are high-risk. It is important to identify where non-CDR datasets could be linked with CDR data, increasing the risk of unauthorised disclosure or access.

12.44 This can either be documented through a data flow diagram or a written statement.⁴⁰

12.45 Accredited data recipients need to review their CDR data environment for completeness and accuracy:

- as soon as practicable when they become aware of material changes to the extent and nature of threats to their CDR data environment, or
- where no such material changes occur, at least annually.

Step 3: Have and maintain an information security capability

12.46 The CDR Rules require an accredited data recipient to have and maintain an information security capability that:

- complies with minimum controls set out in Part 2 to Schedule 2 of the CDR Rules, and
- is appropriate and adapted to respond to risks to information security, having regard to:
 - the extent and nature of threats to CDR data that the accredited data recipient holds
 - the extent and nature of CDR data that it holds, and
 - the potential loss or damage to one or more consumers if all, or part, of the consumer’s CDR data were to be misused, interfered with, or accessed, modified or disclosed without authorisation.

⁴⁰ For further information see the ACCC’s Supplementary accreditation guidelines: information security.

12.47 The accredited data recipient must review and adjust its information security capability as required by the CDR Rules (see paragraphs 12.62– 12.63 following).

Information security controls

12.48 The CDR Rules contain information security controls to be designed, implemented and operated by an accredited data recipient as part of its information security capability. These are detailed in Part 2 to Schedule 2 to the CDR Rules.

12.49 These controls cover:

- having processes in place to limit the risk of inappropriate or unauthorised access to its CDR data environment
- taking steps to secure the network and systems within the CDR data environment
- securely managing information assets within the CDR data environment over their lifecycle
- implementing a formal vulnerability management program to identify, track and remediate vulnerabilities within the CDR data environment in a timely manner
- taking steps to limit, prevent, detect and remove malware in the CDR data environment, and
- implementing a formal information security training and awareness program for all personnel interacting with CDR data.

12.50 Compliance with Privacy Safeguard 12 requires the implementation of these controls across the CDR environment.

12.51 The information security controls in Part 2, Schedule 2 of the CDR Rules are the *minimum controls* required for an applicant to become accredited and for an accredited data recipient to ensure ongoing compliance with Privacy Safeguard 12. An accredited data recipient may choose to implement stronger protections.

12.52 Further information regarding the minimum information security controls is contained in the ACCC's Supplementary accreditation guidelines: information security.

Additional security controls required to respond to risks to information security

12.53 In addition to the information security controls set out in Part 2 Schedule 2 of the CDR Rules, an accredited data recipient must also have and maintain an information security capability that is appropriate and adapted to respond to risks to information security, having regard to:

- the extent and nature of threats to CDR data that it holds, and
- the extent and nature of CDR data that it holds, and the potential loss or damage to one or more consumers if all or part of the consumer's data were to be misused, interfered with, or accessed, modified or disclosed without authorisation.

12.54 Accredited data recipients familiar with the Privacy Act may recognise that this is a similar process to determining what constitutes 'reasonable steps' to meet obligations under APP 1.2 and APP 11.

OSP information security capability

12.55 Where an accredited data recipient uses an OSP to:

- collect CDR data on the accredited data recipient's behalf, and/or
- provide the accredited data recipient with goods or services, using CDR data provided by the accredited data recipient,

the accredited data recipient must ensure their contract with the OSP requires them to take the steps outlined in Schedule 2 as if the OSP were an accredited data recipient.⁴¹

12.56 To comply with this requirement, accredited data recipients may consider the following when engaging an OSP:

- assessing whether the information security capabilities of the OSP, having regard to the nature of the goods or services provided in relation to CDR data, comply with the information security capabilities set out in Part 1 of Schedule 2 to the CDR Rules and the security controls set out in Part 2 of Schedule 2 to the CDR Rules
- requesting and reviewing information from the OSP such as vulnerability and penetration testing reports, internal audit reports, and other information security assessments and questionnaires, and
- including contractual provisions regarding security capability reflecting the definition of a CDR outsourcing arrangement in the CDR Rules.⁴²

12.57 Where an accredited data recipient is an OSP chain principal, a failure by a direct or indirect OSP to comply with Schedule 2 in relation to service data is taken to be a failure by that accredited data recipient.⁴³

12.58 Where an accredited data recipient is a CDR representative principal, and they are considering permitting their CDR representative to engage an OSP under CDR representative arrangement,⁴⁴ they should also consider additional terms in the arrangement to ensure their CDR representative considers the above information security capability matters when engaging an OSP.

CDR representative information security capability

12.59 Where an accredited data recipient has a CDR representative, the accredited data recipient (CDR representative principal) must ensure their written contract with the CDR representative (CDR representative arrangement) requires the CDR representative to comply with Privacy Safeguard 12 as if it were the CDR representative principal, and take the steps outlined in Schedule 2 to protect the data as if the CDR representative were the CDR representative principal.⁴⁵

⁴¹ CDR Rules, paragraph 1.10(3)(b)(ii).

⁴² CDR Rules, subrule 1.10(3).

⁴³ CDR Rules, subrule 7.11(2). In this circumstance, the accredited data recipient would also breach subrule 1.16(2) in relation to direct or indirect OSP's failure.

⁴⁴ CDR Rules, paragraph 1.10AA(3)(b).

⁴⁵ CDR Rules, paragraphs 1.10AA(4)(a)(iv) and 1.10AA(4)(b).

12.60 To comply with this requirement, CDR representative principals may consider the following when entering a CDR representative arrangement:

- assessing whether the information security capabilities of the CDR representative, having regard to the nature of the goods or services provided in relation to CDR data, comply with the information security capabilities set out in Part 1 of Schedule 2 to the CDR Rules and the security controls set out in Part 2 of Schedule 2 to the CDR Rules, and
- requesting and reviewing information from the CDR representative such as vulnerability and penetration testing reports, internal audit reports, and other information security assessments and questionnaires.

12.61 A failure by a CDR representative or a direct or indirect OSP of the CDR representative to comply with Schedule 2 in relation to service data is taken to be a failure by the CDR representative principal.⁴⁶

Reviewing security capability

12.62 Under the CDR Rules, an accredited data recipient must review and adjust its information security capability:

- in response to material changes to both the nature and extent of threats and its CDR data environment, or
- where no such material changes occur, at least annually.⁴⁷

12.63 Where changes in the operations of the accredited data recipient could lead to changes in its risk posture (for example, development of new applications, migration to new infrastructure), the accredited data recipient should review its information security capability to ensure it remains fit for purpose in managing information security risks.

Step 4: implement a formal controls assessment program

Assessing the effectiveness of controls

12.64 An accredited data recipient must establish and implement a testing program to review and assess the effectiveness of its information security capability.

12.65 This testing program must be appropriate and adapted to respond to risks to information security, having regard to:

- the extent and nature of threats to CDR data that it holds
- the extent and nature of CDR data that it holds, and

⁴⁶ CDR Rules, subrule 7.11(3). In this circumstance, a CDR representative principal would also breach subrule 1.16A(2) in relation to a CDR representative's failure, and subrule 1.16(4) in relation to failure of a direct or indirect OSP of a CDR representative.

⁴⁷ CDR Rules, subclause 1.5(2) of Schedule 2.

- the potential loss or damage to one or more consumers if all or part of the consumer's data were to be misused, interfered with or lost, or accessed, modified or disclosed without authorisation.⁴⁸

12.66 The extent and frequency of this testing must be commensurate with:

- the rate at which vulnerabilities and threats change
- material changes to the accredited data recipient's CDR data environment, and
- the likelihood of failure of controls having regard to the results of previous testing.⁴⁹

12.67 In order to maintain accreditation under the CDR framework, accredited persons who do not have streamlined accreditation must also provide regular attestation statements and assurance reports to the Data Recipient Accreditor.⁵⁰ More information can be found in the ACCC's Supplementary accreditation guidelines: information security.

12.68 The accredited data recipient must monitor and evaluate the design, implementation and operating effectiveness of security controls relating to the management of CDR data and have regard to its CDR system obligations and the control requirements in Part 2 of Schedule 2 to the CDR Rules.⁵¹

12.69 The accredited data recipient must escalate and report the results of any testing that identifies design, implementation or operational deficiencies in information security controls relevant to its CDR data environment to senior management.⁵²

12.70 The accredited data recipient must ensure that testing is conducted by appropriately skilled persons who are independent from the performance of controls over the CDR data environment.⁵³

12.71 The accredited data recipient must review the sufficiency of its testing program:

- a. when there is a material change to the nature and extent of threats to its CDR data environment or to the boundaries of its CDR data environment, as soon as practicable, or
- b. where no such material changes occur, at least annually.⁵⁴

Step 5: Manage and report security incidents

12.72 An accredited data recipient must have procedures and practices in place to detect, record, and respond to information security incidents as soon as practicable.⁵⁵ More detail about

⁴⁸ CDR Rules, paragraph 1.6(1)(a) of Schedule 2.

⁴⁹ CDR Rules, paragraph 1.6(1)(b) of Schedule 2.

⁵⁰ CDR Rules, subclauses 2.1(2) and (3) of Schedule 1. Accredited persons who have streamlined accreditation under rule 5.5 are not required to follow clause 2.1 of Schedule 1 to the CDR Rules: CDR Rules, subclause 2.1(1A) of Schedule 1. In the banking sector, streamlined accreditation is available where the accreditation applicant is an ADI that is not a restricted ADI: CDR Rules, subrule 5.5(b) and rule 1.7, Clause 7.3 of Schedule 3.

⁵¹ CDR Rules, subclause 1.6(2) of Schedule 2.

⁵² CDR Rules, subclause 1.6(3) of Schedule 2.

⁵³ CDR Rules, subclause 1.6(4) of Schedule 2.

⁵⁴ CDR Rules, subclause 1.6(5) of Schedule 2.

⁵⁵ CDR Rules, subclause 1.7(1) of Schedule 2.

maintaining these practices can be found in the ACCC's Supplementary accreditation guidelines: information security.

12.73 The accredited data recipient must create and maintain plans to respond to information security incidents that could plausibly occur. These are known as CDR data security response plans.⁵⁶

12.74 The accredited data recipient's CDR data security response plans must include procedures for:

- a. managing all relevant stages of an incident, from detection to post-incident review
- b. notifying CDR data security breaches to the Information Commissioner and to consumers as required under Part IIIC of the Privacy Act,⁵⁷ and
- c. notifying information security incidents to the Australian Cyber Security Centre as soon as practicable and no later than 30 days after the accredited data recipient becomes aware of the security incident.⁵⁸

12.75 The accredited data recipient must review and test its CDR data security response plans to ensure they remain resilient, effective and consistent with its obligations in relation to CDR data security breaches.

- Where there is a material change to the nature and extent of threats to the accredited data recipient's CDR data environment or to the boundaries of the accredited data recipient's CDR data environment, this review and test must be undertaken as soon as practicable.
- Where no such material changes occur, this review and test must be undertaken at least annually.⁵⁹

Additional conditions on sponsors to ensure CDR data is secure

12.76 Where an accredited person proposes to become the sponsor of a person that has applied, or proposes to apply, for sponsored accreditation (the affiliate), they must have a third-party management framework in place to ensure the affiliate maintains appropriate information security capabilities.⁶⁰

12.77 This management framework must include requirements and activities relating to information security, including:

- due diligence prior to establishing new relationships or contracts
- annual review and assurance activities, and
- reporting requirements.

⁵⁶ CDR Rules, subclause 1.7(2) of Schedule 2.

⁵⁷ See the 'Notifiable Data Breach (NDB) scheme' section further below in this Chapter.

⁵⁸ CDR Rules, subclause 1.7(3) of Schedule 2.

⁵⁹ CDR Rules, subclause 1.7(4) of Schedule 2.

⁶⁰ CDR Rules, clause 2.2 of Schedule 1.

12.78 A sponsor must also provide the affiliate with appropriate assistance or training in relation to the steps and obligations outlined in Schedule 2 of the CDR Rules to protect the CDR data.

12.79 The sponsor of the affiliate must:

- maintain the management framework and manage its relationship with the affiliate in accordance with this framework
- provide ongoing assistance and training on technical and compliance matters, and
- take reasonable steps to ensure the affiliate complies with its obligations under Schedule 2 of the CDR Rules.

Notifiable Data Breach (NDB) scheme

12.80 The Notifiable Data Breaches (NDB) provisions in Part IIIC of the Privacy Act apply to accredited data recipients as if personal information was ‘CDR data’.⁶¹

12.81 Under the NDB scheme, accredited data recipients are required to notify affected consumers and the Information Commissioner in the event of an ‘eligible data breach’ under the NDB scheme.⁶²

12.82 A data breach is eligible if it is likely to result in serious harm to any of the consumers to whom the information relates. Entities must conduct a prompt and reasonable assessment if they suspect that they may have experienced an eligible data breach.

12.83 For more information, see the OAIC’s [Notifiable Data Breaches scheme webpage](#).

The OAIC has developed the [Data breach preparation and response guide — A guide to managing data breaches in accordance with the Privacy Act](#) to support the development and implementation of an effective data breach response, including developing a data breach response plan. The principles and concepts from this guide are useful and applicable to CDR data security breaches.⁶³

⁶¹ Competition and Consumer Act, section 56ES.

⁶² See Part IIIC, Division 3 of the Privacy Act. See generally the OAIC’s [Notifiable Data Breaches scheme webpage](#) for further information.

⁶³ The notifiable data breaches provisions of the Privacy Act apply in the CDR system as if personal information was ‘CDR data’ (see Competition and Consumer Act, section 56ES).

PART B: Treatment of redundant data (destruction and de-identification)

Overview of the process for treating redundant data

- 12.84 An accredited data recipient or a designated gateway must destroy or de-identify CDR data that has become ‘redundant’ unless an exception applies.⁶⁴ Information regarding when CDR data becomes ‘redundant’, as well as the exceptions to the requirement to destroy or de-identify redundant data, are discussed below at ‘What is ‘redundant data?’’ and outlined in the flow chart beneath paragraph 12.87.
- 12.85 Once CDR data is redundant, the steps an entity must take to determine whether to destroy or de-identify the CDR data are set out in the CDR Rules and explained under the heading ‘Deciding how to deal with redundant data’ below. What an accredited data recipient told the consumer during the consent phase (about how they treat redundant data) and whether the consumer has made an election to delete will be relevant to this decision, as demonstrated by the flow chart below at paragraph 12.94.
- 12.86 Once the accredited data recipient has determined whether to destroy or de-identify (and provided a consumer has not made an election to delete), it must follow the specific destruction and de-identification processes set out in the CDR Rules and outlined under the headings ‘Steps to destroy redundant data’ and ‘Steps to de-identify redundant data’ below.⁶⁵
- 12.87 Where the de-identification process does not apply or cannot result in de-identified information in accordance with the CDR Rules, the destruction process must be followed as outlined under the heading ‘Steps to destroy redundant data’ below.

⁶⁴ See Competition and Consumer Act, subsection 56EO(2)(a).

⁶⁵ Designated gateways must also take the steps specified in the CDR Rules to destroy or de-identify the redundant data: subsection 56EO(2). However, there are no designated gateways in the banking sector or energy sector. See [Chapter B \(Key concepts\)](#) for the meaning of designated gateway.

Redundant data in the CDR regime

Whether CDR data is redundant

Do you need the CDR data for:

- a purpose permitted under the CDR Rules
- or
- a purpose for which you can use or disclose under the privacy safeguards?

No



Does an exception apply that allows you to keep the redundant data?

- Are you required to retain the redundant data by or under a law or court or tribunal order
- or
- Does the redundant data relate to any current or anticipated legal or dispute resolution proceedings to which you or the consumer are a party?

Yes



You are permitted to retain the redundant data, and must continue to handle the redundant data in accordance with the privacy safeguards (including by continuing to take the steps specified in the CDR Rules to protect the redundant data).

Yes



The CDR data is not redundant data. Continue to handle the CDR data in accordance with the privacy safeguards.

No



You must delete or de-identify the redundant data in accordance with the CDR Rules.



See the flowchart on deleting or de-identifying redundant data.

What is ‘redundant data’?

12.88 ‘Redundant data’ is CDR data that an accredited data recipient or designated gateway no longer needs for a purpose permitted under the CDR Rules, or for any purpose for which it is allowed to be used or disclosed under the privacy safeguards.⁶⁶

12.89 While the expiry of a consent will automatically cause CDR data to become redundant, there are other situations where CDR data will become redundant. For example, when an accredited data recipient’s accreditation is revoked or surrendered.⁶⁷

12.90 The terms ‘purpose’ (in the context of redundant data) and ‘required by or under an Australian law or court/tribunal order’ are discussed in more detail in Chapter B (Key concepts).

12.91 Privacy Safeguard 12 requires an accredited data recipient or designated gateway to take the steps in the CDR Rules to destroy or de-identify redundant data unless:⁶⁸

- the entity is required to retain the data by or under an Australian law or a court/tribunal order, or
- the data relates to any current or anticipated legal proceedings or dispute resolution proceedings to which the entity or the consumer is a party.⁶⁹

12.92 An accredited data recipient may request that the consumer state whether a legal or dispute resolution proceeding to which the consumer is a party is current or anticipated, and may rely on such a statement made by the consumer.⁷⁰

12.93 A legal or dispute resolution proceeding is ‘anticipated’ if there is a real prospect of proceedings being commenced, as distinct from a mere possibility. A dispute resolution proceeding includes those undertaken through external dispute resolution schemes.

12.94 Within a dataset, some of the data may become redundant while other data does not. For instance, where a consumer has a number of banking accounts with a particular data holder, and data associated with one of those accounts is no longer needed by the accredited data recipient to provide the consumer with the requested services, that account data will become redundant data.

Risk point: Where an exception applies, entities risk keeping redundant data longer than they need to.

Privacy tip: Where, for example, laws prevent de-identification or destruction of redundant data, the entity should adopt other measures to limit privacy risks such as archiving and limiting access to those CDR data holdings. Entities should also clearly specify the law that authorises or requires the retention, how long the authorisation lasts, and the degree of information needed.

⁶⁶ See Competition and Consumer Act, subsection 56EO(2)(a).

⁶⁷ CDR Rules, subrule 5.23(4).

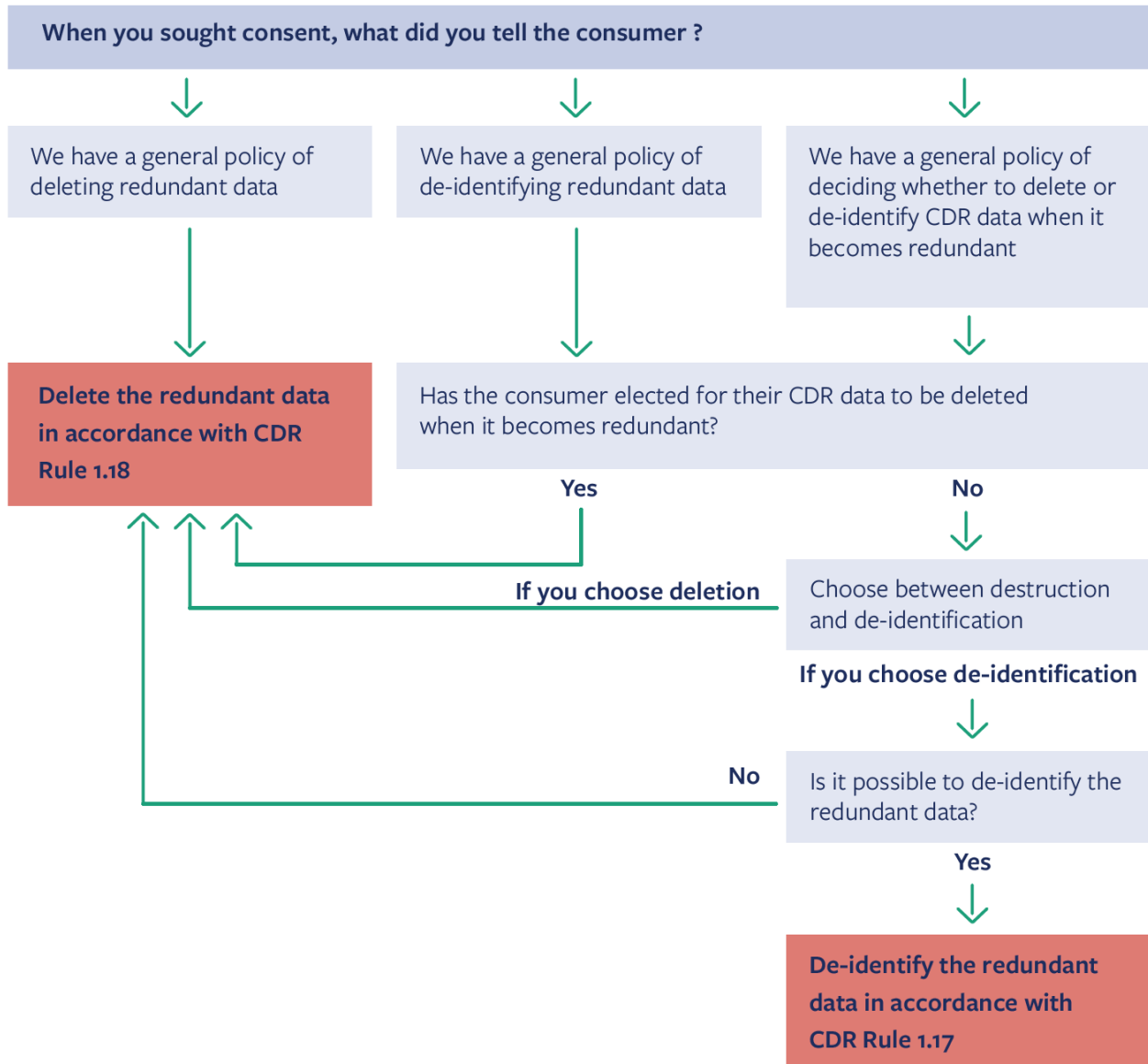
⁶⁸ See Competition and Consumer Act, subsection 56EO(2).

⁶⁹ See Competition and Consumer Act, 56BAA and CDR Rules, rule 1.17A.

⁷⁰ CDR Rules, paragraphs 1.17(A)(2) – (3).

Deciding how to deal with redundant data

Deleting or de-identifying redundant data



Step 1: Notification to consumer of matters relating to redundant data

General policy for dealing with redundant data

12.95 When seeking consent from a consumer in relation to the handling of their CDR data,⁷¹ an accredited person must advise the consumer whether they have a general policy of:

- deleting the redundant data
- de-identifying the redundant data, or
- deciding whether to delete or de-identify the CDR data at the time it becomes redundant data.⁷²

The consumer's right to elect for their redundant data to be deleted

12.96 If an accredited person's general policy is either de-identification or deciding between deletion and de-identification when the CDR data becomes redundant, then the accredited data recipient must allow the consumer to elect for their redundant data to be deleted.

12.97 A consumer can elect at any time for their data to be deleted when redundant. The deletion request applies to CDR data and any data derived from it (to the extent that the relevant consumer is identifiable or reasonably identifiable from the derived data).⁷³

12.98 See Chapter B (Key Concepts) for further guidance about the meaning of 'derived data'.

Step 2: Consider whether the redundant data must be destroyed

12.99 In many cases, an accredited data recipient will not have the option to de-identify under the CDR Rules, and the CDR data must be destroyed.

12.100 An accredited data recipient must consider whether an exception to the requirement to destroy redundant data set out above at 'What is 'redundant data'?' applies to the redundant data. If an exception applies, the accredited data recipient must retain the CDR data while the exception applies.⁷⁴

12.101 The CDR Rules require redundant data to be destroyed where:

- the consumer has elected for their redundant data to be deleted
- if no election has been made, the accredited data recipient advised the consumer at the time of seeking consent that it had a general policy of deleting redundant data. Where an accredited data recipient advised the consumer of a general policy of destruction, the accredited data recipient **must destroy the redundant data**, even if their general policy has since changed, or
- it is not possible to de-identify the CDR data to the required extent (see Step 5).

⁷¹ CDR Rules, paragraph 4.11(3)(h)(i).

⁷² CDR Rules, subrule 4.17(1).

⁷³ CDR Rules, rule 4.16. See also 'reasonably identifiable' in [Chapter B \(Key concepts\)](#).

⁷⁴ CDR Rules, subrule 1.17A(2).

Step 3: If destruction isn't required, choose between destruction and de-identification

12.102 If there is no 'election to delete' in place, and the entity did not advise the consumer that it has a general approach of deleting redundant data, then the entity **can decide between destroying or de-identifying the CDR data** using the steps and processes contained in the CDR Rules and outlined below.

Step 4: Destroying redundant data

12.103 If the accredited data recipient chooses under Step 3 to destroy the redundant data, then they must proceed to destroy the data in accordance with the 'CDR data deletion process' set out in the CDR Rules.⁷⁵ This process is explained further below under the heading 'Steps to destroy redundant data'.

Step 5: De-identifying redundant data

Consider whether it is possible to de-identify the CDR data

12.104 Once an accredited data recipient has determined the de-identification process could apply, and the accredited data recipient is interested in pursuing this option, it must consider whether the CDR de-identification process will ensure that the data is de-identified in accordance with the CDR Rules.

12.105 In making this decision, an accredited data recipient must consider:

- OAIC and Data61's De-Identification Decision-Making Framework
- the techniques that are available for de-identification of data
- the extent to which it would be technically possible for **any person** to be re-identified, or be reasonably identifiable, after de-identification in accordance with such techniques, and
- the likelihood of any person becoming identifiable, or reasonably identifiable from the data after de-identification.⁷⁶

12.106 Based on the above considerations, the accredited data recipient must determine whether it would be possible to de-identify the relevant data so that no person would any longer be identifiable, or reasonably identifiable, from:

- the relevant data after the proposed de-identification, and
- other information that would be held, following the proposed de-identification, by any person (the 'required extent').

12.107 The accredited data recipient must take into account the possibility of re-identification by using other information that may be held by **any person**. That is, whether the CDR data would be suitable for an open release environment (regardless of whether data is in fact

⁷⁵ CDR Rules, rule 1.18

⁷⁶ CDR Rules, subrule 1.17(1).

released into an open environment, or what controls and safeguards apply to the data access environment).⁷⁷

12.108 This is equivalent to using the De-Identification Decision-Making Framework to determine de-identification practices for open release. That is, accredited data recipients must use the De-Identification Decision-Making Framework as they would when intending to openly release de-identified information.

12.109 De-identification will be possible only where CDR data has been through an extremely robust de-identification process that ensures, with a very high degree of confidence, that no persons are reasonably identifiable.

12.110 Accredited data recipients should be aware that there is significant complexity and risk involved with attempting to de-identify unit record data derived from CDR data to the ‘required extent’ as defined in the CDR Rules.

De-identifying redundant data (if de-identification is possible)

12.111 If, having taken the steps outlined in this section, the accredited data recipient determines that it is possible to de-identify the redundant data to the required extent⁷⁸, they can then proceed to de-identify the data in accordance with the ‘CDR data de-identification process’ set out in the CDR Rules.⁷⁹ This process is explained further below under ‘Steps to de-identify redundant data’.

Destroying redundant data (if de-identification is not possible)

12.112 If, having taken the steps outlined above, the accredited data recipient determines it is not possible to de-identify the data to the required extent, the accredited data recipient must delete the CDR data and any derived data in accordance with the CDR data deletion process set out in the CDR Rules, and explained below under ‘Steps to destroy redundant data’.⁸⁰

Steps to destroy redundant data

12.113 The CDR Rules provide that the CDR data deletion process is to be applied for the purposes of destroying redundant data under Privacy Safeguard 12.⁸¹ The CDR data deletion process is set out in rule 1.18 in the CDR Rules.

12.114 Rule 1.18 in the CDR Rules provides that CDR data is to be deleted using the following steps:

- delete, to the extent reasonably practicable, CDR data and any copies of that data
- make a record to evidence the deletion, and

⁷⁷ CDR Rules, paragraph 1.17(2)(f).

⁷⁸ See paragraphs 12.102 to 12.110.

⁷⁹ CDR Rules, rule 1.17.

⁸⁰ CDR Rules, subrule 1.17(4).

⁸¹ CDR Rules, rule 7.13.

- where another person holds the CDR data on behalf of an accredited data recipient and will perform the steps above (for example, an OSP), that accredited data recipient must direct that person to notify it when the steps are complete.

12.115 This process applies:

- to the deletion of CDR data in response to a consumer's election
- where the entity otherwise chooses to delete the redundant data in order to comply with their Privacy Safeguard 12 obligations, and
- where it is not possible to de-identify the CDR data to the required extent (see Step 5 above).

Deleting the CDR data 'to the extent reasonably practicable'

12.116 The CDR data deletion process requires the accredited data recipient to delete, 'to the extent reasonably practicable', CDR data and any copies of that CDR data.⁸²

12.117 The meaning of deleting data 'to the extent reasonably practicable' depends on the circumstances, including:

- **the amount of CDR data** — more rigorous steps may be required as the quantity of data increases
- **the nature of the accredited data recipient**, and of any other entities to whom the CDR data has been disclosed (such as OSPs) — relevant considerations include an accredited data recipient's size, resources and its business model
- the **possible adverse consequences for a consumer** if their CDR data is not properly deleted — more rigorous steps may be required as the risk of adversity increases
- the accredited data recipient's **information handling practices** — such as how it collects, uses and stores personal information, including whether CDR data handling practices are outsourced to third parties, and
- the **practicability, including time and cost involved** — however an accredited data recipient is not excused from deleting CDR data by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take a particular step will depend on whether the burden is excessive in all the circumstances.

What if CDR data cannot practically be deleted?

12.118 The CDR Rules recognise that irretrievable destruction of CDR data such as from a back-up system or a database more generally is not always straightforward,⁸³ and it may not be possible to achieve this immediately (for example, archived data that could be re-installed).

⁸² CDR Rules, subrule 1.18(a).

⁸³ See the CDR data deletion process in subrule 1.18(a) of the CDR Rules, which requires entities to delete CDR data and any copies 'to the extent reasonably practicable'.

12.119 For this reason, CDR data can be put ‘beyond use’, if it is not actually destroyed, provided the accredited data recipient:

- is not able, and will not attempt, to use or disclose the CDR data
- cannot give any other entity access to the CDR data
- surrounds the CDR data with appropriate technical, physical and organisational security, and⁸⁴
- commits to take reasonable steps to irretrievably destroy the data if, or when, this becomes possible.

12.120 It is important to note that the accredited data recipient must continue to take reasonable steps to work towards a solution to eventually delete the CDR data.

Privacy tip: If a consumer requests deletion of their redundant data but the accredited data recipient determines that it is required to retain the data under a relevant Australian law, court/tribunal order, or because of legal or dispute resolution proceedings, the entity should notify the consumer in writing of the reasons that their request was not complied with.

Steps to de-identify redundant data

12.121 If the accredited data recipient determines that it is possible to de-identify the data to the required extent, it must determine and apply the appropriate de-identification technique (or techniques).⁸⁵

12.122 Specifically, the accredited data recipient must:

- determine the technique/s appropriate in the circumstances
- apply that technique/s to de-identify the relevant data to the required extent, and
- delete, in accordance with the CDR data deletion process, any CDR data that must be deleted to ensure that no person is any longer identifiable or reasonably identifiable.⁸⁶

12.123 As soon as practicable after undertaking the de-identification process, the accredited data recipient must record the process including:

- details of the assessment that it is possible to de-identify the relevant data to the required extent
- that the relevant data was de-identified to that extent
- how the relevant data was de-identified, including specifying the technique that was used, and

⁸⁴ This should go beyond the minimum access controls specified in the CDR Rules.

⁸⁵ CDR Rules, subrule 1.17(3). This determination is a point in time assessment, i.e. with the technology available at that time rather than technology that may become available (such as quantum computing, for instance) in the future.

⁸⁶ CDR Rules, subrule 1.17(3).

- any persons to whom the de-identified data is disclosed.⁸⁷

12.124 If the accredited data recipient determines that it is not possible to de-identify CDR data using the appropriate technique, it must delete the relevant data and any CDR data directly or indirectly derived from it.

De-identifying data that has been provided to an OSP or CDR representative

12.125 Where an accredited data recipient has provided an OSP or CDR representative with CDR data that then becomes redundant, the accredited data recipient cannot rely on that OSP or CDR representative to undertake the de-identification process on their behalf.⁸⁸

12.126 In this situation, an accredited data recipient must direct any of its direct OSPs or CDR representatives that have been provided with a copy of the redundant data to delete the redundant data, as well as any data directly or indirectly derived from it and notify the accredited data recipient of the deletion.⁸⁹

12.127 If the direct OSP or CDR representative has provided the redundant data to its own direct OSP (the further recipient), the accredited data recipient must also direct its direct OSP or CDR representative to direct the further recipient to both delete the redundant data (as well as any data directly or indirectly derived from it)⁹⁰ and notify the accredited data recipient of the deletion.

12.128 The accredited data recipient is responsible for ensuring these directions are made, and for ensuring the data is deleted.⁹¹

12.129 Where an accredited data recipient is a CDR representative principal, a failure by the CDR representative to handle redundant data in accordance with Privacy Safeguard 12⁹² is taken to be a failure by the CDR representative principal.⁹³

Other relevant security obligations

Privacy safeguards

12.130 Compliance with the privacy safeguards as a whole will promote security and reduce the risk of CDR data being accidentally or deliberately compromised. This is because the privacy

⁸⁷ CDR Rules, paragraph 1.17(3)(d).

⁸⁸ For information about the meaning of OSP and CDR representative principal, see Chapter B (Key concepts).

⁸⁹ CDR Rules, paragraph 7.12(2)(b)(i). ⁹⁰ CDR Rules, paragraph 7.12(2)(b)(ii).

⁹⁰ CDR Rules, paragraph 7.12(2)(b)(ii).

⁹¹ The OSP or CDR representative is required to comply with this direction – see CDR Rules, rules 1.10 and 1.16, and 1.10AA and 1.16A.⁹² Subsection 56EO(2) of the Act (applied as if the CDR representative were an accredited data recipient and references in subrule 7.12(1) to Division 4.3 were to Division 4.3A).

⁹² Subsection 56EO(2) of the Act (applied as if the CDR representative were an accredited data recipient and references in subrule 7.12(1) to Division 4.3 were to Division 4.3A).

⁹³ CDR Rules, subrule 7.12(3).

safeguards ensure that privacy risks are reduced or removed at each stage of CDR data handling, including collection, storage, use, disclosure, and destruction of CDR data.

- 12.131 Privacy Safeguard 1 requires entities to take reasonable steps to establish and maintain practices, procedures, and systems to ensure compliance with the privacy safeguards, including Privacy Safeguard 12. Privacy Safeguard 1 also requires that certain information about the deletion and de-identification of redundant data must be provided in an accredited data recipient's CDR Policy (see [Chapter 1 \(Privacy Safeguard 1\)](#)).
- 12.132 Privacy Safeguard 3 limits the collection of CDR data, which is an effective risk management practice reducing the scope of data that may be accessed in the case of a cyber-attack (see [Chapter 3 \(Privacy Safeguard 3\)](#)).
- 12.133 Privacy Safeguard 4 contains requirements to destroy information if it is unsolicited and not required to be retained by the entity (see [Chapter 4 \(Privacy Safeguard 4\)](#)). This minimises the amount of data held by an entity and the amount of time the entity holds that information, reducing overall risk of data breach.

Other CDR de-identification processes

- 12.134 There are separate requirements under the CDR Rules to follow when de-identifying CDR data that is not 'redundant data'.⁹⁴
- 12.135 For example, an accredited person must seek a consent from the consumer to:
- use the de-identified data for general research,⁹⁵ and/or
 - disclose (including by selling) the de-identified data.
- 12.136 For further information on seeking consent to use de-identified CDR data that is not redundant data, see [Chapter C \(Consent\)](#).

⁹⁴ CDR Rules, paragraph 7.5(1)(b).

⁹⁵ 'General research' is defined in rule 1.7 in the CDR Rules to mean research undertaken by an accredited data recipient with CDR data de-identified in accordance with the CDR Rules that does not relate to the provision of goods or services to any particular CDR consumer.

Chapter 13:

Privacy Safeguard 13 —

Correction of CDR data

Version 5.0, November 2023



Contents

Key points	3
What does Privacy Safeguard 13 say?	3
Why is it important?	4
Who does Privacy Safeguard 13 apply to?	4
How Privacy Safeguard 13 interacts with the Privacy Act	5
When must an entity correct CDR data?	6
Acknowledging receipt of correction requests	7
Actioning and responding to correction requests (for CDR data that is not AEMO data)	7
Taking action to correct, or qualify, the CDR data	7
When action is not necessary in response to a request	8
How must a correction notice be provided to consumers?	10
What must be included in a correction notice to consumers?	11
Actioning and responding to correction requests (for AEMO data)	11
What are the correction considerations?	12
Accurate	13
Up to date	13
Complete	14
Not misleading	14
Charges to correct CDR data	14
Interaction with other privacy safeguards	15
Privacy Safeguard 5	15
Privacy Safeguard 10	15
Privacy Safeguard 11	15
Privacy Safeguard 12	15

Key points

Privacy Safeguard 13,¹ together with the consumer data rules (CDR Rules) and the Competition and Consumer Regulations, sets out obligations for data holders and accredited data recipients of CDR data in relation to correction requests made by CDR consumers in respect of their CDR data.

Privacy Safeguard 13 does not apply to the Australian Energy Market Operator Limited (AEMO) in its capacity as a data holder.² Accordingly, unless otherwise indicated, all references in this Chapter to data holders exclude AEMO.

What does Privacy Safeguard 13 say?

13.1 Privacy Safeguard 13 requires data holders and accredited data recipients who:

- receive a request from the consumer to correct their CDR data, and
- in the case of data holders, were earlier required or authorised under the CDR Rules to disclose the CDR data

to respond to the request by taking the relevant steps set out in the CDR Rules.

13.2 Rule 7.14 of the CDR Rules prohibits data holders and accredited data recipients from charging a fee for responding to or actioning a correction request.

Privacy Safeguard 13 obligations in respect of CDR data that is not AEMO data

13.3 For CDR data that is not AEMO data, rule 7.15 of the CDR Rules requires an entity to acknowledge receipt of a correction request as soon as practicable and sets out how the entity must, within 10 business days after receipt of the request, and to the extent it considers appropriate:

- correct the CDR data, or
- both:
 - include a statement with the CDR data to ensure that, having regard to the purpose for which the CDR data is held, it is accurate, up to date, complete and not misleading (qualifying statement), and
 - where practicable, attaching an electronic link to a digital record of the data in such a way that the statement will be apparent to any users of the data.

13.4 The entity must also give the consumer a notice, via electronic means, setting out how they responded to the correction request, why a correction or qualifying statement is unnecessary or inappropriate if no changes were made, and the complaint mechanisms available to the consumer.

¹ Competition and Consumer Act, section 56EP.

² Competition and Consumer Regulations, paragraph 28RA(2)(a)(iii). For information about how Privacy Safeguard 13 applies to retailers who receive CDR data from AEMO, see paragraph 13.5 to 13.6.

Privacy Safeguard 13 obligations in respect of AEMO data

- 13.5 Privacy Safeguard 13 does not apply to AEMO.³ However, it does apply (with modifications) to retailers in the energy sector, in relation to CDR data held by AEMO that AEMO has disclosed to the retailer as required by the *Competition and Consumer Act 2010* (Competition and Consumer Act).⁴ Retailers must also comply with Privacy Safeguard 13 in respect of their own CDR data holdings.⁵
- 13.6 Clause 6.1 of Schedule 4 to the CDR Rules requires a retailer to acknowledge receipt of a correction request that relates to AEMO data as soon as practicable and:
- if the request relates to NMI (national metering identifier) standing data or metering data, to initiate the relevant correction procedures under the National Electricity Rules, or
 - if the request relates to DER (distributed energy resource) register data, to provide the consumer with information about how they can contact the distributor to have the data corrected.

Why is it important?

- 13.7 The objective of Privacy Safeguard 13 is to ensure consumers have trust in and control over the accuracy of their CDR data that is disclosed and used as part of the CDR system.
- 13.8 For CDR data that is not AEMO data, Privacy Safeguard 13 does this by ensuring entities are required to correct CDR data in certain circumstances when requested to do so by the consumer. For AEMO data a retailer was earlier required or authorised to disclose under the CDR Rules, Privacy Safeguard 13 does this by requiring the retailer to initiate relevant correction procedures under the National Electricity Rules (in respect of NMI standing data or metering data) or provide the consumer with information about how they can contact the distributor to have their data corrected (in respect of DER register data).
- 13.9 This allows consumers to realise the benefits of the CDR system, such as receiving competitive offers from other service providers, as the accuracy of the data made available to sector participants can be relied upon.

Who does Privacy Safeguard 13 apply to?

- 13.10 Privacy Safeguard 13 applies to data holders and accredited data recipients of CDR data. It does not apply to designated gateways or AEMO.⁶
- 13.11 Importantly, in relation to data holders, Privacy Safeguard 13 only applies where a consumer has requested that a data holder correct their CDR data and the data holder was earlier required or authorised to disclose it under the CDR Rules.⁷ APP 13 will continue to apply to

³ Competition and Consumer Regulations, paragraph 28RA(2)(a)(iii).

⁴ Competition and Consumer Regulations, sub-regulation 28RA(4).

⁵ See paragraphs 13.3 to 13.4 on Privacy Safeguard 13 obligations in respect of CDR data that is not AEMO data.

⁶ Although Privacy Safeguard 13 does not apply to AEMO, it does apply (with modifications) to retailers in the energy sector for requests that relate to AEMO data: see paragraphs 13.5 to 13.6.

⁷ Competition and Consumer Act, subsection 56EP(1).

CDR data that is personal information in all other circumstances. For example, where a consumer makes a correction request, but the CDR data has not previously been disclosed by the data holder under the CDR Rules, APP 13 will apply.

- 13.12 As a non-accredited entity, a CDR representative is not directly bound by Privacy Safeguard 13. However, under the terms of the CDR representative arrangement with their CDR representative principal,⁸ a CDR representative is required to comply with Privacy Safeguard 13 in its handling of service data as if it were the CDR representative principal.^{9,10} A CDR representative principal breaches subrule 7.16(1) of the CDR Rules if its CDR representative fails to comply with Privacy Safeguard 13 (subsection 56EP(2) of the Competition and Consumer Act) as if it were an accredited person (regardless of whether the CDR representative's actions accord with the CDR representative arrangement).¹¹

How Privacy Safeguard 13 interacts with the Privacy Act

- 13.13 It is important to understand how Privacy Safeguard 13 interacts with the *Privacy Act 1988* (the Privacy Act) and the APPs.¹²

- 13.14 APP 13 requires an APP entity to correct personal information held by the entity in certain circumstances.

CDR entity	Privacy protections that apply in the CDR context
Accredited data recipient	<p>Privacy Safeguard 13</p> <p>For an accredited data recipient of a consumer's CDR data, Privacy Safeguard 13 applies to the correction of that CDR data.¹³</p> <p>The APPs do not apply to accredited data recipients in relation to that CDR data.¹⁴</p>

⁸ A CDR representative arrangement is a written contract between a person with unrestricted accreditation (the CDR representative principal) and a person without accreditation (the CDR representative) that meets the minimum requirements listed in subrules 1.10AA(1), (3) and (4) of the CDR Rules.

⁹ CDR Rule, paragraph 1.10AA(4)(a)(v).

¹⁰ See [Chapter B \(Key concepts\)](#) for more information on 'CDR representative principal', 'CDR representative', 'CDR representative arrangement' and 'service data'.

¹¹ CDR Rules, rule 7.16. See also rule 1.16A in relation to a CDR representative principal's obligations and liability.

¹² The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies (APP entities).

¹³ Privacy Safeguard 13 applies from the point when the accredited person becomes an accredited data recipient of the CDR data. An accredited person becomes an accredited data recipient for CDR data when:

- CDR data is held by (or on behalf of) the person
- the CDR data, or any other CDR data from which it was directly or indirectly derived, was disclosed to the person under the consumer data rules, and
- the person is neither a data holder, nor a designated gateway, for the first mentioned CDR data. See Competition and Consumer Act, section 56AK.

¹⁴ The APPs do not apply to an accredited data recipient of CDR data, in relation to that CDR data: Competition and Consumer Act, paragraph 56EC(4)(a). However, subsection 56EC(4) does not affect how the APPs apply to accredited

CDR entity	Privacy protections that apply in the CDR context
Data holder (other than AEMO)	<p>Privacy Safeguard 13 or APP 13</p> <p>Privacy Safeguard 13 applies instead of APP 13 where a consumer has requested that a data holder correct their CDR data, and the data holder was earlier required or authorised to disclose it under the CDR Rules.</p> <p>APP 13 continues to apply to CDR data that is personal information in all other circumstances. This includes where:</p> <ul style="list-style-type: none"> the consumer makes a correction request, but the data has not previously been disclosed by the data holder under the CDR Rules, or the consumer has not made a correction request, but the APP entity is satisfied that the data it holds is incorrect.¹⁵
Data holder (AEMO)	<p>APP 13</p> <p>Privacy Safeguard 13 does not apply to AEMO as a data holder.</p>
Designated gateway	<p>APP 13</p> <p>Privacy Safeguard 13 does not apply to designated gateways.</p>

When must an entity correct CDR data?

13.15 Privacy Safeguard 13 and rule 7.15 of the CDR Rules require an entity to correct or include a qualifying statement with CDR data (other than AEMO data) within 10 business days after the CDR consumer has requested their CDR data be corrected, unless the entity does not consider a correction or qualifying statement to be appropriate.¹⁶

13.16 Different obligations apply for entities that receive a correction request relating to AEMO data. A retailer will not be required to correct AEMO data but will instead be required to:

- for NMI standing data or metering data - initiate relevant correction procedures under the National Electricity Rules, or
- for DER register data - provide the requester with information about how the requester can contact the distributor to have the data corrected.

persons and accredited data recipients who are APP entities, in relation to the handling of personal information outside the CDR system. (Note: Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data: see Privacy Act, subsection 6E(1D).) Subsection 56EC(4) of the Competition and Consumer Act also does not affect how the APPs apply to an accredited person who does not become an accredited data recipient of the CDR data (other than for Privacy Safeguards 1 – 4). See Competition and Consumer Act, paragraph 56EC(5)(aa).

¹⁵ Specifically, a data holder who is also an APP entity must continue to take reasonable steps to correct CDR data that is personal information where it is inaccurate, out-of-date, incomplete, irrelevant or misleading for the purpose for which it is held under APP 13.

¹⁶ For data holders, this obligation only arises if the entity was earlier required or authorised under the CDR Rules to disclose the CDR data.

Acknowledging receipt of correction requests

- 13.17 When a consumer makes a request to correct their CDR data, subrule 7.15(a) of the CDR Rules requires the entity to acknowledge receipt of the correction request as soon as practicable.
- 13.18 An entity must acknowledge it has received the correction request. It is best practice for an entity to update the consumer dashboard to reflect that a correction request has been received, provided the consumer dashboard has such a functionality.
- 13.19 However, it is not a requirement that this acknowledgement be in writing or through the dashboard. For example, acknowledgement provided by other electronic means or over the phone is sufficient. Where an entity acknowledges receipt over the phone, it is best practice to also make a record of this as evidence that it has complied with subrule 7.15(a) of the CDR Rules.
- 13.20 In adopting a timetable that is ‘practicable’, an entity can take technical and resource considerations into account. However, it is the responsibility of the entity to justify any delay in acknowledging receipt of a request.

Actioning and responding to correction requests (for CDR data that is not AEMO data)

Taking action to correct, or qualify, the CDR data

13.21 Rule 7.15 of the CDR Rules requires an entity that receives a correction request relating to CDR data (that is not AEMO data) to either:

- correct the CDR data, or
- both:
 - include a qualifying statement with the data to ensure that, having regard to the purpose for which it is held, the data is accurate, up to date, complete and not misleading, and
 - where practicable, attach an electronic link to a digital record of the data in such a way that the statement will be apparent to any users of the data.

The entity must take one of these steps within 10 business days after receipt of the request, and to the extent that the entity considers appropriate in relation to the CDR data that is the subject of the request.

13.22 The 10 business day period commences on the day after the entity receives the correction request.¹⁷ For example, if the entity receives the correction request on 2 August, the 10 business day period begins on 3 August.

13.23 A ‘business day’ is a day that is not Saturday, Sunday or a public holiday in the place concerned.

¹⁷ See *Acts Interpretation Act 1901*, section 36.

- 13.24 An entity must first consider the extent to which it considers it appropriate to correct or qualify the information. Once it determines this, it must either correct the CDR data or include a qualifying statement with the CDR data. Such corrections or qualifying statements must make the data accurate, up to date, complete and not misleading having regard to the purpose for which it is held (to the best of the entity's knowledge).
- 13.25 The requirement to, where practicable, attach an electronic link to a digital record of the CDR data helps to ensure that any qualifying statement included with the CDR data is prominently displayed to those who access the data. An entity's systems should be set up so that the CDR data cannot be accessed without the qualifying statement or a link to that statement being prominently displayed.
- 13.26 If an entity requires further information or explanation before it can determine which action to take, the entity should clearly explain to the consumer what additional information or explanation is required and/or why the entity cannot act on the information already provided. The entity could also advise where additional material may be obtained. The consumer should be given a reasonable opportunity to comment on the refusal or reluctance of the entity to make a correction without further information or explanation from the consumer.
- 13.27 An entity should also be prepared to search its own records and other readily accessible sources that it reasonably expects to contain relevant information, to find any information in support of, or contrary to, the consumer's request. However, an entity need not conduct a full, formal investigation into the matters about which the consumer requests correction. The extent of the investigation required will depend on the circumstances, including the seriousness of any adverse consequences for the consumer if the CDR data is not corrected as requested.

When action is not necessary in response to a request

- 13.28 An entity may consider that it is not appropriate to make any correction or qualifying statement at all,¹⁸ because (for instance) the CDR data as it exists is accurate, up to date, complete and not misleading, for the purpose it is held.
- 13.29 In such circumstances, the entity must give the CDR consumer a notice in accordance with subrule 7.15(c) in the CDR Rules detailing the reasons why it considered that no correction or qualifying statement was necessary or appropriate and setting out the available complaint mechanisms.¹⁹
- 13.30 Reasons for not correcting CDR data or including a qualifying statement with the data may include:
- while there are inaccuracies in the data, it is nevertheless accurate, up to date, complete and not misleading for the purpose for which it is held
 - the CDR consumer is mistaken and has made the correction request in error
 - the CDR consumer is attempting to prevent an accredited person from collecting accurate CDR data that is unfavourable to the consumer

¹⁸ See CDR Rules, subrule 7.15(b).

¹⁹ Competition and Consumer Act, paragraph 56EP(3)(b).

- the entity is an accredited data recipient of the CDR data, but the request is in respect of data the entity has collected from a data holder, and the accredited data recipient is unable to determine whether the CDR data is correct using its own records and other readily accessible sources,²⁰ with the effect that the consumer should make the request to the data holder, or
- the CDR data has already been corrected, or a qualifying statement already included with the data, on a previous occasion.

Example

Jessica decides to change credit card provider. Jessica authorises her current data holder BankaLot Ltd to disclose her CDR data to accredited person, CreditCardFinder Pty Ltd, which sends BankaLot a consumer data request on Jessica's behalf. Shortly after Jessica is notified that the data has been collected, Jessica requests CreditCardFinder to correct the annual fee amount on her account, as she believes her annual fees are lower.

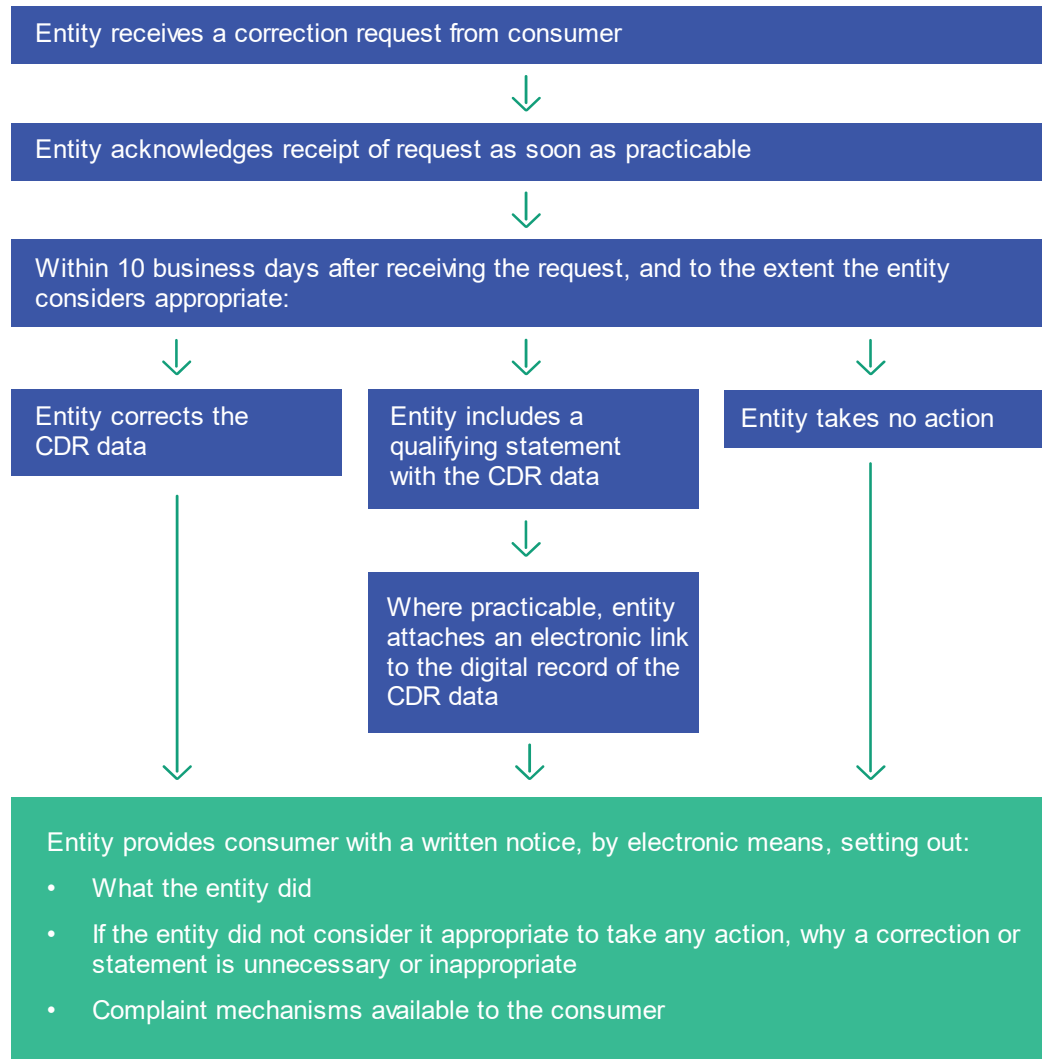
CreditCardFinder acknowledges receipt of the request the following business day through Jessica's consumer dashboard. CreditCardFinder determines that because the CDR data was collected from BankaLot and CreditCardFinder has no method of independently determining the correctness of the data, it is not appropriate for it to make any corrections or include any qualifying statements with the data.

CreditCardFinder then gives Jessica a notice through her consumer dashboard that states this finding, and that if Jessica wants the data to be corrected, she should request that BankaLot make the relevant correction.

The notice also sets out the complaint mechanisms available to Jessica, which are in line with the corresponding section in CreditCardFinder's CDR policy.

²⁰ Note that data derived from CDR data collected by an accredited data recipient continues to be 'CDR data': see Competition and Consumer Act, section 56AI.

How to respond to a correction request (CDR data that is not AEMO data)



How must a correction notice be provided to consumers?

13.31 Subrule 7.15(c) of the CDR Rules requires an entity that receives a request from a CDR consumer to correct CDR data to give the consumer a written notice by electronic means. The written notice must contain the matters set out in paragraph 13.35 below.

13.32 The requirement for written notices to be given by electronic means will be satisfied if the notice is given, for example, over email or over the consumer's dashboard.

13.33 The written notice may be in the body of an email or in an electronic file attached to an email.

13.34 While SMS is an electronic means of communicating a notice, practically it is unlikely to be appropriate as the number of matters that the written notice must address under subrule 7.15(c) of the CDR Rules would likely make the SMS very long.

Privacy tip: In selecting an 'electronic means' for the notice, it is best practice that data holders and accredited data recipients consider the consumer's chosen method for receiving communications (if applicable), the means of communication the consumer used to make

the Privacy Safeguard 13 request, and whether the consumer is likely to receive the notice in a timely manner through a given ‘electronic means’. For example, if the entity received the request in an email from the consumer, it may be most appropriate to provide the notice by responding to that email.

What must be included in a correction notice to consumers?

13.35 The correction notice to the consumer must set out:

- what the entity did in response to the request
- if the entity did not consider it appropriate to correct the data or include a qualifying statement, why a correction or statement is unnecessary or inappropriate, and
- the complaint mechanisms available to the consumer.

13.36 The complaint mechanisms available to the consumer that must be included in the notice are:

- the entity’s internal dispute resolution processes relevant to the consumer, including any information from the entity’s CDR policy about the making of a complaint relevant to the entity’s obligations to respond to correction requests, and
- external complaint mechanisms the consumer is entitled to access, including the consumer’s right to complain to the Australian Information Commissioner under Part V of the Privacy Act,²¹ and any external dispute resolution schemes recognised by the Australian Competition and Consumer Commission under subsection 56DA(1) of the Competition and Consumer Act.

13.37 An entity may, but is not required to, advise the consumer that if they have suffered loss or damage by the entity’s acts or omissions in contravention of the privacy safeguards or CDR Rules, they have a right to bring an action for damages in a court of competent jurisdiction under section 56EY of the Competition and Consumer Act.

Actioning and responding to correction requests (for AEMO data)

13.38 If a retailer receives a correction request relating to AEMO data, the retailer is not required to take action to correct, or qualify, the CDR data. Instead, the retailer must, as soon as practicable:

- initiate the relevant correction procedures under the National Electricity Rules in relation to any NMI standing data or metering data for which correction is requested, and
- if the request relates to DER register data, provide the consumer with information about how the consumer can contact the distributor to have the data corrected.²²

²¹ Competition and Consumer Act, subsection 56ET(4).

²² See CDR Rules, clause 6.1 of Schedule 4.

How to respond to a correction request (AEMO data)

Entity receives a correction request from consumer



Entity acknowledges receipt of request as soon as practicable



As soon as practicable, the entity must:



Initiate the relevant correction procedures under the National Electricity Rules in relation to any NMI standing data or metering data for which correction is requested



If the request relates to DER register data, provide the consumer with information about how the consumer can contact the distributor to have the data corrected

What are the correction considerations?

- 13.39 For CDR data that is not AEMO data, Privacy Safeguard 13 requires that any statement included with CDR data in response to a correction request is to ensure that, having regard to the purpose for which it is held, the CDR data is ‘accurate’, ‘up to date’, ‘complete’ and ‘not misleading’.²³ ‘Held’ is discussed in [Chapter B \(Key concepts\)](#).
- 13.40 Whether or not CDR data is accurate, up to date, complete and not misleading must be determined with regard to the purpose for which it is held.
- 13.41 When working out the purpose for which the CDR data is or was held, entities must disregard the purpose of holding the CDR data so that it can be disclosed as required under the CDR Rules.²⁴
- 13.42 For example, a data holder that is an authorised deposit-taking institution collects transaction data for the purpose of providing a banking service to its customer. It does not hold transaction data for the purpose of being required to disclose the data under the CDR system. Another example is a data holder that is an energy provider collects consumer contact details for the purpose of providing an energy service to its customer. It does not hold the consumer contact details for the purpose of being required to disclose the data under the CDR system. ‘Purpose’ is discussed further in [Chapter B \(Key concepts\)](#).
- 13.43 The four terms listed in Privacy Safeguard 13, ‘accurate’, ‘up to date’, ‘complete’ and ‘not misleading’ are not defined in the Competition and Consumer Act or the Privacy Act.²⁵

²³ Competition and Consumer Act, paragraph 56EP(3)(a)(ii).

²⁴ Competition and Consumer Act, subsection 56EP(4).

²⁵ The terms ‘accurate’, ‘up to date’ and ‘complete’ are also used in Privacy Safeguard 11 in respect of the quality considerations of CDR data. See [Chapter 11 \(Privacy Safeguard 11\)](#) for further information and for examples of an entity determining the purpose for which it holds CDR data.

13.44 The following analysis of each term draws on the ordinary meaning of the terms, the APP Guidelines and Part V of the *Freedom of Information Act 1982*.²⁶ As the analysis indicates, there is overlap in the meaning of the terms.

Accurate

13.45 CDR data is inaccurate if it contains an error or defect or is misleading. An example is factual information about a consumer's account, income, assets, payment history or repayment history or employment status which is incorrect for the purpose it is held.

13.46 CDR data that is derived from other CDR data is not inaccurate by reason only that the consumer disagrees with the method or result of the derivation.²⁷ For the purposes of Privacy Safeguard 13, derived data may be 'accurate' if it is presented as such and accurately records the method of derivation (if appropriate).

13.47 For instance, an accredited data recipient may use the existing information it holds about a consumer to predict their income over a certain period of time. If the data is presented as the estimated future income for the consumer for that period, and states the bases of the estimation (that is, it is based on the consumer's income over the previous financial years), this would not be inaccurate solely because, for instance, the consumer believes their income will be higher or lower during the projected period.

13.48 CDR data may be inaccurate even if it is consistent with a consumer's instructions or if the inaccuracy is attributable to the consumer.

Up to date

13.49 CDR data is not up to date if it contains information that is no longer current. An example is a statement that a consumer has an active account with a certain entity, where the consumer has since closed that account or changed providers.

13.50 Another example is an assessment that a consumer has the ability to meet a loan repayment obligation, where in fact the consumer's ability to do so has since changed.²⁸

13.51 CDR data about a past event may have been up to date at the time it was recorded but has been overtaken by a later development. Whether that data is up to date will depend on the purpose for which it is held. If, for instance, a consumer has had their second child but their CDR data records them as only having one child, the CDR data will still be up to date if the data that records the consumer as having one child is held simply for the purpose of recording whether the consumer is a parent.

13.52 In a similar manner to accuracy, CDR data may not be up to date even if it is consistent with a consumer's instructions or if the inaccuracy is attributable to the consumer.

²⁶ See APP Guidelines, [Chapter 10 \(APP 10\)](#).

²⁷ Data derived from CDR data continues to be 'CDR data': see Competition and Consumer Act, section 56AI.

²⁸ Such an assessment will likely be 'materially enhanced information' under section 10 of the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019, or section 11 of the Consumer Data Right (Energy Sector) Designation 2020, and therefore not 'required consumer data' under the CDR Rules.

Complete

13.53 CDR data is incomplete if it presents a partial or misleading picture of a matter of relevance, rather than a true or full picture.

13.54 An example is data from which it can be inferred that a consumer owes a debt, which in fact has been repaid. The CDR data will be incomplete under Privacy Safeguard 13 if the data is held, for instance, for the purpose of determining the borrowing capacity of the consumer. Where the CDR data is held for a different purpose for which the debt is irrelevant, the fact that the debt has been repaid may not of itself render the CDR data incomplete. If, however, the accredited person has requested a consumer's CDR data for a specific period, and in that period the consumer owed a debt which is recorded in the CDR data, and that debt was repaid in a later period, the CDR data will still be 'complete' in respect of that specific period.

Not misleading

13.55 CDR data will be misleading if it conveys a meaning that is untrue or inaccurate or could lead a user, receiver or reader of the information into error. An example is a statement that is presented as a statement of fact but in truth is a record of the opinion of a third-party. In some circumstances an opinion may be misleading if it fails to include information about the facts on which the opinion was based, or the context or circumstances in which the opinion was reached.

13.56 CDR data may also be misleading if other relevant information is not included.

Example

Angelica consents to XYZ Solutions Pty Ltd (XYZ) (an accredited person) collecting her CDR data from Bright Spark Electricity (Bright Spark) (a data holder) and using that data for the purpose of providing Angelica with recommendations for various energy products.

Angelica has previously spoken with Bright Spark employee, Bert, about energy products offered by Bright Spark and been mistakenly advised that she has made an overpayment on her energy account, when she has not actually made an overpayment. Bert had recorded, as part of Angelica's CDR data, that Angelica has made an overpayment on her energy account.

If Angelica requests that XYZ or Bright Spark correct her CDR data, the entity may include a qualifying statement with the data that Angelica has not made an overpayment on her energy account. Alternatively, the entity may delete or alter the relevant part of the data to make clear that Angelica has not made an overpayment on her energy account. If any one of these actions was taken, the data would no longer be inaccurate or misleading.

Charges to correct CDR data

13.57 Rule 7.14 of the CDR Rules prohibits an entity from charging a fee for responding to, or actioning, a request under Privacy Safeguard 13.

Interaction with other privacy safeguards

Privacy Safeguard 5

- 13.58 Privacy Safeguard 5 requires an accredited data recipient of CDR data to notify a consumer of the collection of their CDR data by updating the consumer's dashboard.
- 13.59 Where an accredited person has collected CDR data, and then collects corrected CDR data after the data holder or accredited data recipient complies with the consumer's requests to correct and disclose corrected data under Privacy Safeguards 11 and 13, the accredited person must notify that consumer under Privacy Safeguard 5 in respect of both collections.

Privacy Safeguard 10

- 13.60 Privacy Safeguard 10 requires a data holder and accredited data recipient to notify a CDR consumer of the disclosure of their CDR data by updating the consumer's dashboard.
- 13.61 Where a data holder or accredited data recipient has disclosed CDR data and then discloses corrected data as a result of the consumer's requests to correct and disclose corrected data under Privacy Safeguards 11 and 13, the entity must notify that consumer under Privacy Safeguard 10 in respect of both disclosures.

Privacy Safeguard 11

- 13.62 A correction request made under Privacy Safeguard 13 may trigger a CDR entity's obligations under Privacy Safeguard 11 (Quality of CDR data).
- 13.63 Under Privacy Safeguard 11, data holders and accredited data recipients have an obligation to advise consumers if they disclose CDR data at a point in time, but then later become aware that some or all of the CDR data disclosed was inaccurate, out of date or incomplete, having regard to the purpose for which the data was held at the time of disclosure. Privacy Safeguard 11 also requires data holders and accredited persons to disclose corrected CDR data to the accredited person who originally received the data, where requested by the affected consumer.
- 13.64 A CDR entity may become aware of inaccuracies in CDR data in a range of ways – including through a consumer's request that the entity correct their CDR data under Privacy Safeguard 13, or during an investigation that is triggered by a Privacy Safeguard 13 request.
- 13.65 Therefore, an entity that corrects CDR data, or includes a qualifying statement with such data in accordance with Privacy Safeguard 13, must also consider whether the consumer must be advised of any previous disclosures of incorrect CDR data, in accordance with Privacy Safeguard 11.²⁹

Privacy Safeguard 12

- 13.66 Where an accredited data recipient corrects CDR data to comply with Privacy Safeguard 13, it should consider whether it needs to take action under Privacy Safeguard 12 to destroy or de-identify the original data.

²⁹ Competition and Consumer Act, subsection 56EN(3).