

Complete version of the Draft Privacy Safeguard Guidelines (combined)

Consultation draft, October 2019



Chapter A: Introductory matters

Consultation draft, October 2019

Contents

Purpose	3
About the Consumer Data Right	3
About the privacy safeguards	4
Who must comply with the privacy safeguards?	5
Which privacy safeguards apply to each entity?	5
Do the privacy safeguards apply instead of the Privacy Act and the APPs?	5
What happens if an entity breaches the privacy safeguards?	6
Where do I get more information?	6

Purpose

- A.1 The Australian Information Commissioner issues these Privacy Safeguard guidelines under s 56EQ(1)(a) of the *Competition and Consumer Act 2010* (Cth) (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) regime.
- A.4 The Privacy Safeguard guidelines outline:
- the mandatory requirements in the privacy safeguards and related Consumer Data Rules — generally indicated by ‘must’ or ‘is required to’
 - the Information Commissioner’s interpretation of the privacy safeguards and Consumer Data Rules — generally indicated by ‘should’
 - examples that explain how the privacy safeguards and Consumer Data 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 mandatory requirements in the privacy safeguards; the particular circumstances of an entity will also be relevant
 - good privacy practice to supplement minimum compliance with the mandatory requirements in the privacy safeguards and Consumer Data 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 Consumer Data Rules in particular circumstances. An entity may wish to seek independent legal advice where appropriate.

About the Consumer Data Right

- A.6 The CDR aims to provide greater choice and control for Australians over how their data is used and disclosed. It allows consumers to access particular data in a usable form and to direct a business to securely transfer that data to an accredited person.
- A.7 Individual consumers and small, medium and large business customers will all be able to exercise the Consumer Data Right in relation to data that is covered by the CDR regime.
- A.8 The CDR will be rolled out in stages starting with the banking sector (known as ‘Open Banking’). Next, CDR will be implemented in the energy and telecommunication sectors. It will then be introduced sector by sector across the broader economy.

¹ 56EQ(5).

About the privacy safeguards

- A.9 These guidelines should be read together with the full text of Division 5 of Part IVD of the Competition and Consumer Act and the Consumer Data Rules.
- A.10 The privacy safeguards are legally binding statutory provisions, which ensure the security and integrity of the CDR regime, supplemented by Consumer Data 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 consumers.
- A.12 The privacy safeguards only apply to CDR data for which there are one or more consumers.² This means that if there is no person that is identifiable or reasonably identifiable from the CDR data,³ because, for instance, it is product data for which there is no consumer, the privacy safeguards do not apply.
- A.13 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.14 The requirements in each of these privacy safeguards interact with and complement each other.
- A.15 In developing the Privacy Safeguard guidelines, the Australia Information Commissioner has had regard to the objects of Part IVD of the Competition and Consumer Act, stated in s 56AA:
- 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.
- A.16 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.17 The number of the chapter corresponds to the number of the privacy safeguard.
- A.18 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.

² 56EB(1).

³ 56AI(3)(c).

A.19 Chapter C contains guidance on consent, which is the basis for collecting and using CDR data under the CDR regime.

Who must comply with the privacy safeguards?

- A.20 The privacy safeguards apply to entities who are authorised or required under the CDR regime to collect, use or disclose CDR data for which there is at least one consumer. This includes accredited persons, accredited data recipients, data holders and designated gateways. Each of these types of entities are defined in the Competition and Consumer Act and discussed in Chapter B (Key Concepts).
- A.21 Each privacy safeguard chapter specifies the type of entity to which it applies.
- A.22 The privacy safeguards extend to acts, omissions, matters and things outside Australia.⁴
- A.23 In respect of CDR data held within Australia, the privacy safeguards apply to all persons, including foreign persons.⁵
- A.24 In respect of an act or omission relating to CDR data held outside Australia, the privacy safeguards only apply if the act or omission:⁶
- 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.

Which privacy safeguards apply to each entity?

CDR entity	Privacy Safeguards that apply
Accredited person	Privacy Safeguards 1, 3, 4 and 5
Accredited data recipient	Privacy Safeguards 1 to 13 inclusive
Data holders	Privacy Safeguards 1, 10, 11 and 13
Designated gateways	Privacy Safeguards 1, 6, 7 and 12

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

A.25 Generally, the privacy safeguards apply in respect of an entity's handling of CDR data instead of the *Privacy Act 1988* (Cth) (Privacy Act) and the Australian Privacy Principles (APPs).⁷

⁴ 56AO(1).

⁵ 56AO(2).

⁶ 56AO(3).

⁷ 56EC(4).

A.26 In each chapter in these guidelines, the interaction between the privacy safeguard and corresponding APP is discussed.

What happens if an entity breaches the privacy safeguards?

A.27 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.28 Where a consumer makes a complaint, the Information Commissioner will generally attempt to conciliate the complaint.

A.29 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,⁸ for example the power to make a determination,⁹ 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.¹⁰

A.30 The Australian Competition and Consumer Commission will also have a general strategic enforcement role where there are repeated or serious breaches.

Where do I get more information?

A.31 The Office of the Australian Information Commissioner (OAIC) has further information about the CDR and its role on the OAIC website, see www.oaic.gov.au/consumer-data-right.

⁸ 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

⁹ s 52 of the Privacy Act

¹⁰ 56EU

Chapter B:

Key concepts

Consultation draft, October 2019



Contents

About this Chapter	4
Accredited data recipient	4
Accredited person	4
CDR data	5
Derived CDR data	5
CDR participant	5
CDR receipt	5
CDR regime	5
Collect	6
Consent	6
Consumer, CDR consumer or ‘eligible’ CDR consumer	7
Reasonably identifiable	7
Relates to	8
Associate	8
Held	9
Eligible CDR consumer	9
Consumer dashboard	10
Consumer data request	10
Direct request service	10
Accredited person request service	11
Valid consumer data request	11
Valid request	11
Consumer data rules	11
Current	12
Current consent	12
Current authorisation	12
Consumer Experience Guidelines	13
Data holder	13
Earliest holding day	14
Data minimisation principle	14
Data standards	14
Designated gateway	15
Designation Instrument	15
Disclosure	15

Eligible	16
Outsourced service provider	16
CDR outsourcing arrangement	16
Purpose	17
Reasonable, Reasonably	17
Reasonable steps	18
Redundant data	18
Required consumer data	18
Required or authorised by an Australian law or by a court/tribunal order	18
Australian law	18
Court/tribunal order	19
Required	19
Authorised	19
Required or authorised to use or disclose CDR data under the Consumer Data Rules	20
Required	20
Authorised	20
Required product data	20
Use	21
Voluntary consumer data	21
Voluntary product data	22

About this Chapter

B.1 This Chapter outlines some key words and phrases that are used in the privacy safeguards and consumer data rules.

Accredited data recipient

B.2 A person is an ‘accredited data recipient’ if the person:

- is an accredited person
- has collected CDR data from a data holder under the consumer data rules
- 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.¹

B.3 A person will only be an ‘accredited data recipient’ in relation to the CDR data that it has collected under the consumer data rules.

B.4 Where an accredited person seeks consent from a consumer to collect and use CDR data, and subsequently seeks to collect CDR data, they do so as an accredited person because they are yet to collect the CDR data.

B.5 Once an accredited person has collected CDR data, they will be an accredited data recipient in relation to that CDR data.

B.6 As such, a person may be both an accredited data recipient and an accredited person at any point in time, in relation to different consumers.²

B.7 Where a privacy safeguard applies to ‘accredited data recipients’, the privacy safeguard only applies in relation to CDR data collected by accredited persons under the consumer data rules.

Accredited person

B.8 An ‘accredited person’ is a person who has been granted accreditation by the Data Recipient Accreditor.³

B.9 The Data Recipient Accreditor is the Australian Competition and Consumer Commission (ACCC).⁴

B.10 To be granted an accreditation, the person must satisfy the accreditation criteria in Part 5 of the Consumer Data Rules.

¹ 56AK. Rather, the person must hold that CDR data as a result of seeking to collect the CDR data from a data holder under the Consumer Data Rules.

² The person would be an accredited person in relation to a consumer that it is seeking consent to collect and use CDR data from and an accredited data recipient in relation to consumers for which it has already collected CDR data.

³ 56CA (1).

⁴ The ACCC has been appointed as the Data Recipient Accreditor by the Treasurer under section 56CG of the Competition and Consumer Act.

CDR data

B.11 ‘CDR data’ is information that is:

- within a class of information specified in the designation instrument for each sector,⁵ or
- derived from the above information (‘derived CDR data’).⁶

Derived CDR data

B.12 ‘Derived CDR data’ is data that has been wholly or partly derived from CDR data, or data derived from previously derived data.⁷ This means data derived from ‘derived CDR data’ is also ‘derived CDR data’.

B.13 ‘Derived’ takes its ordinary meaning. This is because ‘derived’ is not defined in the *Competition and Consumer Act 2010* (Cth) (Competition and Consumer Act) or the *Privacy Act 1988* (Cth) (the Privacy Act).

CDR participant

B.14 A ‘CDR participant’ is a data holder or an accredited data recipient.⁸

CDR receipt

B.15 A ‘CDR receipt’ is a notice given by an accredited person to a CDR consumer who has consented to the accredited person collecting and using their CDR data, or given to a consumer who has withdrawn such a consent.⁹

B.16 CDR receipts must be given in accordance with Consumer Data Rule 4.18.

CDR regime

B.17 The ‘CDR regime’ was enacted by the *Treasury Laws Amendment (Consumer Data Right) Act 2019* (Cth) to insert a new Part IVD into the Competition and Consumer Act.

⁵ The designation instrument specifies classes of data for each sector. The designation instrument for the banking sector sets out the classes of information that are subject to the CDR regime, 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 regime. The designation instrument for the banking sector is available [here](#).

⁶ 56AI(1). The designation instrument for the banking sector (available [here](#)) excludes ‘materially enhanced information’ from the class of information about the use of a product. However, ‘materially enhanced information’ is nonetheless CDR data (as it is data derived from a specified class of information in the relevant designation instrument). For further information, see the Explanatory Statement to the designation instrument for the banking sector (available [here](#)) as well as the explanation of ‘voluntary consumer data’ in this Chapter.

⁷ 56AI(2).

⁸ 56AL(1).

⁹ Consumer Data Rule 4.18(1).

B.18 The CDR regime includes the Consumer Data Rules, privacy safeguards, data standards, designation instruments, and any regulations made in respect of the provisions inserted into the Competition and Consumer Act by these amendments.

Collect

B.19 ‘Collects’ is defined in section 4(1) of the Competition and Consumer Act, which 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 Competition and Consumer Act).

B.20 ‘Record’ is defined in the Privacy Act to include a document or an electronic or other device, but does not include:¹⁰

- anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition
- Commonwealth records as defined by subsection 3(1) of the *Archives Act 1983* that are in the open access period for the purposes of that Act
- certain records in the care of the National Archives of Australia
- documents placed by or on behalf of a person (other than an agency) in the memorial collection within the meaning of the *Australian War Memorial Act 1980*, or
- letters or other articles in the course of transmission by post.¹¹

Consent

B.21 Consent must meet the requirements set out in the Consumer Data Rules.

B.22 Consent is the only basis on which an accredited person may collect and use CDR data.

B.23 Consent also underpins how an accredited person or accredited data recipient may collect and use CDR data in the CDR regime.¹²

B.24 For further information, including the requirements by which an accredited person must seek consent from a consumer, see [Chapter C \(Consent\)](#).

¹⁰ The Privacy Act definition of ‘record’ also excludes a generally available publication, but as stated in B.19 generally available publications are included in the CDR definition of ‘collects’. See Privacy Act, s 6.

¹¹ Privacy Act, s 6

¹² For example, an accredited person may only use or disclose CDR data in accordance with a current consent from the consumer unless an exception applies. One way in which an accredited person is authorised to use or disclose CDR data under the Consumer Data Rules is to provide goods or services requested by the consumer. This must be done in compliance with the data minimisation principle and in accordance with a current consent from the consumer (Consumer Data Rule 7.5(1)(a)). For further information, see [Chapter 6 \(Privacy Safeguard 6\)](#).

Consumer, CDR consumer or ‘eligible’ CDR consumer

- B.25 The ‘CDR consumer’ is the person who is able to:
- access the CDR data held by a data holder, and
 - direct that the data be disclosed to them or to an accredited person.
- B.26 A ‘CDR consumer’ is an identifiable or reasonably identifiable person to whom CDR data relates because of the supply of a good or service either to the person or to an associate of the person.¹³
- B.27 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 or family member.¹⁴
- B.28 The CDR data that relates to the CDR consumer must be held by:
- a data holder of the CDR data
 - an accredited data recipient of the CDR data or
 - an entity that holds the data on behalf of a data holder or accredited data recipient of the CDR data.¹⁵
- B.29 Section 4B(1) of the Competition and Consumer Act does not apply for the purposes of determining whether a person is a CDR consumer.¹⁶ This section explains when a person is taken to have acquired particular goods or services as a consumer, outside of the CDR regime.
- B.30 The Privacy Safeguard guidelines use the term ‘consumer’ to refer to ‘CDR consumer’.

Reasonably identifiable

- B.31 For a person to be a CDR consumer, the person must be identifiable, or ‘reasonably identifiable’, from the CDR data or other information held by the entity.
- B.32 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 B.47-B.50 for a discussion on the meaning of ‘held’), and
 - whether it is practicable to use that information to identify the person.
- B.33 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

¹³ 56AI(3)(a). Note that s 56AI(3)(a)(ii) allows for regulations to be made to prescribe circumstances in which CDR data may relate to a person.

¹⁴ In the banking sector, a key example of this is where CDR data relates to a joint account.

¹⁵ 56AI(3).

¹⁶ 56AI(4).

person as a CDR consumer – the entity would need to handle CDR data which relates to the CDR consumer in accordance with the privacy safeguards.

B.34 See B.113-B.116 for a discussion on the meaning of ‘reasonably’.

Relates to

B.35 For a person to be a CDR consumer, CDR data must ‘relate to’ that person.

B.36 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.¹⁷ The relevant context in the CDR regime is the Competition and Consumer Act and the Privacy Act.

B.37 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 consumer data rules.¹⁸

B.38 CDR data will not ‘relate to’ a person unless the data itself is somehow relevant or appropriate for that person’s use as a consumer under the CDR regime.

B.39 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.42-B.46 below).

B.40 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.¹⁹

B.41 By using the broad phrase ‘relates to’, the CDR regime captures meta-data.²⁰

Associate

B.42 For a person to be a CDR consumer, 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’.

B.43 In this context, ‘associate’ has the same meaning as in the *Income Tax Assessment Act 1936* (Cth) (the ITA Act).²¹ Section 318 of the ITA Act defines ‘associates’ with respect to natural persons, companies, trustees and partnerships.²²

B.44 For natural persons, an associate is:

- a relative
- a partner

¹⁷ *PMT Partners Pty Ltd (in liq) v Australian National Parks and Wildlife Service* (1995) 184 CLR 301, 331 (Toohey and Gummow JJ).

¹⁸ s 56AI(3)(a).

¹⁹ Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2018, [1.108].

²⁰ 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 2018, [1.106].

²¹ 56AI(3).

²² For the purposes of the CDR regime, associates of partnerships are not directly relevant, as a partnership is not a ‘person’.

- 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.45 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.46 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 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.

Held

- B.47 CDR data that relates to a CDR consumer must be ‘held’ by:
- a data holder of the CDR data
 - an accredited data recipient of the CDR data, or
 - an entity that holds the data on behalf of a data holder or accredited data recipient of the CDR data.²³
- B.48 A person ‘holds’ data if they have possession or effective control of a medium that contains the CDR data. As ‘held’ is not defined in the Competition and Consumer Act, it takes its ordinary meaning, consistent with the OAIC’s [APP Guidelines](#).
- B.49 If a person has a right or power to deal with particular data, the person has effective control of the data and therefore ‘holds’ the data.
- B.50 For example, a person ‘holds’ data where the person:
- physically possesses the medium on which the data is stored (including a physical record that contains the data) and can access the data physically or by use of an electronic device (such as decryption software), or
 - has the right or power to deal with the data, even if the person does not physically possess or own the medium on which the data is stored, such as where the person has outsourced the storage of data to a third party but retains the right to deal with it, including to access and amend that data.

Eligible CDR consumer

- B.51 While ‘CDR consumer’ is defined in the Competition and Consumer Act, only ‘eligible’ CDR consumers may make consumer data requests under the Consumer Data Rules.
- B.52 A consumer for the banking sector is ‘eligible’ if they have an account with the data holder that is open and set up in such a way that it can be accessed online.²⁴
- B.53 A consumer for the banking sector who is an individual must be 18 years or older.
- B.54 A person may be an eligible consumer if they are a body corporate, body politic or individual.

²³ 56AI(3).

²⁴ Consumer Data Rules, Schedule 3, clause 2.1.

Consumer dashboard

- B.55 Each accredited person and each data holder must provide a ‘consumer dashboard’ for CDR consumers.
- B.56 An accredited person’s consumer dashboard is an online service that can be used by CDR consumers. Each dashboard is visible only to the accredited person and the relevant CDR consumer.
- CDR consumers can use their dashboard to manage consumer data requests and associated consents for the accredited person to collect and use CDR data.
 - The service must also notify the consumer of information related to CDR data collected pursuant to a consent.
- B.57 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. The service must also notify the consumer of information related to CDR data disclosed pursuant to an authorisation.

Consumer data request

- B.58 A ‘consumer data request’ is either:
- a request made directly by a CDR consumer to a data holder²⁵ or
 - a request made by an accredited person to a data holder, 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.²⁶
- B.59 A request directly from a CDR consumer must be made using the data holder’s direct request service and may be for some or all of the consumer’s CDR data.²⁷
- B.60 A request from an accredited person must be made through the data holder’s accredited person request service and must relate only to data the person has consent from the consumer to collect and use. A request from an accredited person must comply with the data minimisation principle.²⁸
- B.61 Refer to [Chapter C: Consent](#) for further information.

Direct request service

- B.62 A data holder’s ‘direct request service’ is an online service allowing eligible CDR consumers to make consumer data requests directly to the data holder in a timely and efficient manner.²⁹

²⁵ Consumer Data Rule 3.3(1).

²⁶ Consumer Data Rule 4.4(1).

²⁷ Consumer Data Rule 3.3(1).

²⁸ Consumer Data Rule 4.4(1).

²⁹ Consumer Data Rule 1.13(2)

B.63 It also allows CDR consumers to receive the requested data in human-readable form and sets out any fees for disclosure of voluntary consumer data.

B.64 This service must conform with the data standards.

Accredited person request service

B.65 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.³⁰

B.66 It also allows accredited persons to receive requested data in machine-readable form.

B.67 This service must conform with the data standards.

Valid consumer data request

B.68 A consumer data request is 'valid' if it is made directly by an eligible CDR consumer.³¹

Valid request

B.69 A 'valid' request is defined in the Consumer Data Rules in Part 3 (Consumer data requests made by eligible CDR consumers) and Part 4 (Consumer data requests made by accredited persons).

B.70 Under Part 3, a request is 'valid' if:

- the CDR consumer has requested the accredited person to provide goods or services to themselves or another person and the accredited person needs the CDR data to provide those goods or services
- the accredited person has asked the consumer to give their consent for the person to collect and use the CDR data in order to provide those goods or services and
- the CDR consumer has given consent in response to the accredited person's request (and that consent has not been withdrawn).³²

B.71 Under Part 4, a consumer data request made by a CDR consumer directly to a data holder is 'valid' if it is made by a CDR consumer who is eligible to make the request.³³

B.72 An 'eligible' consumer for the banking sector is discussed above at the CDR Consumer key concept.

Consumer data rules

B.73 The ACCC has the power to make rules,³⁴ with the consent of the Minister,³⁵ to determine how the CDR functions in each sector. Consumer data rules may be made on all aspects of

³⁰ Consumer Data Rule 1.13(3).

³¹ Consumer Data Rule 3.3(3).

³² Consumer Data Rule 4.3.

³³ Consumer Data Rule 3.3(3).

³⁴ 56BA(1)

³⁵ 56BR

the CDR regime (as provided in Part IVD the Competition and Consumer Commission Act) including the privacy safeguards, accreditation of an entity, the Data Standards Body and the format of CDR data and the data standards.

- B.74 On 2 September 2019, the ACCC published a lock down version of the Consumer Data Rules and accompanying Explanatory Statement, available at [CDR Rules \(banking\)](#).
- B.75 This lock down version of the Consumer Data Rules cover the foundational rules required to implement the CDR in the banking sector.
- B.76 Initially, the Consumer Data Rules will apply only to certain products that are offered by certain data holders in the banking sector. It is intended that the rules will progressively apply to a broader range of data holders and products over time.

Current

Current consent

- B.77 Consent to collect and use particular CDR data is ‘current’ if it has not expired under Consumer Data Rule 4.14.³⁶
- B.78 Consumer Data Rule 4.14 provides that consent expires if:
- it is withdrawn
 - the accredited person is notified by the data holder of the withdrawal of authorisation
 - the period of consent has ended
 - 12 months has passed after consent was given
 - another Consumer Data Rule provides that consent expires or
 - the accredited person’s accreditation is revoked or surrendered.

Current authorisation

- B.79 Authorisation to disclose particular CDR data to an accredited person is ‘current’ if it has not expired under Consumer Data Rule 4.26.
- B.80 Consumer Data Rule 4.26 provides that authorisation expires if:
- it is withdrawn
 - the CDR consumer ceases to be eligible
 - the data holder is notified by the accredited person of the withdrawal of consent to collect the CDR data
 - the period of authorisation has ended
 - authorisation was for a single occasion and the disclosure has occurred
 - 12 months has passed after authorisation was given
 - another Consumer Data Rule provides that authorisation expires, or

³⁶ Consumer Data Rule 1.7(1) (Definitions).

- the accreditation of the accredited person to whom the data holder is authorised to disclose is revoked or surrendered.

Consumer Experience Guidelines

- B.81 The ‘Consumer Experience Guidelines’ (or CX Guidelines) are data standards made by the Data Standards Body and the Data Standards Chair.
- B.82 The Consumer Experience Guidelines set out guidelines for best practice design patterns to be used by entities seeking consent from consumers under the CDR.
- B.83 The Consumer Experience Guidelines cover:
- the process and decision points that a consumer steps through when consenting to share their data
 - what (and how) information should be presented to consumers to support informed decision making, and
 - language that should be used (where appropriate) to ensure a consistent experience for consumers across the broader CDR ecosystem.
- B.84 The Consumer Experience Guidelines contain supporting examples illustrating how the Consumer Experience Guidelines can be implemented.
- B.85 The Consumer Experience Guidelines are available on CSIRO’s Data61 Consumer Data Standards website, www.consumerdatastandards.org.au.

Data holder

- B.86 A person is a data holder of CDR data if the person holds CDR data, is not a designated gateway for the data, began to hold the data after the earliest holding day, and any of the three cases below apply:³⁷
- The person is specified or belongs to a class of persons specified in a designation instrument and the CDR data or other CDR data from which the CDR data was directly or indirectly derived was not disclosed to the person under the Consumer Data Rules.³⁸
 - The CDR data or other CDR data from which the CDR data was directly or indirectly derived was not disclosed to the person under the Consumer Data Rules and the person is an accredited data recipient of other CDR data.³⁹
 - The CDR data or other CDR data from which the CDR data was directly or indirectly derived was disclosed to the person under the Consumer Data Rules, the person is an accredited person and the conditions specified in the Consumer Data Rules are met.

³⁷ 56AJ(1) and Consumer Data Rules 1.7(1) and 1.7(3).

³⁸ For example, the person is an accredited data recipient of that CDR data or is an outsourced service provider to whom the CDR data was disclosed under Consumer Data Rule 4.8(2).

³⁹ 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.

Earliest holding day

- B.87 A designation instrument must specify the ‘earliest holding day’ for a particular sector. This is the day on which data held by an entity may be CDR data.⁴⁰
- B.88 Under the designation instrument for the banking sector, the earliest holding day is 1 January 2017.⁴¹

Data minimisation principle

- B.89 The data minimisation principle limits the scope and amount of CDR data an accredited person may collect and use.
- B.90 An accredited person collects and uses CDR data in compliance with the data minimisation principle if:⁴²
- a. when making a consumer data request on behalf of a CDR consumer, the person does not seek to collect:
 - i. more CDR data than is reasonably needed, or
 - ii. CDR data that relates to a longer time period than is reasonably required in order to provide the goods or services requested by the CDR consumer and
 - b. the person does not use the collected data or derived data beyond what is reasonably needed in order to provide the requested goods or services.
- B.91 The test is one of purpose and proportionality. An accredited person may only seek to collect or use CDR data for the purpose of providing the requested goods or services, and the CDR data sought or used must be reasonably needed (i.e. proportional) for that purpose.
- B.92 It is not sufficient that the data is used or sought for the purpose of providing the requested goods or services. CDR data may be used or sought for the purpose of providing the requested goods or services, at the same time as being disproportionate to that purpose. For example, the amount of data sought or the number of data holders it is sought from may not be proportionate for that purpose.

Data standards

- B.93 A ‘data standard’ is a standard made in writing and published on the internet⁴³ by the Data Standards Chair of the Data Standards Body as appointed by the Treasurer.
- B.94 Data standards are about:
- the format and description of CDR data
 - the disclosure of CDR data

⁴⁰ 56AJ(1)(b).

⁴¹ 5(3).

⁴² Consumer Data Rule 1.8.

⁴³ 56FC.

- the collection, use, accuracy, storage, security and deletion of CDR data
- de-identifying CDR data, or
- other matters prescribed by regulations.⁴⁴

B.95 The current data standards are available on CSIRO’s Data61 Consumer Data Standards website, consumerdatastandards.org.au/.

Designated gateway

B.96 A ‘designated gateway’ is a person is specified in a legislative instrument made under s 56AC(2) of the Competition and Consumer Act.⁴⁵

B.97 There are currently no designated gateways in the CDR regime.

Designation Instrument

B.98 A ‘designation instrument’ is a legislative instrument made by the Minister under section 56AC(2) of the Competition and Consumer Act.⁴⁶

B.99 A designation instrument designates a sector of the Australian economy for the purposes of the CDR regime by specifying classes of information that can be transferred under the CDR, among other things.

B.100 These guidelines use ‘designation instrument’ to refer to the designation instrument for the banking sector (the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019), dated 4 September 2019.

Disclosure

B.101 ‘Disclosure’ is not defined in the Competition and Consumer Act or the Privacy Act.

B.102 Under the CDR regime ‘disclose’ takes its ordinary, broad meaning as it does under the Privacy Act.⁴⁷

B.103 An entity discloses CDR data when it makes the data accessible or visible to others outside the entity and releases the subsequent handling of the data from its effective control. 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 regime, can occur even where the data is already held by the recipient.⁴⁸

B.104 ‘Disclosure’ is a separate concept from:

- ‘Unauthorised access’ which is addressed in Privacy Safeguard 12. An entity is not taken to have disclosed CDR data where a third party intentionally exploits the entity’s

⁴⁴ 56FA(1).

⁴⁵ 56AL.

⁴⁶ 56AM(1).

⁴⁷ See OAIC, [Australian Privacy Principles Guidelines \(22 July 2019\)](#), Chapter B: Key Concepts [B.63 – B.69].

⁴⁸ For a similar approach to interpreting ‘disclosure’, see *Pratt Consolidated Holdings Pty Ltd v Commissioner of Taxation* [2011] AATA 907, [112]–[119].

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.139-B.140 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.105 ‘Eligible’ CDR consumers are discussed above at paragraphs B.51-B.54.

Outsourced service provider

B.106 The Consumer Data Rules provide that an ‘outsourced service provider’ is a person to whom an accredited person discloses CDR data under a ‘CDR outsourcing arrangement’.⁴⁹

B.107 A third-party service provider will not be an ‘outsourced service provider’ if data is not ‘disclosed’ to them.

CDR outsourcing arrangement

B.108 A person discloses CDR data to another person under a ‘CDR outsourcing arrangement’ if it does so under a written contract between the discloser and the recipient under which:⁵⁰

- the recipient will provide, to the discloser, goods or services using CDR data
- the recipient must take the steps in Schedule 2 of the Consumer Data Rules to protect CDR data disclosed to it by the outsourcer as if it were an accredited data recipient
- the recipient must not use or disclose any such CDR data other than in accordance with the contract
- the recipient must not disclose such CDR data to another person otherwise than under a CDR outsourcing arrangement, and if it does so, it must ensure that the other person complies with the requirements of the CDR outsourcing arrangement, and
- the recipient must, if directed by the discloser:
 - delete (in accordance with the CDR data deletion process) or return to the discloser any CDR data disclosed to it by the outsourcer
 - provide to the discloser records of any deletion that are required to be made under the CDR data deletion process, and
 - direct any other person to which it has disclosed CDR data to take corresponding steps.

B.109 A CDR outsourcing arrangement requires the recipient to provide goods or services using CDR data. This means that, if an accredited person has an arrangement with a third party

⁴⁹ Consumer Data Rule 1.7(1) (Definitions) and 1.10.

⁵⁰ Consumer Data Rule 1.7(1) (Definitions) and 1.10.

service provider in respect of collected CDR data but the third party does not use the CDR data to provide goods or services, the third party will not fall under the definition of ‘outsourced service provider’ and cannot be disclosed CDR data under the Consumer Data Rules.

Purpose

- B.110 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.⁵¹
- B.111 The purpose of an act is the reason or object for which it is done.
- B.112 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.⁵² 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.

Reasonable, Reasonably

- B.113 ‘Reasonable’ and ‘reasonably’ are used in the privacy safeguards and Consumer Data Rules to qualify a test or obligation. An example is that a ‘CDR consumer’ is a person who is identifiable or ‘reasonably’ identifiable from certain CDR data or related information.⁵³
- B.114 ‘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.115 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.⁵⁴ What is reasonable can be influenced by current standards and practices.
- B.116 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’,⁵⁵ and ‘involves an evaluation of the known facts, circumstances and considerations which may bear rationally upon the issue in question’.⁵⁶ There may be a conflicting range of objective circumstances to be considered, and the factors in support of a conclusion should outweigh those against.

⁵¹ 4F(1)(b).

⁵² 4F.

⁵³ 56AI(3)(c).

⁵⁴ 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).

⁵⁵ *George v Rockett* (1990) 170 CLR 104, 112.

⁵⁶ *McKinnon v Secretary, Department of Treasury* (2006) 228 CLR 423, 430 (Gleeson CJ & Kirby J).

Reasonable steps

- B.117 The ‘reasonable steps’ test is an objective test and is to be applied in the same manner as ‘reasonable’ and ‘reasonably’.
- B.118 An entity must be able to justify that reasonable steps were taken.

Redundant data

- B.119 CDR data is ‘redundant data’ if the data is collected by an accredited data recipient under the CDR regime and:
- the entity no longer needs any of the data for a purpose permitted under the Consumer Data Rules or for a purpose for which the entity may use or disclose it under Division 5 of the Competition and Consumer Act.
 - the entity is not required to retain the data by or under an Australian law or court/tribunal order and the data does not relate to any current or anticipated legal or dispute resolution proceedings to which the entity is a party.⁵⁷

Required consumer data

- B.120 CDR data is ‘required consumer data’ if it is required to be disclosed by a data holder to:
- a CDR consumer in response to a valid consumer data request under Consumer Data Rule 3.4(3), or
 - an accredited person in response to a consumer data request under Consumer Data Rule 4.6(4).
- B.121 ‘Required consumer data’ for the banking sector is defined in paragraph 3.2 of Schedule 3 to the Consumer Data Rules.⁵⁸

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

Australian law

- B.122 ‘Australian law’ has the meaning given to it in the Privacy Act. It means:
- an Act of the Commonwealth, or of a State or Territory
 - regulations or any other instrument made under such an Act
 - a Norfolk Island enactment, or

⁵⁷ 56EO(2).

⁵⁸ 3.2(3) of Schedule 3 of the Consumer Data Rule sets out what CDR data will be neither required consumer data nor voluntary consumer data.

- a rule of common law or equity.⁵⁹

Court/tribunal order

- B.123 ‘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.⁶⁰
- B.124 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.125 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.126 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.127 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.128 A person that 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.129 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.130 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 committed⁶¹ 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.131 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 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.⁶²

⁵⁹ Privacy Act, s 6(1).

⁶⁰ Privacy Act, s 6(1).

⁶¹ For example, section 316(1) of the *Crimes Act 1900* (NSW).

⁶² See *Coco v The Queen* (1994) 179 CLR 427.

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

Required

- B.132 A data holder is ‘required’ to disclose CDR data under the Consumer Data Rules:
- in response to a valid consumer data request under Consumer Data Rule 3.4(3), subject to Consumer Data Rule 3.5
 - in response to a consumer data request from an accredited person on behalf of a CDR consumer under Consumer Data Rule 4.6(4), subject to Consumer Data Rule 4.7, where the data holder has a current authorisation to disclose the data from the CDR consumer and
 - in response to a product data request under Consumer Data Rule 2.3(1), subject to Consumer Data Rule 2.5, where a data holder is required to disclose required product data under Consumer Data Rule 2.4(3) (however the privacy safeguards do not apply to required product data).
- B.133 An accredited data recipient is never ‘required’ to disclose CDR data under the Consumer Data Rules.

Authorised

- B.134 A data holder may be ‘authorised’ to disclose CDR data to an accredited person by a CDR consumer.⁶³ Such an authorisation must be in accordance with Division 4.4 of the Consumer Data Rules.
- B.135 A data holder is also authorised to disclose voluntary product data in response to a product data request under Consumer Data Rule 2.4(2), however the privacy safeguards do not apply to required product data.
- B.136 An accredited data recipient is ‘authorised’ to disclose CDR data under the Consumer Data Rules:
- to the CDR consumer under Consumer Data Rule 7.5(1)(c)
 - to an outsourced service provider under Consumer Data Rule 7.5(1)(d), and
 - to a third party if the CDR data is de-identified, under Consumer Data Rule 7.5(1)(e).

Required product data

- B.137 In the banking sector, ‘required product data’ means CDR data for which there are no CDR consumers, and which is:⁶⁴
- within a class of information specified in the banking sector designation instrument

⁶³ Consumer Data Rule 4.5.

⁶⁴ 3.1(1) of Schedule 3 to the Consumer Data Rules

- about the eligibility criteria, terms and conditions, price, availability or performance of a product
- publicly available, in the case where the CDR data is about availability or performance
- product specific data about a product, and
- held in a digital form.

B.138 The privacy safeguards do not apply to required product data.⁶⁵

Use

B.139 ‘Use’ is not defined in the Competition and Consumer Act. ‘Use’ is a separate concept from disclosure, which is discussed at paragraphs B.101-B.104 above.

B.140 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.

Voluntary consumer data

B.141 ‘Voluntary consumer data’ is CDR data a data holder may disclose to a CDR consumer under Consumer Data Rule 3.4(2) or to an accredited person under Consumer Data Rule 4.6(2).

B.142 For the banking sector, ‘voluntary consumer data’ is CDR data that is not required consumer data and for which there is a CDR consumer.⁶⁶

B.143 An example of voluntary consumer data is ‘materially enhanced information’, which is excluded from a specified class of information under section 10 of the Designation Instrument for the banking sector,⁶⁷ but may nonetheless be CDR data (as it is data derived from a specified class of information in the relevant designation instrument).

⁶⁵ 56EB(1).

⁶⁶ 3.2(2) of Schedule 3 of the Consumer Data Rules. 3.2(3) of Schedule 3 of the Consumer Data Rule sets out what CDR data will be neither required consumer data nor voluntary consumer data.

⁶⁷ Section 10 carves out information about the use of a product from being specified under section 7 where that information has been materially enhanced. Section 10(3) sets out, for the avoidance of doubt, information which is *not* materially enhanced information.

Voluntary product data

B.144 In the banking sector, ‘voluntary product data’ means CDR data for which there are no CDR consumers:

- that is within a class of information specified in the banking sector designation instrument
- that is product specific data about a product, and
- that is not required product data.⁶⁸

B.145 The privacy safeguards do not apply to voluntary product data.⁶⁹

⁶⁸ 3.1(2) of Schedule 3 to the Consumer Data Rules

⁶⁹ 56EB(1).

Chapter C:

Consent —

The basis for collecting and using CDR data

Consultation draft, October 2019

Contents

Key points	3
Why is it important?	3
How is consent in the CDR regime different to the Privacy Act?	3
How does consent fit into the CDR regime?	4
Consents to collect and use CDR data	6
Requirements for asking for consent	6
General processes	6
Where voluntary consumer data is involved	7
Name and accreditation number	8
Data minimisation principle	8
Disclosure to outsourced service providers	9
Withdrawal of consent	9
Treatment of redundant data	9
De-identification of CDR data	10
Restrictions on seeking consent	11
How consents to collect and use CDR data must be managed	12
Consumer dashboards	12
Withdrawal of consent	13
Expiry of consent	14

Key points

- An accredited person may only collect and use Consumer Data Right (CDR) data with the consent of the consumer.
- An accredited person must ask for a consumer’s consent in accordance with the Consumer Data Rules, which seek to ensure that a consumer’s consent is voluntary, express, informed, specific as to purpose, time limited and easily withdrawn.
- An accredited person’s processes for asking for 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.

Why is it important?

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

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

- C.3 It is important to understand how consent in the CDR regime differs from consent under the *Privacy Act 1988* (Cth) (the Privacy Act).
- C.4 The CDR regime requires express consent from consumers for the collection and use of their CDR data. Consent must meet the requirements set out in the Consumer Data Rules. Without express consent, the accredited person is not able to collect or use CDR data.
- C.5 However, under the Privacy Act, consent is not the only basis upon which an entity may collect or use personal information.¹ In addition, where consent is involved, the consent can be either express or implied.²
- C.6 The Consumer Data Rules contain specific requirements for the accredited person’s processes for seeking consent in the CDR regime, as well as for information that must be presented to a consumer when they are being asked to consent.
- C.7 The requirements by which an accredited person must seek consent from a consumer are discussed in this Chapter.

¹ 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 [Chapter 3: APP 3 – Collection of solicited personal information](#) and [Chapter B: Key Concepts](#) of the OAIC Australian Privacy Principles Guidelines (22 July 2019),

² See s 6(1) of the Privacy Act and [Chapter B: Key Concepts](#) of the OAIC Australian Privacy Principles Guidelines.

How does consent fit into the CDR regime?

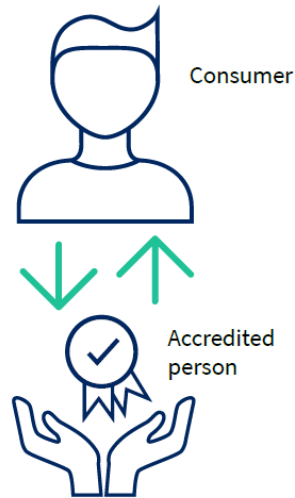
- C.8 Consent is the only basis on which an accredited person may collect and use CDR data.
- C.9 Where an accredited person:
- offers a good or service through the CDR regime and
 - needs to access a consumer's CDR data in order to provide such goods or services,
- the accredited person must obtain the consumer's consent to the collection and use of their CDR data to provide the good or service.
- C.10 An accredited person may only collect data in response to a 'valid request' from the consumer. The consumer's consent to the collection and use of their CDR data is a fundamental component of the 'valid request'.
- C.11 Upon obtaining a 'valid request' from the consumer, the accredited person may seek to collect the consumer's CDR data from the relevant data holder/s of the CDR data. The accredited person collects this CDR data by making a 'consumer data request' to the relevant data holder/s.³
- C.12 [Privacy Safeguard 3](#) prohibits an accredited person from seeking to collect data under the CDR regime unless it is in response to a 'valid request' from the consumer.
- C.13 Consent also underpins how an accredited person may use CDR data under [Privacy Safeguard 6](#). An accredited person may only use or disclose CDR data in accordance with a current consent from the consumer.⁴

³ For information regarding 'valid requests' and 'consumer data requests', see [Chapter 3 \(Privacy Safeguard 3\)](#). See also the flow chart underneath paragraph C.13 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.

⁴ One way in which an accredited person is authorised to use or disclose CDR data under the Consumer Data Rules is to provide goods or services requested by the consumer. This must be done in compliance with the data minimisation principle and in accordance with a current consent from the consumer (Consumer Data Rule 7.5(1)(a)). For further information, see [Chapter 6 \(Privacy Safeguard 6\)](#).

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, for up to 12 months
- Consumer provides their express consent

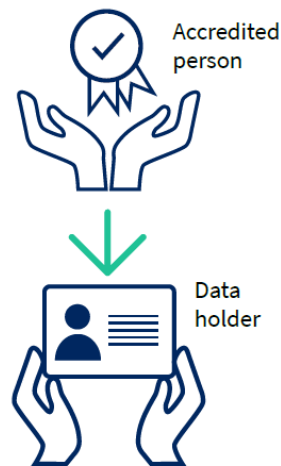


The consumer has given the accredited person a valid request



Making a consumer data request on behalf of the consumer

- Consumer gives accredited person a valid request
- Accredited person asks the data holder to disclose the consumer's CDR data
- Accredited person requests the data using the data holder's 'accredited person request service'



Data holder sends consumer data to accredited data recipient



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

Consents to collect and use CDR data

- C.14 An accredited person must ask the consumer to give consent to collect and use CDR data in accordance with Division 4.3 of the Consumer Data Rules.
- C.15 The requirements in Division 4.3 are outlined below under ‘Requirements for asking for consent’, ‘Restrictions on seeking consent’ and ‘How consents to collect and use CDR data must be managed’.
- C.16 The Consumer Data Rules state that the objective of Division 4.3 is to ensure that consent given by a consumer to collect and use CDR data is voluntary, express, informed, specific as to purpose, time limited and easily withdrawn.⁵
- C.17 In obtaining a valid request from a consumer, an accredited person must comply with requirements⁶ relating to:
- an accredited person’s processes for asking for consent⁷
 - information to be presented to the consumer when asking for consent⁸
 - restrictions on seeking consent⁹
 - providing information, including in relation to withdrawal¹⁰ and expiry of consent.¹¹
- C.18 Where a consumer is a business¹² and wishes to use the accredited person’s good or service through the CDR regime, 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.¹³ Importantly, the CDR regime currently extends only to business accounts in an individual’s name.

Requirements for asking for consent

General processes

- C.19 An accredited person’s processes for asking for consent must:
- accord with the data standards and

⁵ Consumer Data Rule 4.9. The explanatory statement to the Rules states that while the CDR regime places a high threshold on consent, it is not intended to make consent so complex as to discourage participation in the CDR regime. The focus of consents to collect and use should be on transparency and ensuring consumers understand the potential consequences of what they are agreeing to.

⁶ in Subdivision 4.3.2 of the Consumer Data Rules.

⁷ Consumer Data Rule 4.10.

⁸ Consumer Data Rule 4.11.

⁹ Consumer Data Rule 4.12.

¹⁰ Consumer Data Rule 4.13.

¹¹ Consumer Data Rule 4.14.

¹² And more broadly, where a consumer is not a natural person (i.e. they are a legal person).

¹³ An entity is entitled, under s 128 of the *Corporations Act 2001* (Cth), to make the assumptions set out in s 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.

- be as easy to understand as practicable, including by using concise language and, where appropriate, visual aids.¹⁴
- C.20 In ensuring processes are easy to understand, an accredited person should, at a minimum, be guided by the language and processes of the [Consumer Experience Guidelines](#).¹⁵
- C.21 An accredited person must not:
- include or refer to other documents so as to reduce comprehensibility in seeking consent: this makes the consent harder to understand.
 - bundle consents with other consents or permissions¹⁶: this practice has the potential to undermine the voluntary nature of the consent.
- C.22 Each time an accredited person seeks a consumer’s consent, they must allow the consumer to actively select or clearly indicate:¹⁷
- the particular types of CDR data to which they are consenting
 - the specific uses of that CDR data
 - whether the data will be:
 - collected on a single occasion and used over a specified period of time (not exceeding 12 months) or
 - collected on an ongoing basis and used over a specified period of time (not exceeding 12 months).
- C.23 Each time an accredited person seeks a consumer’s consent, they must also:
- ask for the consumer’s express consent for the selections in paragraph C.22 above
 - ask for the consumer’s express consent to any direct marketing they intend to undertake, and
 - not pre-select these options.¹⁸

Where voluntary consumer data is involved

- C.24 If a consumer’s request covers voluntary consumer data,¹⁹ the data holder may decide to charge the accredited person a fee. If the accredited person intends to pass on the fee to the consumer, the accredited person must make this clear to the consumer.
- C.25 To do this, the accredited person must:
- clearly distinguish between the required consumer data and the voluntary consumer data they are seeking to collect

¹⁴ Consumer Data Rule 4.10

¹⁵ Consumer Data Rule 4.10. The ‘Consumer Experience Guidelines’ provide best practice interpretations of the Consumer Data Rules relating to consent and are discussed in [Chapter B \(Key Concepts\)](#).

¹⁶ Consumer Data Rule 4.10. Bundled consent refers to the ‘bundling’ together of multiple requests for consumer’s consent to a wide range of collections and uses of CDR data, without giving the consumer the opportunity to choose which collections and uses they agree to and which they do not.

¹⁷ Consumer Data Rule 4.11(1)(b) and 4.12(1).

¹⁸ Consumer Data Rule 4.11.

¹⁹ For information regarding ‘required consumer data’ and ‘voluntary consumer data’, see [Chapter B, Key Concepts](#).

- inform the consumer of the amount of the fee, and the consequences if the consumer does not consent to the collection of the voluntary consumer data and
- allow the consumer to actively select or otherwise clearly indicate whether they consent to the collection of that data.

Name and accreditation number

- C.26 The accredited person must ensure that their name is clearly displayed in the consent request.
- C.27 The accredited person's accreditation number must also be included in the consent request.²⁰ This number has been assigned to the accredited person by the Data Recipient Accreditor.
- C.28 For more information on the Data Recipient Accreditor and the accreditation process and conditions, see the ACCC's [Accreditation Guidelines](#).

Data minimisation principle

- C.29 Collection of CDR data is limited by the data minimisation principle,²¹ which provides that an accredited person:
- must not collect more data than is reasonably needed in order to provide the requested goods or services, including over a longer time period than is reasonably required, 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.²²

Example: An accredited person is responding to a 'valid request' from a 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 is in breach of the data minimisation principle.

- C.30 The accredited person must explain how their collection and use is in line with the data minimisation principle.²³
- C.31 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.²⁴
- For example, the accredited person must explain how the data is necessary to deliver the service they are providing.²⁵

²⁰ Consumer Data Rule 4.11(3).

²¹ Consumer Data Rule 4.12(2).

²² Consumer Data Rule 1.8.

²³ For further information regarding the data minimisation principle, see [Chapter B Key Concepts](#).

²⁴ Consumer Data Rule 4.11(3)(c)(i)

²⁵ Consumer Data Rule 4.11(3)(c).

C.32 The accredited person must also explain the reason for the data collection period. The collection period must be no longer than is ‘reasonably required’ to provide the goods or services.²⁶

- This means that the accredited recipient 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 consumer at the point of consent.

C.33 The accredited person must also explain that they will not use the CDR data beyond what is reasonably needed to provide the relevant goods or services.²⁷

Disclosure to outsourced service providers

C.34 Where the accredited person might disclose the consumer’s CDR data to an outsourced service provider²⁸ (including one that is based overseas), the accredited person must:

- tell the consumer that the accredited person will disclose the consumer’s CDR data to an outsourced service provider
- provide the consumer with a link to the accredited person’s CDR policy, noting that further information about disclosures to outsourced service providers can be found in that policy.²⁹

Withdrawal of consent

C.35 The accredited person must explain to the consumer:

- that their consent can be withdrawn at any time
- how to withdraw consent
- the consequences (if any) of withdrawing consent, including what will happen to redundant CDR data.³⁰

Treatment of redundant data

C.36 The accredited person must tell the consumer whether the accredited person has a general policy of:

- deleting redundant data
- de-identifying redundant data or

²⁶ Consumer Data Rule 4.11(3)(c)(i)

²⁷ Consumer Data Rule 4.11(3)(c)(ii)

²⁸ For further information regarding outsourced service providers, see [Chapter B Key Concepts](#).

²⁹ Consumer Data Rule 4.11(f). An accredited person’s CDR policy must include, amongst other things, a list of outsourced service providers, the nature of their services, the CDR data and classes of CDR data that may be disclosed. For further information, see [Chapter 1 \(Privacy Safeguard 1\)](#).

³⁰ Consumer Data Rule 4.11(g).

- deciding, when the CDR data becomes redundant, whether to delete or de-identify the redundant data.³¹

C.37 Where the accredited person will³² or may³³ de-identify redundant data, the accredited person must also:

- allow the consumer to elect for their redundant CDR data to be deleted,³⁴ including by outlining the consumer's right to elect for this to occur and providing instructions for how the consumer can make the election³⁵
- tell the 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 means³⁶
- tell the 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 consumer³⁷ and
- if applicable, provide the consumer with examples of how the accredited person could use the redundant data once de-identified.³⁸

C.38 See [Chapter 12 \(Privacy Safeguard 12\)](#) for further information on the treatment of redundant data (i.e. destruction or de-identification).

De-identification of CDR data

C.39 Where an accredited person is asking for the consumer's consent to de-identify some or all of the CDR data for the purpose of disclosing (including by selling) the de-identified data, the accredited person must tell the consumer:

- what the CDR de-identification process is³⁹
- that the accredited person would disclose (for example, by sale) the de-identified data to one or more other persons
- 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)
- 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)

³¹ Consumer Data Rule 4.11(h).

³² That is, because the accredited person communicated (when seeking consent) a general policy of de-identifying redundant CDR data.

³³ 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.

³⁴ Consumer Data Rule 4.11(1)(e), 4.16. The accredited person must allow the consumer to make this election when providing their consent to the accredited person collecting and using their CDR data, and at any other point in time before the consent expires (4.16(1)).

³⁵ Consumer Data Rule 4.11(h).

³⁶ Consumer Data Rule 4.17(2)(a), 4.17(2)(b).

³⁷ Consumer Data Rule 4.17(2)(a).

³⁸ Consumer Data Rule 4.17(2)(c).

³⁹ More information on this requirement is in [Chapter 12 \(Privacy Safeguard 12\)](#).

- that the consumer would not be able to elect to have the de-identified data deleted once it becomes redundant data.

C.40 Where the accredited person is seeking consent to de-identify some or all of the consumer's CDR data for the purpose of disclosing (including by selling) the de-identified data, the accredited person must explain how the collection and use (i.e. de-identification) of the CDR data is in line with the data minimisation principle (see paragraphs C.30–C.33 above).

C.41 This necessarily involves explaining how de-identification and disclosure of the consumer's CDR data is reasonably needed to provide the goods or services to the consumer.⁴⁰

Restrictions on seeking consent

C.42 Consumer Data Rule 4.12 provides that when seeking consent from a consumer, an accredited person must not ask for consent to:⁴¹

- collect and use CDR data for a period exceeding 12 months
- collect or use the data in a manner that is in breach of the data minimisation principle⁴²
- sell the CDR data (unless the CDR data will be de-identified in accordance with the prescribed de-identification process, and the accredited person has complied with the requirements in paragraphs C.39–C.41 above)
- 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.⁴³

C.43 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 consumer who is providing the consent. This is permitted where:

- 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.

⁴⁰ This is because an accredited person is required under Consumer Data Rule 4.11(3)(c) to indicate how it would comply with the data minimisation principle in relation to CDR data it seeks consent to de-identify. See paragraphs C.30–C.33 above. See [Chapter 12 \(Privacy Safeguard 12\)](#) for information about de-identification.

⁴¹ Consumer Data Rule 4.12.

⁴² The data minimisation principle is discussed in [Chapter B \(Key Concepts\)](#), and at paragraph C.29 above.

⁴³ 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.

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 to collect and use CDR data must be managed

Consumer dashboards

- C.44 An accredited person must provide a consumer dashboard for each consumer who has provided consent to the collection and use of their CDR data.
- C.45 An accredited person's consumer dashboard is an online service that can be used by each consumer to manage consumer data requests⁴⁴ and associated consents for the accredited person to collect and use CDR data.
- C.46 The consumer dashboard must contain the following details of each consent to collect and use CDR data that has been given by the consumer:⁴⁵
- the CDR data to which the consent relates
 - the specific use or uses for which the consumer has given consent
 - when the consumer gave consent
 - whether the consent was for the collection of CDR data on a single occasion or over a period of time
 - if the consumer consented to collection of CDR data over a period of time – what that period is and how often data has been (and is expected to be) collected over that period
 - if the consent is current – when it will expire
 - if the consent is not current – when it expired
 - what CDR data was collected
 - when the CDR data was collected
 - the data holder/s of the CDR data that was collected.
- C.47 The consumer dashboard must have a functionality that allows the consumer, at any time, to:
- withdraw consent
 - elect their CDR data be deleted once it becomes redundant
 - withdraw an election regarding whether their CDR data should be deleted once it becomes redundant.

⁴⁴ See [Chapter B \(Key Concepts\)](#).

⁴⁵ Consumer Data Rule 1.14(3).

- C.48 These functionalities must be simple and straightforward to use, and prominently displayed.
- C.49 For examples of how to present this information on the consumer dashboard, and other best practice recommendations relating to the consumer dashboard, see the [Consumer Experience Guidelines](#).

Withdrawal of consent

- C.50 A consumer who has given consent for an accredited person to collect and use their CDR data may withdraw the consent at any time.
- C.51 The main consequence of the withdrawal of consent is that the consent expires,⁴⁶ and 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).⁴⁷
- C.52 A consumer may withdraw consent by communicating the withdrawal in writing to the accredited person or by using the accredited person's consumer dashboard.⁴⁸
- C.53 For examples of how to implement the withdrawal functionality on the consumer dashboard, and other best practice recommendations relating to the withdrawal functionality of the consumer dashboard, see the [Consumer Experience Guidelines](#).⁴⁹
- C.54 If a consumer withdraws consent using the accredited person's consumer dashboard, the automatic processes required by the data standards mean that the withdrawal is immediately effective.
- C.55 If a withdrawal is not communicated over the consumer dashboard, the accredited person must give effect to the withdrawal as soon as practicable, but not more than two business days after receiving the communication. This communication may be by electronic means such as email, or non-electronic means such as by post.
- C.56 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.57 An accredited person 'gives effect' to the withdrawal by ensuring that the same processes and procedures have occurred in relation to the withdrawal of that consent through writing as if the withdrawal had been effected through the consumer dashboard.⁵⁰

⁴⁶ 4.26(1)(b).

⁴⁷ More information on 'redundant data' and the requirement to destroy or de-identify redundant data is in [Chapter 12 \(Privacy Safeguard 12\)](#).

⁴⁸ 4.13.

⁴⁹ For example, if an accredited data recipient does not have a general policy of deleting redundant data, and the consumer has not already requested that their redundant data be deleted, the accredited recipient: must allow consumers to elect to have their redundant data deleted prior to the final withdrawal step; and should consider prompting consumers to exercise their right to elect to have their redundant data deleted at appropriate times (e.g. when inaction on the part of the consumer may cause them to lose the opportunity to exercise this right).

⁵⁰ The accredited person's consumer dashboard must have a functionality that allows a consumer to withdraw consents: Rule 1.14(c)(i)(A).

- C.58 ‘Giving effect’ to the withdrawal includes updating the consumer dashboard to reflect that the consent has expired,⁵¹ as required by Consumer Data Rule 4.19.⁵²
- C.59 Where a consumer has elected for their CDR data to be deleted upon becoming redundant data, their withdrawal of consent will not affect this election.⁵³
- C.60 For examples of how to present this information on the consumer dashboard, and other best practice recommendations relating to the consumer dashboard, see the [Consumer Experience Guidelines](#).

Expiry of consent

- C.61 Where a consent expires, 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.⁵⁴
- C.62 Consumer Data Rule 4.14 provides that consent expires in the following circumstances:
- **If the consent is withdrawn:** if a withdrawal notice is given via the consumer dashboard, the consent expires immediately.⁵⁵ Where withdrawal is not given through the consumer dashboard, the consent expires when the accredited person gives effect to the withdrawal, or two business days after receiving the communication, whichever is sooner.⁵⁶
 - **When the accredited person is notified by the data holder of the withdrawal of authorisation:** upon notification from the data holder that the consumer has withdrawn authorisation, the consent expires immediately.⁵⁷
 - **At the end of the period of consent (no longer than 12 months after consent was given):** consent expires at the end of the specified period for which the consumer gave consent for the accredited person to collect and use the CDR data. This specified period cannot be longer than 12 months.⁵⁸
 - **If another Consumer Data Rule provides that consent expires:** for example, a consent to collect CDR data expires once a person becomes a data holder rather than an accredited data recipient for the CDR data⁵⁹ or

⁵¹ See Consumer Data Rule 1.14(3)(g).

⁵² Consumer Data 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.

⁵³ Consumer Data Rule 4.13(3) provides that withdrawal of consent does not affect an election under Consumer Data Rule 4.16 that the consumer’s collected CDR data be deleted once it becomes redundant. Consumer Data Rule 4.16 is discussed in [Chapter 12 \(Privacy Safeguard 12\)](#).

⁵⁴ More information on ‘redundant data’ and the requirement to destroy or de-identify redundant data is in [Chapter 12 \(Privacy Safeguard 12\)](#).

⁵⁵ Consumer Data Rule 4.14(1)(b).

⁵⁶ Consumer Data Rule 4.14(1)(a).

⁵⁷ If the consumer has given the data holder an authorisation to disclose CDR data to the accredited person, and then withdraws that authorisation, the data holder must notify the accredited person under Consumer Data Rule 4.25(2).

⁵⁸ Consumer Data Rule 4.12(1). Consumer Data Rule 4.14(1)(d) reinforces this maximum duration by providing that consent expires after the 12 month period after the consent was given.

⁵⁹ As a result of clause 7.2(3)(a) of Schedule 3 to the Consumer Data Rules and section 56AJ(4).

- **If the accredited person's accreditation is revoked or surrendered:** consent expires when the revocation or surrender takes effect.⁶⁰

⁶⁰ For further information, see the [ACCC Consumer Data Right Draft Accreditation Guidelines](#).

Chapter 1:

Privacy Safeguard 1 —

Open and transparent management of CDR data

Consultation draft, October 2019

Contents

Key points	3
What does Privacy Safeguard 1 say?	3
Importance of open and transparent management of CDR data	3
Who Privacy Safeguard 1 applies to	3
How Privacy Safeguard 1 interacts with the Privacy Act and APP1	4
Summary of application of Privacy Safeguard 1 by CDR entity	4
Implementing practices, procedures and systems to ensure compliance with the CDR regime	5
Existing privacy governance arrangements	5
Examples of practices, procedures and systems	6
Circumstances that affect reasonable steps	8
The amount of CDR data handled by the CDR entity	8
Having a CDR policy	9
Developing the CDR policy	9
Information that must be included in a CDR policy	10
Availability of the CDR policy	13
Consumer requests for a CDR policy	13

Key points

- Privacy Safeguard 1, together with Consumer Data Rule 7.2, outlines the requirements for all Consumer Data Right (CDR) entities (accredited data recipients, data holders and designated gateways) to handle 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 regime, and are able to 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. The policy must be provided free of charge and made available in accordance with the Consumer Data Rules.

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 establish and maintain internal practices, procedures and systems that ensure compliance with the CDR regime, including the Privacy Safeguards and Consumer Data Rules and
- have a clearly expressed and up-to-date policy describing how they manage CDR data. The policy must be available free of charge and in a form consistent with the Consumer Data Rules and provided to the consumer upon request.

Importance of open and transparent management of CDR data

1.2 The objective of Privacy Safeguard 1 is to ensure CDR entities handle CDR data in an open and transparent way. It is the bedrock principle.

1.3 By complying with this Privacy Safeguard, CDR entities will be establishing an accountable and auditable practice procedures and systems that will assist in complying 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.

1.4 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.

Who Privacy Safeguard 1 applies to

1.5 Privacy Safeguard 1 applies to data holders, designated gateways and accredited data recipients.

How Privacy Safeguard 1 interacts with the Privacy Act and APP1

- 1.6 It is important to understand how Privacy Safeguard 1 interacts with the *Privacy Act 1988* (the Privacy Act) and Australian Privacy Principle (APP) 1.¹
- 1.7 Like Privacy Safeguard 1, APP 1 provides certain obligations that require APP entities to manage personal information in an open and transparent way (see [Chapter 1: Open and transparent management of personal information of the APP Guidelines](#)).

Summary of application of Privacy Safeguard 1 by CDR entity

CDR entity	Privacy principle that applies to CDR data
Accredited person	<p>Australian Privacy Principle 1 and Privacy Safeguard 1</p> <p>Privacy Safeguard 1 applies in parallel with APP 1. This means that accredited persons must, at all times, have systems, practices and procedures to comply with both the Privacy Safeguards and the APPs (including having both a CDR policy and Privacy Policy in place,) regardless of whether CDR data has been transferred.</p>
Accredited data recipient	<p>Privacy Safeguard 1</p> <p>Privacy Safeguard 1 applies instead of APP 1, meaning APP 1 will not apply to CDR data an accredited data recipient receives through the CDR regime.</p> <p>APP 1 will continue to apply to any personal information handled by the accredited data recipient that is not CDR data.² This is because all accredited data recipients are subject to the Privacy Act and the APPs for any personal information, even if it is not CDR data.</p>
Designated gateway	<p>Australian Privacy Principle 1 and Privacy Safeguard 1</p> <p>Privacy Safeguard 1 applies in parallel with APP 1. This means that a designated gateway must, at all times, 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), regardless of whether CDR data has been transferred.</p>
Data holder	<p>Australian Privacy Principle 1 and Privacy Safeguard 1</p> <p>Privacy Safeguard 1 applies in parallel with APP 1. This means that a data holder must, at all times, have systems, practices and procedures to comply with both the Privacy Safeguards and the APPs, and have a CDR policy and a Privacy Policy in place, regardless of whether CDR data has been transferred.</p>

¹ The Privacy Act includes 13 APPs that regulate the handling of personal information by APP entities. See Chapter B: Key concepts of the APP Guidelines for further information.

² See s 6E(1D) of the Privacy Act.

Implementing practices, procedures and systems to ensure compliance with the CDR regime

- 1.8 Privacy Safeguard 1 requires all CDR entities to take steps that are reasonable in the circumstances to establish and maintain internal practices, procedures and systems that:
- ensure compliance with the CDR regime, including the Privacy Safeguards and the Consumer Data Rules, and
 - enable the entity to deal with inquiries or complaints from consumers about the entity's compliance with the CDR regime, including the Privacy Safeguards and Consumer Data Rules.
- 1.9 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 regime.
- 1.10 The Consumer Data Rules contain several governance mechanisms, policies and procedures that will assist entities to take steps that are reasonable to comply with the CDR regime.³ However, while compliance with the Consumer Data Rules will assist entities to take steps that are reasonable, this does not of itself mean that the entity has complied with Privacy Safeguard 1.
- 1.11 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 Consumer Data Rules (including how these interact with other obligations). This should occur before the entity first starts participating in the CDR regime.
- 1.12 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 Consumer Data Rules in isolation or at a late stage risk unnecessary costs or inadequate solutions that fail to address the full compliance picture.

Privacy tip: Entities should embed 'privacy-by-design' in relation to handling CDR data across and within their organisation. This ensures CDR requirements are considered holistically. The OAIC has a range of tools to assist entities develop their wider privacy program, including the [Privacy management framework](#).

Existing privacy governance arrangements

- 1.13 Where an entity has existing privacy practices and procedures for personal information it handles under the Privacy Act, it may be appropriate to extend these to its CDR data.
- 1.14 However, the mere extension of current practices and procedures does not mean in and of itself that an entity has taken *reasonable steps* to implement practices, procedures and systems.

³ For example, accredited data recipients are required to establish a formal governance framework for managing information security risks under the Privacy Safeguard 12 Consumer Data Rules.

- 1.15 Entities will need to take further action to modify practices, procedures and systems to meet obligations under Privacy Safeguard 1 to ensure compliance with the particularities of the CDR regime.

Examples of practices, procedures and systems

- 1.16 The following are given as examples of practices, procedures and systems that a CDR entity should consider implementing under Privacy Safeguard 1.
- 1.17 These examples may overlap and interact with existing requirements set out by the Consumer Data Rules or the draft ACCC [CDR Accreditation Guidelines](#).

Have a CDR data management plan

- 1.18 In practice, CDR entities should develop a CDR management plan or CDR management framework which identifies goals and targets, appoints key roles and responsibilities for privacy management, and adopts governance mechanisms to bring their privacy planning together.
- 1.19 Entities should proactively review and audit the adequacy and currency of their organisational practices, procedures and systems involving CDR data.
- 1.20 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, or they may have a separate CDR management plan.
- 1.21 A CDR entity should also regularly review and update this CDR data management plan to ensure that it reflects the entity's CDR data privacy goals and handling practices.

What is a CDR data management plan?

A CDR data management plan can be a helpful way to identify specific, measurable goals and targets, and sets out how an entity will meet its compliance obligations under Privacy Safeguard 1. The CDR data management plan should also include processes to measure and document the CDR entity's performance against their CDR data management plan.

Embed a culture that respects and protects CDR data

- 1.22 Good CDR data management stems from good privacy governance. Entities should ensure leadership and governance arrangements create a culture of privacy that respects and protects CDR data.
- 1.23 To embed a culture of privacy, entities could:
- Appoint a member of senior management to be responsible for the strategic leadership and overall privacy 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 issues.

Establish robust and effective privacy practices, procedures and systems

1.24 Good privacy management requires the development and implementation of robust and effective practices, procedures and systems.

1.25 For example, an entity could:

- Implement risk management processes that allow identification, assessment and management of privacy risks, including CDR security risks.⁴
- Establish clear processes for reviewing and responding to CDR data complaints.
- Integrate Privacy Safeguards training into induction processes and provide regular staff training to those who deal with CDR data. This regular training should occur at a minimum once per year.⁵
- Establish processes that allow consumers to promptly and easily access and correct their CDR data, in accordance with the Consumer Data Rules.

Regularly reviewing and evaluating privacy processes

1.26 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.
- Measure performance against the CDR data management plan.
- Create feedback channels for both staff and consumers to continue to learn lessons from complaints and breaches, as well as customer feedback more generally.

Enhance response to privacy issues

1.27 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 organisation's practices, procedures and systems.
- Consider having practices, procedures and systems externally assessed to identify areas where privacy processes may be improved.⁶

⁴ Accredited data recipients are already required to meet strong minimum information security controls under Privacy Safeguard 12. See Schedule 2 of the Consumer Data Rules and the ACCC's *draft Supplementary accreditation guidelines: information security* available on the [ACCC's CDR draft accreditation guidelines page](#).

⁵ Accredited data recipients already have certain obligations to provide privacy and security training under Privacy Safeguard 12. See Schedule 2 of the Consumer Data Rules and the ACCC's *draft Supplementary accreditation guidelines: information security* available on the [ACCC's CDR draft accreditation guidelines page](#).

⁶ Accredited persons have obligations to provide regulate assurance reports (an audit report) and attestation statements concerning compliance with certain Privacy Safeguard 12 Consumer Data Rules. See the ACCC's *draft Supplementary accreditation guidelines: information security* available on the [ACCC's CDR draft accreditation guidelines page](#).

- Continuously monitor and address new privacy risks.

Circumstances that affect reasonable steps

- 1.28 The requirement to implement practices, procedures and systems is qualified by a ‘reasonable steps’ test.
- 1.29 This requires an objective assessment of what is considered reasonable in the specific circumstance, which could include:
- the Consumer Data Rules and other legislative obligations that apply to the CDR entity
 - the nature of the CDR entity
 - the amount of CDR data handled by the CDR entity
 - the possible adverse consequences for a consumer in the case of a breach
 - the practicability, including time and cost involved.

The CDR regime obligations that apply to the CDR entity

- 1.30 The CDR regime obligations (such as the Privacy Safeguards and the Consumer Data Rules) that apply to the entity will be relevant to determining what steps will be reasonable. For example, an accredited data recipient will need to put in place different mechanisms than a data holder to ensure it is compliant with the CDR regime.

Nature of the entity

- 1.31 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.
- 1.32 For instance, where a CDR entity uses outsourced service providers (such as cloud-based service providers for hosting services or data centres and backup providers), the reasonable steps it should take may be different to those it would take if it did not operate in this manner.

The amount of CDR data handled by the CDR entity

- 1.33 More rigorous steps may be required as the amount of CDR handled by a CDR entity increases. Generally, as the amount CDR data that is held increases, so too will the steps to ensure that it is reasonable.

Adverse consequences for a consumer

- 1.34 Entities should consider the possible adverse consequences for the consumers concerned if the CDR data is not handled in accordance with the CDR Regime. 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

- 1.35 The practicality of implementing, 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.
- 1.36 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.
- 1.37 CDR entities are also not excused from any specific processes, procedures or systems that are required by the CDR Regime.

Having a CDR policy

Developing the CDR policy

- 1.38 CDR policies are a key tool for ensuring open and transparent management of personal information which can build trust and engage consumers.
- 1.39 Privacy Safeguard 1 requires CDR entities to have a clearly expressed and up-to-date CDR policy about how they manage CDR data. The policy must be distinct from any of the CDR entity’s privacy policies,⁷ for example, by being contained in a separate document to the entity’s privacy policy.
- 1.40 At a minimum, a CDR policy should be clearly expressed. Specifically, it should be easy to understand (avoiding jargon, legalistic and in-house terms), easy to navigate, and only include information that is relevant to the management of CDR data by the entity.
- 1.41 A CDR entity must regularly review and update its CDR policy to ensure that it reflects the entity’s CDR data handling practices. This review should, at a minimum, be undertaken as part of annual planning processes. An entity could also:
 - include a notation on the policy indicating when it was last updated
 - invite comment on the policy to gain feedback and evaluate its effectiveness, and
 - explain how any comments will be dealt with.
- 1.42 As the Consumer Data Rules require a CDR policy to be available on the entity’s website and on an application for mobile device, it should be available in a style and length that makes it suitable for online and mobile friendly publication.
- 1.43 It is open to a CDR entity to choose the style and format for its CDR policy, so long as the policy is clearly expressed, up-to-date and otherwise compliant with the requirements of Privacy Safeguard 1 and the Consumer Data Rules. This may include the use of innovative formats to best communicate the privacy messaging to consumers, such as the use of infographics, animation or video or other forms of technology to increase user experience. However, when creating a CDR policy, entities should remember that the key objective is to be transparent with consumers about the handling of CDR data.

⁷ Rule 7.2(2).

- 1.44 Using a layered approach to provide the information may assist a consumer’s understanding of the information in the policy. A layered approach means providing a condensed version of the full policy to outline key information, with direct links to the more detailed information in the full policy.⁸

Information that must be included in a CDR policy

- 1.45 Privacy Safeguard 1 contains a non-exhaustive list of information that a CDR entity must include in its CDR policy. Additional requirements for each CDR entity are set out in the Consumer Data Rules.
- 1.46 There are different requirements depending on whether the CDR entity is an accredited data recipient, a data holder, or a designated gateway.
- 1.47 Where an entity occupies more than one role in the CDR regime (for example is both a data holder and an accredited data recipient), the entity can either have a single CDR policy that outlines how CDR data is handled in both capacities, or a separate CDR policy for each capacity.

Accredited data recipients

- 1.48 Privacy Safeguard 1 requires that accredited data recipients must include the following in their CDR policy:
- classes⁹ of CDR data held. *The Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019* (the Designation) sets out three classes of information for the banking sector: customer information¹⁰, product use information¹¹, and Information on the product¹².
 - how the CDR data is held
 - purposes for which an entity can collect, hold, use or disclose CDR data
 - how a consumer may access or correct CDR data
 - how a consumer can complain and how the entity will deal with a complaint
 - whether overseas disclosure is likely
 - circumstances in which the CDR entity may disclose CDR data to a person who is not an accredited person¹³
 - events about which the CDR entity will notify the consumers of such CDR data
 - when the entity must delete or de-identify CDR data in accordance with a request by a consumer.

⁸ For an example of a layered approach, see OAIC, Summary of the OAIC’s APP Privacy Policy, OAIC website <www.oaic.gov.au>.

⁹ The classes of information are set out in the designation instrument for the relevant sector.

¹⁰ Specified in section 6 of the [Designation](#)

¹¹ Specified in section 7 of the [Designation](#)

¹² Specified in section 8 of the [Designation](#)

¹³ An accredited data recipient is not authorised to disclose to any person who is not an accredited person except directly to the consumer, or where the person is an outsourced service provider

1.49 In addition, the Consumer Data Rules provide other matters that must be included in the CDR policy, including:

- A statement indicating the consequences to the consumer if they withdraw a consent to collect or to use CDR data. This could include information about any early cancellation fees.
- A list of outsourced service providers, the nature of their services, the CDR data and classes of CDR data that may be disclosed.
- Where the accredited data recipient is likely to disclose CDR data overseas to a service provider who is not accredited, a list of countries in which the overseas persons are likely to be based (if it is practicable to specify those countries in the policy).¹⁴
- Where the accredited data recipient proposes to store CDR data other than in Australia or an external territory, the countries in which the accredited data recipient proposes to store CDR data.
- Where the accredited data recipient seeks or intends that it will seek consent from consumers to de-identify their CDR data in accordance with Consumer Data Rule 4.11(3)(e):
 - why the accredited data recipient asks for consents to de-identify CDR data
 - how the accredited data recipient de-identifies CDR data, including a description of techniques that it uses to de-identify CDR data
 - if the accredited data recipient 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 accredited data recipient discloses de-identified CDR data.
- When and how the accredited data recipient destroys ‘redundant data’, and how a consumer may elect for the accredited data recipient to destroy their CDR data when it becomes redundant data.
- Where the accredited data recipient has a general policy of de-identifying CDR data once it becomes redundant data:
 - if the accredited data recipient uses the de-identified CDR data, examples of how the accredited data recipient ordinarily uses de-identified CDR data
 - how the accredited data recipient de-identifies CDR data, including a description of techniques that it uses to de-identify CDR data
 - if the accredited data recipient ordinarily discloses (by sale or otherwise) de-identified CDR data to one or more persons: the fact of this disclosure; the classes of

¹⁴ An example of when it may be impracticable to specify the countries in which service providers are likely to be located is where CDR data is likely to be disclosed to numerous overseas service providers and the burden of determining where those service providers are likely to be located is excessively time-consuming, costly or inconvenient in all the circumstances. However, an accredited data recipient is not excused from specifying the countries by reason only that it would be inconvenient, time-consuming or impose some cost to do so. It is the responsibility of the accredited data recipient to be able to justify that this is impracticable. If CDR data is disclosed to numerous overseas locations, one practical option may be to list those countries in an appendix to the CDR policy rather than in the body of the policy. Another option in these circumstances may be to include a link in the CDR policy to a regularly updated list of those countries, accessible from the accredited data recipient’s website. Where it is not practicable to specify the countries, the accredited data recipient could instead identify general regions (such as European Union countries).

persons such data is ordinarily disclosed to; and the purposes for which the accredited data recipient discloses de-identified CDR data.

- Further information regarding how a consumer can complain and how the accredited data recipient 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
 - options for review.

Data holder

1.50 Privacy Safeguard 1 requires that data holders must include in their CDR policy how a consumer can access and correct the CDR data, and how they may complain.

1.51 In addition, the Consumer Data Rules provide other matters that must be included in the CDR policy, including:

- 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 are¹⁵
- how a 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
 - complaint handling process, including time periods associated with the various stages
 - options for redress
 - options for review.

Designated gateway

1.52 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 Consumer Data Rules

¹⁵ Voluntary product data means CDR data for which there are no consumers that is not required product data: Consumer Data Rules Schedule 3, clause 3.1. Voluntary consumer data means CDR data for which there are consumers that is not required consumer data: Consumer Data Rules Schedule 3, clause 3.2.

- how a consumer may complain about a failure of the CDR entity to comply with the Privacy Safeguards or the Consumer Data Rules, and how the CDR entity will deal with such a complaint.

Availability of the CDR policy

- 1.53 The CDR policy must be publicly and freely available in accordance with the Consumer Data Rules.¹⁶ This furthers the objective of Privacy Safeguard 1 of ensuring that CDR data is managed in an open and transparent way.
- 1.54 The Consumer Data Rules provide that the CDR policy must be readily available on each online platform where the CDR entity ordinarily deals with consumers. For example, where an entity ordinarily deals with consumers through websites and mobile applications, the CDR policy must be readily available on each of the entity’s websites and each application for mobile device.
- 1.55 The CDR policy should be prominently displayed, accessible and easy to download. For example, a prominent link or icon, displayed on relevant pages of the entity’s website or mobile application, could provide a direct link to the CDR policy.
- 1.56 Appropriate accessibility measures should be put in place so that the policy may be accessed by consumers with special needs (such as consumers with a vision impairment, or consumers from a non-English speaking background). While these accessibility measures would not necessarily have to be available online or in a mobile application, there needs to be a clear and accessible method to contact to entity and request this information.

Consumer requests for a CDR policy

- 1.57 If a copy of the CDR entity’s policy is requested by a consumer for the CDR data, the CDR entity must give the consumer a copy in accordance with Consumer Data Rule 7.2.
- 1.58 The Consumer Data Rules provide that, if requested by consumer, the CDR entity must give the consumer a copy of the policy electronically or hard copy as requested by the consumer.

¹⁶ 56ED (7)

Chapter 2:

Privacy Safeguard 2 —

Anonymity and pseudonymity

Consultation draft, October 2019

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	3
Summary of application of Privacy Safeguard 2 by CDR participant	4
Why anonymity and pseudonymity are important	4
What is the difference between anonymity and pseudonymity?	5
Providing anonymous and pseudonymous options	5
Exceptions	6
Requiring identification — required or authorised by law	6
Requiring identification — impracticability	6

Key points

- An accredited data recipient must provide a consumer with the option of dealing anonymously or pseudonymously with the entity, unless an exception applies.
- The data standards allow an accredited data recipient to provide these options when seeking the consumer's consent to collect and use their Consumer Data Right (CDR) data.

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 data recipient in relation to the CDR data.
- 2.2 Consumer Data Rule 7.3 sets out that an accredited data recipient does not need to allow anonymity or pseudonymity where:
 - it is impracticable to deal with a consumer who has not identified themselves or has used a pseudonym in relation to the CDR data, or
 - the accredited data recipient is required or authorised by or under a law, or a court/tribunal order, to deal with an identified CDR consumer in relation to particular CDR data.
- 2.3 'Anonymity' and 'pseudonymity' are different concepts. Privacy Safeguard 2 requires that both options be made available to consumers dealing with an accredited data recipient unless one of the two exceptions applies.

Who does Privacy Safeguard 2 apply to?

- 2.4 Privacy Safeguard 2 applies to accredited data recipients. It does not apply to data holders or designated gateways.

How Privacy Safeguard 2 interacts with the Privacy Act

- 2.5 It is important to understand how Privacy Safeguard 2 interacts with the Privacy Act and the Australian Privacy Principles (APPs).¹
- 2.6 Like Privacy Safeguard 2, APP 2 requires entities to provide individuals with the option of not identifying themselves or of using a pseudonym.

¹ The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies.

Summary of application of Privacy Safeguard 2 by CDR participant

CDR Entity	Privacy principle that applies to CDR data
Accredited person	<p>Australian Privacy Principle 2 (and, in practice, Privacy Safeguard 2)</p> <p>Privacy Safeguard 2 does not apply to an accredited person.</p> <p>Notwithstanding, an accredited person should adhere to Privacy Safeguard 2 by providing the consumer with the option of not identifying themselves, or of using a pseudonym, when asking the consumer to provide their consent to collect and use CDR data.</p> <p>This is because an accredited person will become an accredited data recipient for a CDR consumer's CDR data upon collecting such CDR data.</p>
Accredited data recipient	<p>Privacy Safeguard 2</p> <p>Privacy Safeguard 2 applies instead of APP 2, meaning APP 2 will not apply to CDR data that has been received by an accredited data recipient through the CDR regime.</p> <p>APP 2 will continue to apply to any personal information handled by the accredited data recipient that is not CDR data.²</p> <p>This is because all accredited data recipients are subject to the Privacy Act and the APPs for any personal information, even if it is not CDR data.</p>
Designated gateway	<p>Australian Privacy Principle 2</p> <p>Privacy Safeguard 2 does not apply to a designated gateway.</p> <p>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.</p>
Data holder	<p>Australian Privacy Principle 2</p> <p>Privacy Safeguard 2 does not apply to a data holder.</p>

Why anonymity and pseudonymity are important

- 2.7 Anonymity and pseudonymity are important privacy concepts. They enable consumers to choose the extent to which they are identifiable by the accredited data recipient.
- 2.8 There can be benefits to anonymity and pseudonymity, as consumers may be more likely to inquire about products and services under the CDR regime 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.

² See s 6E(1D) of the Privacy Act.

What is the difference between anonymity and pseudonymity?

- 2.9 Anonymity means that a consumer may deal with an accredited data recipient without providing any personal information or identifiers. The accredited data recipient 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 consents to the transfer of CDR data about their current service with no identifying information to enquire generally about a service an accredited data recipient can provide.
- 2.10 Pseudonymity means that a CDR 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.

Providing anonymous and pseudonymous options

- 2.11 An accredited data recipient must provide a CDR consumer with the option of 'dealing' anonymously or pseudonymously with the entity, unless an exception applies.
- 2.12 The time of dealing is when an accredited data recipient asks for the consumer's consent to collect and use their CDR data.³ Examples of 'dealing' with a consumer include:
- asking for the consumer's consent to collect and use their CDR data⁴
 - communicating with the consumer (for example, when providing a CDR receipt to the consumer or ongoing notifications).⁵
- 2.13 The data standards provide that:
- identifying information will not be conveyed to the accredited data recipient unless the consumer agrees, and
 - information provided by the consumer for the purposes of authentication with the data holder will not be seen by the accredited data recipient.

³ See Chapter C: Key Concepts (Consent) and 'Valid Request' in Chapter 3 (Privacy Safeguard 3).

⁴ See Chapter C: Key Concepts (Consent) and 'Valid Request' in Chapter 3 (Privacy Safeguard 3).

⁵ See Consumer Data Rules 4.18 and 4.20.

Anonymity and pseudonymity in the banking sector

Generally, an accredited data recipient in the banking sector is not able to deal with a consumer on an anonymous basis. This is because:

- there may be obligations under law to verify the identity of the customer prior to providing goods or services and/or
- it is impracticable for a consumer to remain anonymous, given CDR data in the banking industry is highly granular and will likely reveal something which could identify them.

Exceptions

Requiring identification — required or authorised by law

- 2.14 Consumer Data Rule 7.3 provides that an accredited data recipient is not required to offer CDR consumers 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 CDR consumer in relation to particular CDR data’.
- 2.15 The meaning of ‘required or authorised by law or court/tribunal order’ is discussed in Chapter B (Key concepts).
- 2.16 If an accredited data recipient 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.
- 2.17 If an entity is ‘authorised’ by a law or order to deal with an identified consumer, the entity can require the consumer to identify themselves, but equally will have discretion to allow the consumer to deal with the entity anonymously or pseudonymously. 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.⁶
- 2.18 The following are given as examples of where a law or order may require or authorise an accredited data recipient to deal only with an identified consumer:
- discussing or accessing the consumer’s banking details with the consumer, such as account information
 - opening a bank account for a consumer, or providing other financial services where legislation requires the consumer to be identified
 - supplying a pre-paid mobile phone to a consumer where legislation requires identification.

Requiring identification — impracticability

- 2.19 Consumer Data Rule 7.3 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 CDR consumer who has not identified themselves.

⁶ For further information, see Chapter B (Key concepts).

2.20 An accredited data recipient that is relying on the impracticability exception should not collect more CDR data than is required to facilitate the dealing with the consumer.

2.21 Examples of where it may be open to an accredited data recipient to rely on the 'impracticability' exception include where:

- providing an anonymous option is impracticable, as the CDR data required to meet a consumer's request will almost certainly identify or reasonably identify the consumer (for example bank account or transaction details in the banking sector)
- the burden of the inconvenience, time and cost of dealing with an unidentified or pseudonymous consumer
- changing internal systems or practices to include the option of anonymous or pseudonymous dealings, would be excessive in all the circumstances.

Chapter 3:

Privacy Safeguard 3 —

Seeking to collect CDR data from CDR participants

Consultation draft, October 2019

Contents

Key points	3
What does Privacy Safeguard 3 say?	3
Why is it important?	3
Who does Privacy Safeguard 3 apply to?	4
How does Privacy Safeguard 3 interact with the Privacy Act?	4
Summary of application of Privacy Safeguard 3 by CDR participant	4
What is meant by ‘seeking to collect’ CDR data?	5
When can an accredited person seek to collect CDR data?	5
What is a ‘valid request?’	6
Process for asking for consent	6
Consumer data request	7
Data minimisation principle	7
Interaction with other Privacy Safeguards	10
Privacy Safeguard 4	10
Privacy Safeguard 5	10

Key points

- Privacy Safeguard 3 prohibits an accredited person from attempting to collect data under the Consumer Data Right (CDR) regime unless it is in response to a ‘valid request’ from the consumer.
- The Consumer Data 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 Consumer Data Rules for collection of CDR data. This includes the ‘data minimisation principle’, where 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 required.

What does Privacy Safeguard 3 say?

- 3.1 An accredited person must not seek to collect CDR data from a CDR participant (i.e. a data holder or an accredited data recipient) unless:
- the CDR consumer has requested the accredited person’s good or service and provided a valid request under the Consumer Data Rules, and
 - the accredited person complies with all other requirements in the Consumer Data Rules for the collection of CDR data from the CDR participant.¹
- 3.2 Under the Consumer Data Rules:
- the valid request must meet specific requirements, including compliance with the Consumer Data Rules regarding consent, and
 - accredited persons must have regard to the data minimisation principle, which limits the scope of a consumer data request that an accredited person may make on behalf of a CDR 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.²

Note: *An accredited person can currently only collect CDR data from a data holder. An accredited person is not currently authorised under the Consumer Data Rules to collect CDR data from an accredited data recipient.*

Why is it important?

- 3.4 The CDR regime is driven by consumers. Consumer consent for the collection of their CDR data is at the heart of the CDR regime.

¹ 56EF.

² 56EF(2).

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. It does not apply to data holders or designated gateways.

3.7 See [Chapter B \(Key Concepts\)](#) for the meaning of accredited persons.

How does Privacy Safeguard 3 interact with the Privacy Act?

3.8 It is important to understand how Privacy Safeguard 3 interacts with the Privacy Act and the APPs.³

3.9 Like Privacy Safeguard 3, APP 3 outlines when an entity may collect solicited personal information (See [Chapter 3: APP 3 – Collection of solicited personal information of the APP Guidelines](#)).

Summary of application of Privacy Safeguard 3 by CDR participant

CDR entity	Privacy principle that applies
Accredited person	<p>Privacy Safeguard 3 and Australian Privacy Principle 3</p> <p>APP 3 applies in parallel to Privacy Safeguard 3.</p> <p>Privacy Safeguard 3 applies instead of APP 3 when an accredited person is seeking to collect CDR data.</p> <p>APP 3 will continue to apply to any personal information collected by an accredited person that is not CDR data.</p>
Accredited data recipient	<p>Privacy Safeguard 3</p> <p>Privacy Safeguard 3 applies instead of APP 3,⁴ meaning APP 3 will not apply to CDR data that has been received by an accredited data recipient through the CDR regime.</p> <p>APP 3 will continue to apply to any personal information handled by the accredited data recipient that is not CDR data.⁵</p>

³ The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies (APP entities). See also Chapter B: Key Concepts of the APP guidelines.

⁴ 56EC(4)(a). Section 56EC(4) provides that the APPs do not apply to an accredited data recipient of CDR data in relation to the CDR data. An accredited person who holds CDR data that was disclosed to the person under the Consumer Data Rules falls within the definition of ‘accredited data recipient’ for that data (unless they are a data holder or designated gateway for the data) (see s 56AK).

⁵ All accredited data recipients are subject to the Privacy Act and the APPs in relation to information that is personal information but is not CDR data. This means that non-CDR personal information handling by accredited data recipients is

CDR entity	Privacy principle that applies
Designated gateway	Australian Privacy Principle 3 Privacy Safeguard 3 does not apply to a designated gateway.
Data holder	Australian Privacy Principle 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 from when the 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 means 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 Consumer Data Rules is by making a ‘consumer data request’ to a data holder on behalf of the consumer. Consumer data requests are explained below at paragraphs 3.21–3.25. The point at which an accredited person makes a consumer data request is demonstrated by the flow chart under paragraph 3.28.
- 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’. ‘Record’ and ‘generally available publication’ have the same meaning as within the Privacy Act.⁶

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 unless it is in response to a valid request from a CDR consumer and the accredited person complies with all other requirements in the Consumer Data Rules for the collection of CDR data.
- 3.15 An accredited person is currently only authorised to seek to collect CDR data from a data holder.

covered by the Privacy Act and the APPs, while the handling of CDR data is covered by the CDR regime and the Privacy Safeguards. See s 6E(1D) of the Privacy Act.

⁶ Privacy Act, s 6(1): ‘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.

Privacy Act, s 6(1): ‘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.

What is a ‘valid request?’

3.16 Under Consumer Data Rule 4.3, a CDR consumer gives an accredited person a ‘valid’ request to seek to collect their CDR data from a data holder if:

- the request is for the accredited person to provide goods or services
- the accredited person needs the CDR consumer’s CDR data⁷ to provide the requested goods or services
- the accredited person asks the consumer’s consent to the collection of their CDR data, in accordance with Subdivision 4.3.2 of the Consumer Data Rules (see paragraphs 3.17–3.20 below for further information) and
- the consumer expressly consents to this collection of their CDR data.

Process for asking for consent

3.17 Subdivision 4.3.2 of the Consumer Data Rules outline the requirements for consent for the purposes of making a valid request for collection of CDR data.

3.18 Specifically, the 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): 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): including to allow the consumer to select or specify the types of data to which they provide consent and provide express consent for the accredited person to collect the selected data. Additional requirements apply where the accredited person is seeking consent to de-identify CDR data (Rule 4.15).
- **Restrictions on seeking consent** (Rule 4.12): including that an accredited person cannot seek to collect or use CDR data for a period exceeding 12 months.
- Obligations about **managing the withdrawal of consent** (Rule 4.13): including that a consumer may withdraw the consent at any time by communicating it in writing to the accredited person or by using the consumer dashboard.
- Time of **expiry of consent** (Rule 4.14): 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).

3.19 The accredited person is also required to have regard to the [Consumer Experience Guidelines](#)⁸ when asking a CDR consumer to give consent.

3.20 These specific requirements and processes for the above Consumer Data Rule requirements are explained in [Chapter C \(Consent\)](#).

⁷ Note that the data may be required consumer data or voluntary consumer data for these purposes.

⁸ Consumer Data Rule 4.10(a)(ii). The ‘Consumer Experience Guidelines’ provide best practice interpretations of the Consumer Data Rules relating to consent and are discussed in Chapter B (Key Concepts).

Consumer data request

- 3.21 If a consumer has given an accredited person a valid request (see paragraph 3.16 above), and the consumer’s consent for the accredited person to collect and use their CDR data is current,⁹ the accredited person may request the relevant data holder to disclose some or all of the CDR data that:
- is the subject of the relevant consent to collect and use CDR data; and
 - it is able to collect and use in compliance with the data minimisation principle.¹⁰
- 3.22 In doing so, the accredited person makes a ‘consumer data request’ to a data holder on behalf of the consumer.¹¹ The accredited person may make consumer data requests to more than one data holder where the relevant CDR data required to provide the requested goods or services is held by different data holders. 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.
- 3.23 When the accredited person makes a consumer data request on behalf of a CDR consumer, they must not seek to collect more CDR data than is reasonably needed, or that relates to a longer time period than reasonably required, in order to provide the requested goods or services.¹²
- 3.24 The accredited person must make the consumer data request:
- using the data holder’s accredited person request service, and
 - in accordance with the data standards.¹³
- 3.25 An accredited person complies with Privacy Safeguard 3 after giving a data holder a consumer data request in the manner set out above.¹⁴

Data minimisation principle

- 3.26 Collection of CDR data is limited by the data minimisation principle (Rule 4.12(2)), where an accredited person:
- must not collect more data than is reasonably needed in order to provide the requested goods or services, and
 - may use the collected data only consistent with the consent provided, and only as reasonably needed in order to provide the requested goods or services.
- 3.27 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 data holder a consumer data request.
- 3.28 The data minimisation principle is discussed further in Chapter B (Key Concepts).

⁹ ‘Current consent’ is discussed in Chapter B (Key Concepts).

¹⁰ Consumer Data Rule 4.4(1).

¹¹ Consumer Data Rule 4.4(2).

¹² Consumer Data Rules 1.8(a), 4.4(1)(d).

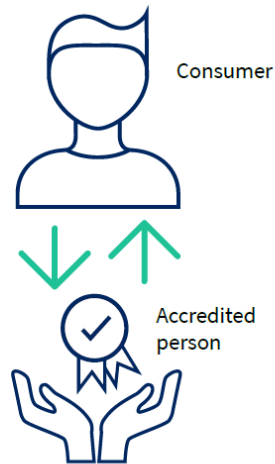
¹³ Consumer Data Rule 4.4(3).


¹⁴ The effect of Consumer Data Rule 4.4(2) is that a request for CDR data from an accredited person on behalf of a CDR consumer that does not comply with Consumer Data Rule 4.4(1) is not a ‘consumer data request’.

Example: As part of a consumer data request to seek information about their eligibility to open a bank account, the accredited person asks a consumer for their consent to collect information about their marital status from the data holder, when this has no bearing on the applicant's eligibility for the service. This is a breach of the data minimisation principle.

Obtaining consumer consent for the collection and use of CDR data

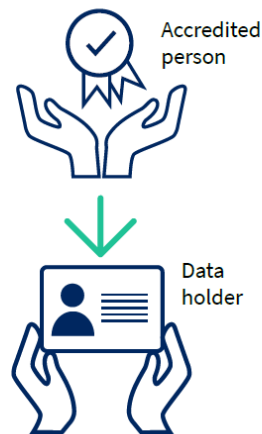
- Accredited person offers a good or service which requires CDR data
- Consumer wishes to be provided the good or service
- Accredited person asks the consumer to consent to the collection and use of their CDR data for this purpose, for up to 12 months
- Consumer provides their express consent



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 data holder to disclose the consumer's CDR data
- Accredited person requests the data using the data holder's 'accredited person request service'



Data holder sends consumer data to accredited data recipient



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

Interaction with other Privacy Safeguards

Privacy Safeguard 4

- 3.29 The Privacy Safeguards distinguish between an accredited person collecting solicited CDR data (Privacy Safeguard 3) and unsolicited CDR data (Privacy Safeguard 4).
- 3.30 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)).
- 3.31 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

- 3.32 Privacy Safeguard 5 requires an accredited person who has collected data in accordance with Privacy Safeguard 3 to notify the CDR consumer of the collection in accordance with the Consumer Data Rules (See Chapter 5 (Privacy Safeguard 5)).

Chapter 4:

Privacy Safeguard 4 —

Dealing with unsolicited CDR data from CDR participants

Consultation draft, October 2019



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 does Privacy Safeguard 4 interact with the Privacy Act and APP 4?	4
Summary of application of Privacy Safeguard 4 by CDR entity	4
Unsolicited CDR data	4
What circumstances does Privacy Safeguard 4 apply to?	5
Where CDR data is collected outside the Consumer Data Rules	5
What is the obligation to destroy unsolicited data?	6
‘Destroy’	6
As soon as practicable	6
Not required to retain the data	6
How does Privacy Safeguard 4 interact with other Privacy Safeguards?	7

Key points

- Privacy Safeguard 4 requires an accredited person to destroy unsolicited Consumer Data Right (CDR) data that the entity is not required to retain by 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 CDR participant, purportedly under the Consumer Data Rules, but 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.¹
- 4.3 This obligation applies regardless of whether the accredited person collects the CDR data directly from a data holder or indirectly through a designated gateway.²

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.
- 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 control and ownership consumers have over their data under the CDR regime 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 and APP 4 when dealing with unsolicited personal information.

¹ 56EG(1).

² 56EG(2).

How does Privacy Safeguard 4 interact with the Privacy Act and APP 4?

- 4.8 It is important to understand how Privacy Safeguard 12 interacts with the Privacy Act 1988 (the Privacy Act) and Australian Privacy Principles (APPs).³
- 4.9 Like Privacy Safeguard 4, APP 4 relates 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 3.⁴

Summary of application of Privacy Safeguard 4 by CDR entity

CDR Entity	Privacy principle that applies to CDR data
Accredited person	<p>Privacy Safeguard 4</p> <p>Although APP 4 applies in parallel with Privacy Safeguard 4, an accredited person will be an ‘accredited data recipient’ for the CDR data purportedly collected under the Consumer Data Rules, which means that APP 4 will not apply in respect of that data.</p> <p>APP 4 will continue to apply to any personal information handled by the accredited person that is not CDR data.</p>
Accredited data recipient	<p>Privacy Safeguard 4</p> <p>Privacy Safeguard 4 applies instead of APP 4, meaning APP 4 will not apply to CDR data that has been received by an accredited data recipient through the CDR regime.</p> <p>APP 4 will continue to apply to any personal information handled by the accredited data recipient that is not CDR data. This is because all accredited data recipients are subject to the Privacy Act and the APPs for any personal information, even if it is not CDR data.</p>
Designated gateway	<p>Australian Privacy Principle 4</p> <p>Privacy Safeguard 4 does not apply to a designated gateway.</p>
Data holder	<p>Australian Privacy Principle 4</p> <p>Privacy Safeguard 4 does not apply to a data holder.</p>

Unsolicited CDR data

- 4.10 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 Consumer Data Rules.
- 4.11 An example of how an accredited person might collect such ‘unsolicited’ CDR data is where:

³ The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies (APP entities). See also [Chapter B: Key Concepts of the APP guidelines](#).

⁴ See [Chapter 3: APP 3 – Collection of solicited personal information](#).

- the accredited person makes a consumer data request on a CDR consumer's behalf to collect CDR data from a data holder, in accordance with Privacy Safeguard 3 and Consumer Data Rule 4.4
- the data holder has or receives authorisation from the CDR 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).⁵

4.12 A discussion of how an accredited person may properly seek to collect CDR data is contained in Chapter 3 (Privacy Safeguard 3) at [3.14].

What circumstances does Privacy Safeguard 4 apply to?

4.13 Privacy Safeguard 4 applies to CDR data collected by an accredited person from a CDR participant:

- purportedly under the Consumer Data Rules; but
- not as the result of seeking to collect that CDR data under the Consumer Data Rules.⁶

Where CDR data is collected outside the Consumer Data Rules

4.14 Neither Privacy Safeguard 3 nor Privacy Safeguard 4 apply where an accredited person seeks to collect CDR data outside of the Consumer Data Rules. This is because Privacy Safeguard 3 only applies where an accredited person seeks to collect data under the Consumer Data Rules, and Privacy Safeguard 4 only applies where an accredited person collects CDR data purportedly under the Consumer Data Rules.

4.15 An accredited person who collects CDR data outside of the Consumer Data Rules is not an 'accredited data recipient' as defined in s 56AK, as the CDR data will not be disclosed to the person under the Consumer Data Rules. Therefore, Privacy Safeguard 6 (which concerns use of disclosure of CDR data) and Privacy Safeguard 12 (which concerns security of CDR data) do not apply in such circumstances.

4.16 Instead, the accredited person will be a data holder of that CDR data, if they are an accredited data recipient of 'other CDR data'.⁷ In respect of the CDR data received outside the Consumer Data Rules, the person must comply with the privacy safeguards applicable to data holders, and if the person is an APP entity, the Privacy Act and APPs in respect of personal information, to the extent not overridden by the Privacy Safeguards.

⁵ In these circumstances the data holder may be in breach of APP 6 if personal information was disclosed outside the authorisation provided by the CDR consumer.

⁶ s 56EG(1)(a).

⁷ 56AJ(3)(b). 'Other CDR data' is CDR data other than the CDR data that the accredited person has collected outside of the Consumer Data Rules: see Notes 1 and 2 regarding s 56AJ(3).

Example

Penny makes a valid consumer data request of her bank to disclose all of her CDR data under Consumer Data Rule 3.3. Her bank then discloses all her CDR data it holds pursuant to Consumer Data Rule 3.4.

Penny has a mortgage broker, Brent, who is registered as an accredited person. Penny gives Brent her CDR data via a USB and asks him to find the best deal to refinance her loan on the market. Brent agrees and takes the USB.

Brent has collected CDR data outside of the Consumer Data Rules. Neither Privacy Safeguard 3 nor Privacy Safeguard 4 apply.

Brent is, however, a 'data holder' of the CDR data under section 56AJ(1) and (3). He must comply with Privacy Safeguards 1, 10, 11 and 13.

If Brent is an APP entity, he must also comply with the Privacy Act and relevant APPs in respect of the personal information he has collected from Penny.

What is the obligation to destroy unsolicited data?

'Destroy'

4.17 Privacy Safeguard 4 requires unsolicited CDR data to be 'destroyed'. Destruction of CDR data is discussed in detail in [Chapter 12 \(Privacy Safeguard 12\)](#).

As soon as practicable

4.18 Privacy Safeguard 4 requires unsolicited CDR data to be destroyed 'as soon as practicable'.

4.19 The test of practicability is an objective test. It is the responsibility of the entity to be able to justify that it is not practicable to destroy unsolicited data promptly after its collection.

4.20 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.

4.21 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 destroying unsolicited CDR data.

4.22 The timeframe in which an entity must destroy unsolicited CDR data begins at the time the entity becomes aware that the data was not solicited. How quickly an entity becomes aware of unsolicited CDR data may depend on its available technical and other resources.

Not required to retain the data

4.23 The obligation to destroy unsolicited data does not apply to CDR data that an entity is required to retain by or under an Australian law or court/tribunal order.⁸

⁸ 56EG(1)(b).

- 4.24 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 other Privacy Safeguards?

- 4.25 Privacy Safeguard 3 prohibits an accredited person from seeking to collect CDR data from a data holder unless in response to a valid request from a CDR consumer, and in compliance with the Consumer Data Rules (see [Chapter 3 \(Privacy Safeguard 3\)](#)).
- 4.26 Privacy Safeguard 12 requires an accredited data recipient to destroy or de-identify redundant CDR data unless the entity is required by or under an Australian law or court/tribunal 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 \(Privacy Safeguard 12\)](#)).
- 4.27 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

Consultation draft, October 2019

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 does Privacy Safeguard 5 interact with the Privacy Act and APP 5?	4
Summary of application of Privacy Safeguard 5 by CDR entity	4
How must notification be given?	5
Who must be notified?	5
When must notification be given?	5
What matters must be included in the notification?	6
What CDR data was collected	6
When the CDR data was collected	6
The data holder of the CDR data	7
Other notification requirements under the Consumer Data Rules	7
How does Privacy Safeguard 5 interact with other Privacy Safeguards?	7

Key points

- An accredited person must notify the relevant consumer when they collect Consumer Data Right (CDR) data.
- This notification must occur through their consumer dashboard as soon as practicable after the accredited person has received the CDR data.

What does Privacy Safeguard 5 say?

- 5.1 If an accredited person collects CDR data under Privacy Safeguard 3, the accredited person must notify the consumer/s of the collection by taking the steps identified in the Consumer Data Rules.¹
- 5.2 The notification must:
- be given to the consumers whom the Consumer Data Rules require to be notified
 - cover the matters set out in the Consumer Data Rules, and
 - be given at or before the time specified in the Consumer Data Rules.
- 5.3 Under Consumer Data Rule 7.4, an accredited person must notify the CDR consumer through their consumer dashboard as soon as practicable after CDR data is collected from a CDR participant.
- 5.4 For information about the concept of ‘collects’ refer to Chapter B, Key Concepts.

Why is this important?

- 5.5 Notification of collection of CDR data is an integral element of the CDR regime 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 CDR participants.

Risk point: Clear and prompt communication to consumers will promote trust in the CDR scheme. If a consumer has a poor experience, they may not be interested in continuing to participate.

Privacy tip: In addition to notifying the CDR consumer of the collection of their CDR data via the consumer dashboard, an accredited person must provide the consumer with a ‘CDR receipt’ as soon as practicable after the consumer consents to the collection and use of their CDR data.² This ‘CDR receipt’ must be given in writing but not through the consumer dashboard (e.g. via text or email).

¹ Section 56EH

² Consumer Data Rule 4.18. A ‘CDR receipt’ is a notice that sets out certain details of the consent to collect and use, the name of each data holder that the consumer has consented to the collection of CDR data from and any other information the accredited person provided to the consumer when asking for their consent. A copy of the CDR receipt may be included in the consumer’s consumer dashboard.

This will encourage engagement and maximise the chance that a consumer is informed (given that a consumer may not actively check their consumer dashboard).

Who does Privacy Safeguard 5 apply to?

- 5.7 Privacy Safeguard 5 applies to accredited persons. 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 Australian Privacy Principles (APPs), including APP 3 and APP 5, when collecting personal information.

How does Privacy Safeguard 5 interact with the Privacy Act and APP 5?

- 5.9 It is important to understand how Privacy Safeguard 5 interacts with the Privacy Act and the APPs.³
- 5.10 Like Privacy Safeguard 5, APP 5 outlines when an entity that collects information must tell an individual about certain matters.
- 5.11 The Privacy Act and APP 5 provide protection where collected data is personal information but not CDR data.

Summary of application of Privacy Safeguard 5 by CDR entity

CDR entity	Privacy principle that applies
Accredited person	<p>Privacy Safeguard 5</p> <p>APP 5 applies in parallel to Privacy Safeguard 5.</p> <p>Privacy Safeguard 5 applies instead of APP 5 when notifying consumers of the collection of CDR data.</p> <p>APP 5 will continue to apply to any personal information handled by the accredited person that is not CDR data.</p>
Accredited data recipient	<p>Privacy Safeguard 5</p> <p>Privacy Safeguard 5 applies instead of APP 5, meaning APP 5 will not apply to CDR data that an accredited data recipient receives through the CDR regime.</p> <p>APP 5 will continue to apply to any personal information handled by the accredited data recipient that is not CDR data.</p>

³ The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies.

CDR entity	Privacy principle that applies
Designated gateway	Australian Privacy Principle 5 Privacy Safeguard 5 does not apply to a designated gateway.
Data holder	Australian Privacy Principle 5 Privacy Safeguard 5 does not apply to a data holder.

How must notification be given?

- 5.12 Accredited persons must provide notification by updating the consumer dashboard of a consumer.
- 5.13 Further guidance about the consumer dashboard is set out in [Chapter B \(Key concepts\)](#) and [Chapter C \(Consent\)](#).

Who must be notified?

- 5.14 The accredited person must notify the consumer who gave the accredited person consent to collect the CDR data.
- 5.15 There may be more than one CDR consumer to whom a set of CDR data applies, for example, where there are joint account holders of a bank account. In this example, the accredited person is only required by the Consumer Data Rule 7.4 to update the consumer dashboard of the requesting joint account holder.

When must notification be given?

- 5.16 An accredited person must notify the consumer as soon as practicable after the CDR data is collected.
- 5.17 Notification should generally occur in as close to real time as possible (i.e. as close to the time of first collection as possible).
- 5.18 However, whether the notification occurs ‘as soon as practicable’ will depend on the circumstances, and the following factors may be relevant:
- time and cost involved
 - technical matters
 - any individual needs of the consumer (for example, additional steps required to make the content accessible).
- 5.19 It is the responsibility of the accredited person to be able to justify any delay in notification.
- 5.20 An accredited person is not excused from providing notification by reason only that it would be inconvenient, time consuming or costly to do so.

Risk point: Delays to notification of collection may result in confusion for a CDR consumer and non-compliance for an accredited person.

Privacy tip: Accredited persons 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?

5.21 The minimum matters that must be noted in a CDR consumer’s consumer dashboard are:

- what CDR data was collected
- when the CDR data was collected
- the data holder of the CDR data.⁴

What CDR data was collected

5.22 The accredited person must ensure CDR data is described with enough specificity to allow the CDR consumer to easily understand what CDR data was collected.

5.23 An accredited person should have regard to the Data Language Standards when implementing this requirement.⁵ 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

Where the CDR data was collected on a ‘one-off’ basis:⁶

5.24 The accredited person should include the date on which the CDR data was collected.

5.25 Where CDR data was collected at different times, the accredited person should include the date on which each dataset was collected.

5.26 Examples of where an accredited person collects CDR data at different times include where:

- the CDR data is held by more than one data holder, and those data holders disclose CDR data to the accredited person on different dates
- the CDR data is held by one data holder, and that data holder discloses CDR data to the accredited person on different dates

⁴ Consumer Data Rule 7.4.

⁵ The Data Language Standards can be found within the Consumer Experience Guidelines. 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 will help ensure there is a consistent interpretation and description of the consumer data that will be shared in the CDR regime.

⁶ This is where the accredited person indicated the CDR data would be collected on a single occasion and used over a specified period of time (Consumer Data Rule 4.11(1)(b)(i)).

*Where the CDR data was collected and will continue to be collected over a period of time:*⁷

- 5.27 The accredited person should include the date range between which CDR data will be collected, with the starting date being the date on which the CDR data was first collected.
- 5.28 The accredited person should, in addition to stating the time period for collection, note the frequency of data collection for ongoing collection.
- 5.29 The accredited person should have regard to the Consumer Experience Guidelines when implementing this requirement.⁸

The data holder of the CDR data

- 5.30 Where an accredited person is authorised to make consumer data requests on the CDR consumer's behalf to multiple data holders, an accredited person should indicate the CDR data that relates to each data holder.
- 5.31 An accredited person must have regard to the Consumer Experience Guidelines relating to the data recipient dashboard landing page when implementing this requirement.

Other notification requirements under the Consumer Data Rules

- 5.32 In addition to the Privacy Safeguard 5 notification requirements in relation to collection, there are other notification requirements relating to consent that must be complied with:
 - providing CDR receipts to the CDR consumer (Rule 4.18)⁹
 - general obligation to update the consumer dashboard (Consumer Data Rule 4.19)
 - ongoing notification requirements for CDR consumer consents (Rule 4.20).

How does Privacy Safeguard 5 interact with other Privacy Safeguards?

- 5.33 CDR participants must comply with Privacy Safeguard 1 by taking reasonable steps to implement practices, procedures and systems that will ensure they comply with the CDR legislation, including Privacy Safeguard 5. See [Chapter 1 \(Privacy Safeguard 1\)](#).
- 5.34 The Privacy Safeguard 5 requirement to notify consumers about the collection of their CDR data relates to all CDR data collected under Privacy Safeguard 3 (see [Chapter 3 \(Privacy Safeguard 3\)](#)).

⁷ This is where the accredited person indicated the CDR data would be collected and used over a specified period of time (Consumer Data Rule 4.11(1)(b)(ii)).

⁸ See the examples of implementation of the data recipient dashboard regarding 'data sharing arrangement' in the Consumer Experience Guidelines.

⁹ A 'CDR receipt' is a notice that sets out certain details of the consent to collect and use, the name of each data holder that the consumer has consented to the collection of CDR data from and any other information the accredited person provided to the consumer when asking for their consent. A copy of the CDR receipt may be included in the consumer's consumer dashboard.

5.35 While Privacy Safeguard 5 only relates to notification on *collection*, Privacy Safeguard 10 sets out when CDR participants must notify consumers about the *disclosure* of their CDR data. See [Chapter 10 \(Privacy Safeguard 10\)](#).

Chapter 6:

Privacy Safeguard 6 —

Use or disclosure of CDR data by accredited data recipients or designated gateways

Consultation draft, October 2019

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?	3
How does Privacy Safeguard 6 interact with the Privacy Act and APP 6?	4
Summary of application of Privacy Safeguard 6 by CDR entity	4
Why is it important?	5
What is meant by ‘use’ and ‘disclose’?	5
‘Use’	5
‘Disclose’	5
When can an accredited data recipient use or disclose CDR data?	6
Use or disclosure required or authorised under the Consumer Data Rules	6
Use or disclosure under Australian law or a court/tribunal order	11

Key points

- Privacy Safeguard 6, together with Rules 7.5 and 7.7, sets out the obligations and restrictions on accredited data recipients in the use and disclosure of Consumer Data Right (CDR) data.
- Generally, accredited data recipients and designated gateways can only use or disclose CDR data where required or authorised under the Consumer Data Rules. In most cases, the consumer is required to expressly consent to these uses of their CDR data.
- Consumer Data Rule 7.5 outlines the permitted uses or disclosures of CDR data.
- Consumer Data Rule 4.12(3) also prohibits certain uses or disclosures of CDR data.

What does Privacy Safeguard 6 say?

Accredited data recipients

- 6.1 An accredited data recipient must not use or disclose CDR data unless the:
- disclosure is required under the Consumer Data Rules in response to a valid request from a CDR consumer for the CDR data, or
 - use or disclosure is otherwise required or authorised under the Consumer Data 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 must satisfy the requirements under Consumer Data Rules 7.5 and 4.12(3).

Designated gateways

- 6.3 A designated gateway of CDR data must not use or disclose CDR data unless the:
- disclosure is required under the Consumer Data Rules, or
 - use or disclosure is authorised under the Consumer Data Rules, or
 - 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.

Who does Privacy Safeguard 6 apply to?

- 6.4 Privacy Safeguard 6 applies to accredited data recipients and designated gateways.
- 6.5 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 Australian privacy Principles (APPs), including APP 6, when using or disclosing personal information.

Note: Currently, there are no designated gateways in the CDR regime responsible for facilitating the transfer of information between data holders and accredited persons (see Chapter B: Key Concepts for the meaning of designated gateway)

How does Privacy Safeguard 6 interact with the Privacy Act and APP 6?

6.6 It is important to understand how Privacy Safeguard 6 interacts with the Privacy Act 1988 (the Privacy Act) and Australian Privacy Principles (APPs).¹

6.7 Like Privacy Safeguard 6, APP 6 relates to the use or disclosure of personal information.²

Summary of application of Privacy Safeguard 6 by CDR entity

CDR entity	Privacy principle that applies to CDR data
Accredited person	<p>Australian Privacy Principle 6</p> <p>Privacy Safeguard 6 does not apply to an accredited person who is not an accredited data recipient of the relevant CDR data.</p>
Accredited data recipient	<p>Privacy Safeguard 6</p> <p>Privacy Safeguard 6 applies instead of APP 6,³ meaning APP 6 will not apply to CDR data that has been received by an accredited data recipient through the CDR regime.</p> <p>APP 6 will continue to apply to any personal information handled by the accredited data recipient that is not CDR data.⁴</p>
Designated gateway	<p>Privacy Safeguard 6</p> <p>Privacy Safeguard 6 applies instead of APP 6, meaning APP 6 will not apply to CDR data that has been received by a designated gateway through the CDR regime.</p> <p>APP 6 will continue to apply to the designated gateway where they are handling personal information in their capacity as an APP entity.</p>
Data holder	<p>Australian Privacy Principle 6</p> <p>Privacy Safeguard 6 does not apply to a data holder.</p>

¹ The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies (APP entities).

² 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 Chapter 6: APP 6 — Use or disclosure of personal information.

³ 56EC(4)(a). Section 56EC(4) provides that the APPs do not apply to an accredited data recipient of CDR data in relation to the CDR data. An accredited person who holds CDR data that was disclosed to the person under the Consumer Data Rules falls within the definition of ‘accredited data recipient’ for that data (unless they are a data holder or designated gateway for the data) (see s 56AK).

⁴ All accredited data recipients are subject to the Privacy Act and the APPs in relation to information that is personal information but is not CDR data. This means that non-CDR personal information handling by accredited data recipients is covered by the Privacy Act and the APPs, while the handling of CDR data is covered by the CDR regime and the Privacy Safeguards. See s 6E(1D) of the Privacy Act.

Why is it important?

- 6.8 Consumer consent for uses of their CDR data, including subsequent disclosure, is at the heart of the CDR regime.
- 6.9 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 going to be given to. This is an essential part of the CDR regime.

What is meant by ‘use’ and ‘disclose’?

‘Use’

- 6.10 The term ‘use’ is not defined within the Consumer and Competition Act.⁵
- 6.11 An accredited data recipient or designated gateway ‘uses’ CDR data where it handles or undertakes an activity with the CDR data, within the entity’s 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
 - the entity passing the CDR data from one part of the entity to another.

‘Disclose’

- 6.12 The term ‘disclose’ is not defined within the Consumer and Competition Act.⁶
- 6.13 An accredited data recipient or designated gateway ‘discloses’ CDR data where it makes it accessible to others outside the entity and releases the subsequent handling of the information from its effective control. This focuses on the act done by the disclosing party. The state of mind or intentions of the recipient does not affect the act of disclosure.
- 6.14 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).
- 6.15 Examples of disclosure include where an accredited data recipient or designated gateway:
- shares the CDR data with another entity or individual
 - discloses CDR data to themselves, but in their capacity as a different entity
 - 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
 - displays a computer screen so that the CDR data can be read by another entity or individual.

⁵ The term ‘use’ is also not defined in the Privacy Act.

⁶ The term ‘disclose’ is also not defined in the Privacy Act.

When can an accredited data recipient use or disclose CDR data?

6.16 This section outlines when an accredited data recipient may use or disclose CDR data.⁷

6.17 This chapter does not consider when a designated gateway may use or disclose CDR data. This is because there are not currently any designated gateways for the banking sector.

Use or disclosure required or authorised under the Consumer Data Rules

6.18 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 Consumer Data Rules.⁸

6.19 Consumer Data Rule 7.5 authorises the following permitted uses or disclosures of CDR data⁹:

- using CDR data to provide goods or services requested by the consumer in compliance with the data minimisation principle and in accordance with a consent from the CDR consumer
- directly or indirectly deriving CDR data from the collected CDR data for the above purpose
- disclosing to the CDR consumer any of their CDR data
- disclosing the CDR consumer's CDR data to an outsourced service provider:
 - for the purpose of doing the things referred to the above three dot points, and
 - 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.

6.20 However, an accredited data recipient must not ask a CDR consumer to give consent to use or disclose their CDR data for the following prohibited uses or disclosures:

- selling the CDR data (unless de-identified in accordance with the CDR data de-identification process); or
- using it for the purpose of identifying, compiling insights in relation to, or building a profile in relation to, any identifiable person who is not a CDR consumer who made the

⁷ 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 Consumer Data Rules in response to a valid request from a CDR consumer for the CDR data (56EI(1)(a)). The Consumer Data 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 Consumer Data Rules or under an Australian law or a court/tribunal order. These circumstances are outlined in this chapter from paragraph 6.18 onwards.

⁸ Section 56EI(1)(b). The use or disclosure of CDR data is not currently required under the Consumer Data Rules. The use or disclosure of CDR data is authorised under the Consumer Data Rules if it is a 'permitted use or disclosure' under Consumer Data Rule 7.5 that does not relate to direct marketing (Consumer Data Rule 7.7).

consumer data request (including through aggregating the CDR data), unless the accredited data recipient is seeking consent to:

- derive, from that CDR data, CDR data about that person's interactions with the CDR consumer, and
- use that derived CDR data in order to provide the requested goods or services.¹⁰

Example

MinYin is a money transfer app allowing friends to split bills and request payments without the need to log-in to banking apps. Elizabeth wishes to try out MinYin's service via a CDR transfer.

When seeking Elizabeth's consent to the CDR transfer, MinYin also asks for consent to analyse Elizabeth's frequent payees to identify those who use the app. MinYin tells Elizabeth that it needs this information to be able to send and receive payment requests from those friends.

MinYin has followed the requirements in rule 4.12(3), as MinYin used Elizabeth's CDR data to identify persons who are not Elizabeth for a permitted purpose. The permitted purpose here is to derive data about Elizabeth's interactions with that person in order to deliver the service to Elizabeth.

MinYin changes its CDR consent process to also ask for consent to attempt to identify demographic information about those payees. MinYin intends to analyse data on Elizabeth's payees to build a profile of her social circle. It will then sell this information.

MinYin has now sought consent for a prohibited use of CDR data, breaching the requirement in rule 4.12(3). This is because MinYin used Elizabeth's CDR data to identify persons who are not Elizabeth for a prohibited purpose. The prohibited purpose here is to build a 'silent profile' on Elizabeth's social circle for a purpose other than providing Elizabeth's service to her.

6.21 The above permitted uses and disclosures (in paragraph 6.19) are discussed further below.

Using CDR data in accordance with a current consent to provide goods or services requested by the consumer

6.22 An accredited data recipient is authorised to use CDR data in accordance with a current consent from the CDR consumer to provide goods or services requested by the CDR consumer.¹¹

6.23 The relevant uses are those uses to which the CDR consumer expressly consented when the CDR consumer provided a valid request for the accredited data recipient to make a consumer data request on their behalf to collect the CDR consumer's CDR data from the data holder. Valid requests are discussed further in [Chapter 3 \(Privacy Safeguard 3\)](#).

6.24 For information regarding how consents to collect and use CDR data must be managed, [see Chapter C \(Consent\)](#).

¹⁰ Consumer Data Rule 4.12(3).

¹¹ Consumer Data Rule 7.5(1)(a).

Example

SpendLess Pty Ltd is an accredited data recipient for Oliver's CDR data, and provides Oliver with tailored budgeting tips through its mobile budgeting application.

SpendLess notices that Oliver has similar spending habits to several of its other consumers who are of a similar demographic background. SpendLess runs Oliver's transaction data through an algorithm with the other consumers' transaction data to analyse trends and provide predictive and bigger picture budgeting recommendations to Oliver.

When providing his valid request to SpendLess, Oliver consented to the analysis of his transaction data for the purpose of providing him with tailored budgeting tips. He did not consent to his transaction data being used to allow SpendLess to compile broader insights in conjunction with other datasets.

SpendLess has not used Oliver's CDR data in accordance with his consent and is therefore in breach of Consumer Data Rule 7.5(1)(a). Assuming the other consumers provided valid requests on the same terms as Oliver, SpendLess is also in breach of Consumer Data Rule 7.5(1)(a) in relation to the other consumers whose transaction data was combined with Oliver's.

Using CDR data in compliance with the data minimisation principle

- 6.25 An accredited data recipient must comply with the data minimisation principle when using the CDR data to provide goods or services requested by the CDR consumer.¹²
- 6.26 The data minimisation principle provides that the accredited data recipient must 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 CDR consumer.¹³
- 6.27 The data minimisation principle and meaning of 'reasonably needed' is discussed in more detail in Chapter B (Key concepts) and, as it relates to consent for collection, in Chapter 3 (Privacy Safeguard 3).

Risk point: An accredited data recipient should pay careful consideration to its processes and systems to ensure it is compliant with the data minimisation principle in all of its uses of CDR data. This includes a separate consideration of the minimum CDR data required to provide each good or service (including each upgraded good or service) to a CDR consumer.

Privacy tip: An accredited data recipient should set up its systems and processes so that it can identify minimum required CDR data for a particular good or service. This reduces variance and ensures prompt and compliant responses to CDR consumers' requests for CDR data, and ensures these responses do not exceed the limitations imposed by the data minimisation principle.

Deriving or indirectly deriving CDR data

- 6.28 An accredited data recipient is permitted to directly or indirectly derive CDR data from the collected CDR data for the purpose of providing goods or services requested by the

¹² Consumer Data Rule 7.5(1)(a).

¹³ Consumer Data Rule 1.8(b).

consumer.¹⁴ The accredited data recipient is not required to obtain the consumer's consent to do so.

6.29 However, where an accredited data recipient:

- wishes to derive, from the consumer's CDR data, CDR data about the interactions between the consumer and an identifiable person who is not the consumer, and
 - will use that derived data to provide the goods or services requested by the consumer
- the accredited data recipient must seek consent from the consumer before doing so.¹⁵

6.30 Derived data is discussed in more detail in Chapter B (Key concepts).

Disclosing CDR data to the consumer

6.31 An accredited data recipient is permitted to disclose to a CDR consumer any of their CDR data.¹⁶

6.32 This includes CDR data collected from the data holder in response to the CDR consumer's valid request, as well as data that has been directly and/or indirectly derived from such CDR data.

6.33 This is a permitted disclosure and does not require the consent of the CDR consumer.¹⁷

Disclosing CDR data to an outsourced service provider

6.34 An accredited data recipient is permitted to disclose the CDR consumer's CDR data to an outsourced service provider for the purpose of:

- using the CDR consumer's CDR data to provide goods or services requested by the CDR consumer, including by directly or indirectly deriving CDR data from the CDR data, and
- disclosing, to the CDR consumer, any of their CDR data

to the extent reasonably needed to fulfil those purposes.¹⁸

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 engages KnowYourMoney Pty Ltd to analyse consumers' data and report on consumers' spending trends per categories so that SpendLess can provide tailored budgeting advice to consumers.

SpendLess discloses Oliver's account and transaction data to KnowYourMoney. However, KnowYourMoney only needs Oliver's transaction data for this purpose. KnowYourMoney does not need to analyse Oliver's account data in order to report upon Oliver's spending trends.

¹⁴ Consumer Data Rule 7.5(1)(b).

¹⁵ Consumer Data Rule 4.12(4).

¹⁶ Consumer Data Rule 7.5(1)(c).

¹⁷ Consumer Data Rules 7.5(1)(c) and 4.11.

¹⁸ Consumer Data Rule 7.5(1)(d).

In doing so, SpendLess Pty Ltd has disclosed Oliver’s CDR data to an outsourced service provider beyond the extent reasonably needed to fulfil the purpose of providing the service requested by Oliver. SpendLess Pty Ltd will be in breach of rule 7.5(1)(d).

- 6.35 The consumer’s CDR data includes data collected from the data holder 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.
- 6.36 Disclosure of a CDR consumer’s CDR data by an accredited data recipient to an outsourced service provider for the purpose outlined in paragraph 6.34 is a permitted disclosure and does not require the consent of the CDR consumer.
- 6.37 However, where an accredited data recipient intends to disclose CDR data of a CDR consumer to an outsourced service provider, the accredited data recipient must:
- provide certain information to the CDR consumer at the time of seeking the CDR consumer’s consent to collect and use the CDR consumer’s CDR data,¹⁹ and
 - include certain information about outsourced service providers in its CDR policy.²⁰
- 6.38 An outsourced service provider is a person to whom an accredited data recipient discloses CDR data under a CDR outsourcing arrangement.²¹
- 6.39 An accredited data recipient who discloses CDR data to a person under a CDR outsourcing arrangement must ensure that the person complies with its requirements under the arrangement.
- 6.40 In order to meet this requirement, the accredited data recipient must ensure that the relevant CDR outsourcing arrangement requires the outsourced service provider to adhere to the accredited data recipient’s Privacy Safeguard obligations.
- 6.41 The contract should also provide the accredited data recipient with the appropriate levels of transparency to allow them to monitor and audit the CDR outsourcing arrangement.
- 6.42 Where an accredited data recipient has disclosed CDR data to a person under a CDR outsourcing arrangement, any use or disclosure of that data by the person (or their subcontractor) will be taken to have been by the accredited data recipient. This occurs regardless of whether the use or disclosure is in accordance with the arrangement.²²
- 6.43 For further information, see Chapter B Key Concepts ‘Outsourced service providers’.

Disclosing de-identified CDR data

- 6.44 An accredited data recipient is permitted to disclose to any person, by sale or otherwise, CDR data that has been de-identified in accordance with the CDR data de-identification process.²³

¹⁹ Consumer Data Rule 4.11(3)(f). See Chapter 3 (Privacy Safeguard 3).

²⁰ Consumer Data Rule 7.2(4). See Chapter 1 (Privacy Safeguard 1).

²¹ Consumer Data Rule 1.10. A CDR outsourcing arrangement exists when an accredited data recipient discloses CDR data to another person if it does so under a written contract between the parties.

²² Consumer Data Rule 7.6(2). This is the case whether the CDR data was disclosed directly to the person by the accredited data recipient, or indirectly through one or more further CDR outsourcing arrangements (Consumer Data Rule 7.6(3)).

²³ Consumer Data Rule 7.5(1)(e).

- 6.45 In order to do so, however, the accredited data recipient must have first:
- received consent from the CDR consumer to de-identify some or all of the collected CDR data for the purpose of disclosing (including by selling) the de-identified data;²⁴ and
 - provided the CDR consumer with additional information relating to the de-identification of CDR data.²⁵
- 6.46 An accredited data recipient must ensure it complies with the CDR data de-identification process when de-identifying CDR data.²⁶ De-identification is discussed further in Chapter 12.

Use or disclosure under Australian law or a court/tribunal order

- 6.47 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.²⁷
- 6.48 For the purposes of Privacy Safeguard 6, an Australian law does not include the APPs under the Privacy Act.²⁸
- 6.49 ‘Australian law’ and ‘court/tribunal order’ are discussed in [Chapter B \(Key concepts\)](#).
- 6.50 The accredited data recipient must keep a written note of any uses or disclosures made on this ground.
- 6.51 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
 - to whom the CDR data has been disclosed, if applicable.

²⁴ Consumer Data Rule 4.11(3)(e).

²⁵ Consumer Data Rule 4.15.

²⁶ Consumer Data Rule 1.17.

²⁷ Section 56EI(1)(c).

²⁸ Sections 56EI(1) (Note 3) and 56EC(4)(a).

Chapter 7:

Privacy Safeguard 7 —

Use or disclosure of CDR data for direct marketing by accredited data recipients or designated gateways

Consultation draft, October 2019

Contents

Key points	3
What does Privacy Safeguard 7 say?	3
Why is it important?	3
Who does Privacy Safeguard 7 apply to?	3
How Privacy Safeguard 7 interacts with the Privacy Act	3
Summary of application of Privacy Safeguard 7 by CDR entity	4
Meaning of direct marketing	4
Interaction with other Privacy Safeguards	5
Interaction with other legislation	5

Key points

- Privacy Safeguard 7 prohibits the use or disclosure of CDR data for direct marketing by accredited data recipients and designated gateways, unless the use or disclosure is required or authorised under the Consumer Data Rules.
- Direct marketing involves the use or disclosure of CDR data to promote goods and services directly to a consumer.

What does Privacy Safeguard 7 say?

- 7.1 Privacy Safeguard 7 prohibits the use or disclosure of CDR data for direct marketing by accredited data recipients and designated gateways, unless the use or disclosure is required or authorised under the Consumer Data Rules.

Why is it important?

- 7.2 To provide a positive consumer experience and ensure consumer control over their data, consumers should not be subjected to unwanted direct marketing.
- 7.3 Privacy Safeguard 7 prohibits direct marketing in the Consumer Data Right (CDR) regime unless it is required or authorised under the Consumer Data Rules.

Who does Privacy Safeguard 7 apply to?

- 7.4 Privacy Safeguard 7 applies to accredited data recipients and designated gateways. It does not apply to data holders.

How Privacy Safeguard 7 interacts with the Privacy Act

- 7.5 It is important to understand how Privacy Safeguard 7 interacts with the *Privacy Act 1988* (Cth) (the Privacy Act) and Australian Privacy Principles (APPs).¹
- 7.6 Like Privacy Safeguard 7, APP 7 sets out when an APP entity is prohibited from using or disclosing personal information for the purpose of direct marketing.

¹ The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies (APP entities).

Summary of application of Privacy Safeguard 7 by CDR entity

CDR entity	Privacy principle that applies to CDR data
Accredited person	<p>Australian Privacy Principle 7</p> <p>Privacy Safeguard 7 does not apply to an accredited person who is not an accredited data recipient of the relevant CDR data.</p>
Accredited data recipient	<p>Privacy Safeguard 7</p> <p>Privacy Safeguard 7 applies instead of APP 7,² meaning APP 7 will not apply to CDR data that has been received by an accredited data recipient through the CDR regime.</p> <p>APP 7 will continue to apply to any personal information handled by the accredited data recipient that is not CDR data.³ This is because all accredited data recipients are subject to the Privacy Act and the APPs for any personal information, even if it is not CDR data.</p>
Designated gateway	<p>Privacy Safeguard 7</p> <p>Privacy Safeguard 7 applies instead of APP 7,⁴ meaning APP 7 will not apply to CDR data that has been received by a designated gateway through the CDR regime.</p> <p>APP 7 will continue to apply to the designated gateway where they are handling personal information in their capacity as an APP entity.</p>
Data holder	<p>Australian Privacy Principle 7</p> <p>Privacy Safeguard 7 does not apply to a data holder.</p>

Meaning of direct marketing

- 7.7 ‘Direct marketing’ is not defined in the Competition and Consumer Act. The term is also used in APP 7 but is not defined in the Privacy Act.⁵
- 7.8 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 or services.

² 56EC(4)(a). Section 56EC(4) provides that the APPs do not apply to an accredited data recipient of CDR data in relation to the CDR data. An accredited person who holds CDR data that was disclosed to the person under the Consumer Data Rules falls within the definition of ‘accredited data recipient’ for that data (unless they are a data holder or designated gateway for the data) (see s 56AK).

³ All accredited data recipients are subject to the Privacy Act and the APPs in relation to information that is personal information but is not CDR data. This means that non-CDR personal information handling by accredited data recipients is covered by the Privacy Act and the APPs, while the handling of CDR data is covered by the CDR regime and the Privacy Safeguards. See s 6E(1D) of the Privacy Act.

⁴ Section 56EC(4)(d).

⁵ 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).

- 7.9 This means that ‘direct marketing’ requires an element of promotion, where goods and services are promoted to elicit or encourage a response from the consumer.
- 7.10 An entity does not ‘direct market’ where the offer of goods or services forms part (or all) of the goods or services requested by the consumer as part of the consumer’s valid request.⁶
- 7.11 For example, it is not direct marketing where:
- A consumer wishes to obtain suitable offers from multiple providers for a product and provides an accredited data recipient with a valid request to collect their CDR data for the purpose of providing tailored offers from various providers. In doing so, the accredited data recipient uses the CDR data to provide the requested good or service. This use is not direct marketing and Privacy Safeguard 7 does not apply. The accredited data recipient must comply with Privacy Safeguard 6.
 - A consumer is considering switching providers for a product. The consumer provides an accredited data recipient with a valid request to seek to collect their CDR data from their current provider (the data holder) and use that data to provide suitable offers in relation to the product. In doing so, the accredited data recipient uses the CDR data to provide the good or service. This use is not direct marketing and Privacy Safeguard 7 does not apply. The accredited data recipient must comply with Privacy Safeguard 6.

Interaction with other Privacy Safeguards

- 7.12 The prohibition against direct marketing in Privacy Safeguard 7 is complemented by Privacy Safeguard 6 (see Chapter 6 (Privacy Safeguard 6)). Privacy Safeguard 6 prohibits an accredited data recipient from using or disclosing data unless required or authorised under the Consumer Data Rules or another Australian law or court or tribunal order.

Interaction with other legislation

- 7.13 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.
- 7.14 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,⁷ 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 Consumer Data Rules).

⁶ For information regarding ‘valid requests’, see Chapter 3 (Privacy Safeguard 3).

⁷ 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* (Cth), s 11(2)).

Chapter 8:

Privacy Safeguard 8 —

Overseas disclosure of CDR data by accredited data recipients

Consultation draft, October 2019

Contents

Key points	3
What does Privacy Safeguard 8 say?	3
Why is this important?	3
Who does Privacy Safeguard 8 apply to?	4
How does Privacy Safeguard 8 interact with the Privacy Act and the APPs?	4
Summary of application of Privacy Safeguard 8 by CDR participant	4
When does an accredited data recipient ‘disclose’ CDR data to an overseas recipient?	5
What is an overseas recipient?	5
Conditions for disclosing CDR data to an overseas recipient	6
Disclosing CDR data to an overseas recipient who is an accredited person	6
Disclosing CDR data after taking ‘reasonable steps’ to ensure an overseas recipient does not contravene the privacy safeguards	6
Disclosing CDR data with a ‘reasonable belief’ the overseas recipient is subject to a substantially similar law (and the consumer can enforce that law)	8
Conditions specified in the Consumer Data Rules	9
When is an accredited person accountable for the acts or omission of an overseas recipient?	10

Key points

- Privacy Safeguard 8 sets out the circumstances in which an accredited data recipient can disclose CDR data to a recipient located overseas.
- An accredited data recipient must not disclose CDR data to a recipient located overseas unless:
 - the overseas recipient is also an accredited person, or
 - the accredited data recipient takes reasonable steps to ensure the overseas recipient will not contravene the privacy safeguards (and the accredited data recipient remains liable for any contravention of the privacy safeguards by the overseas recipient), or
 - the accredited data recipient reasonably believes the overseas recipient is subject to a law equivalent to the Privacy Safeguards and there are mechanisms available to the consumer to enforce that protection.

What does Privacy Safeguard 8 say?

- 8.1 An accredited data recipient must not disclose CDR data to a person located overseas unless:
- a. the overseas recipient is an accredited person, or
 - b. the accredited data recipient takes reasonable steps to ensure the overseas recipient does not breach the Privacy Safeguards¹ and has a CDR policy in relation to the CDR data, or
 - c. the accredited data recipient reasonably believes the overseas recipient is bound by a law or scheme that is substantially similar to the privacy safeguards and a CDR consumer will be able to enforce that law or scheme in relation to the CDR data, or
 - d. conditions specified in the Consumer Data Rules for overseas disclosure are met. There are currently no Consumer Data Rules in relation to Privacy Safeguard 8.
- 8.2 Where an accredited data recipient takes reasonable steps to ensure the overseas recipient does not breach the Privacy Safeguards (as described in condition 2 above), but the overseas recipient nevertheless contravenes a relevant privacy safeguard, the accredited data recipient is accountable for that contravention, notwithstanding the fact they complied with their Privacy Safeguard 8 obligations.
- 8.3 For the purposes of a CDR outsourcing arrangement, an accredited data recipient must comply with Privacy Safeguard 8 and the Consumer Data Rules that relate to CDR outsourcing arrangements (Rule 1.10, Rule 7.5(1)(d) and Rule 7.6).

Why is this important?

- 8.4 As an overarching objective of the CDR framework, CDR consumers should be able to trust that an accredited data recipient will manage that data appropriately and in compliance with the Privacy Safeguards, even when it is disclosed overseas.

¹ The relevant Privacy Safeguards are the privacy safeguard penalty provisions in defined in s56EU (Privacy Safeguards 3 – 13 inclusive, and the requirement to have a CDR policy in Privacy Safeguard 1).

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 to an overseas recipient.

Who does Privacy Safeguard 8 apply to?

8.6 Privacy Safeguard 8 applies to accredited data recipients.

8.7 It does not apply to data holders or designated gateways. However, data holders and designated gateways should ensure that they adhere to their obligations under the Privacy Act 1988 and the APPs, including APP 8, when disclosing personal information to an overseas recipient.

How does Privacy Safeguard 8 interact with the Privacy Act and the APPs?

8.8 It is important to understand how Privacy Safeguard 8 interacts with the Privacy Act 1988 (the Privacy Act) and Australian Privacy Principles (APPs).²

8.9 The Privacy Safeguards are assumed to apply to an overseas recipient where the overseas recipient's act or omission in relation to the CDR data would contravene the Privacy Safeguards.

Summary of application of Privacy Safeguard 8 by CDR participant

CDR Participant	Privacy principle that applies to CDR data
Accredited person	<p>Australian Privacy Principle 8</p> <p>Privacy Safeguard 8 does not apply to an accredited person who is not an accredited data recipient of the relevant CDR data.</p>
Accredited data recipient	<p>Privacy Safeguard 8</p> <p>Privacy Safeguard 8 applies instead of APP 8,³ meaning APP 8 will not apply to CDR data that has been received by an accredited data recipient through the CDR regime, and is being disclosed to a person located overseas.</p> <p>APP 8 will continue to apply to any personal information handled by the accredited data recipient that is not CDR data. This is because all accredited data recipients are subject to the Privacy Act and the APPs for any personal information, even if it is not CDR data.⁴</p>

² The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies (APP entities).

³ 56EC(4)(a). Section 56EC(4) provides that the APPs do not apply to an accredited data recipient of CDR data in relation to the CDR data. An accredited person who holds CDR data that was disclosed to the person under the Consumer Data Rules falls within the definition of 'accredited data recipient' for that data (unless they are a data holder or designated gateway for the data) (see s 56AK).

⁴ See s 6E(1D) of the Privacy Act.

CDR Participant	Privacy principle that applies to CDR data
Designated gateway	Australian Privacy Principle 8 Privacy Safeguard 8 does not apply to a designated gateway.
Data holder	Australian Privacy Principle 8 Privacy Safeguard 8 does not apply to a data holder.

When does an accredited data recipient ‘disclose’ CDR data to an overseas recipient?

- 8.10 The term ‘disclose’ is not defined in the CDR legislation. It is discussed in Chapter B (Key Concepts).
- 8.11 An accredited data recipient discloses CDR data when it makes it accessible to others outside the entity and releases the subsequent handling of the information from its effective control.
- 8.12 The release of the information may be a release in accordance with the Consumer Data Rules, or an accidental release or an unauthorised release.
- 8.13 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.

What is an overseas recipient?

- 8.14 Under Privacy Safeguard 8, an overseas recipient is a person,⁵ who receives CDR data from an accredited data recipient, who is not:
- in Australia or in an external Territory, and
 - a CDR consumer for the CDR data.
- 8.15 Where an accredited data recipient in Australia sends CDR data to an overseas office of the same entity, Privacy Safeguard 8 will not apply.
- 8.16 This is to be distinguished from the case where an accredited data recipient in Australia sends CDR data to a ‘related body corporate’ located outside of Australia. In that case, the related body corporate is a different entity to the accredited data recipient in Australia. It may therefore be an overseas recipient (assuming it does not meet the ‘located in Australia or external Territory’ requirement) and Privacy Safeguard 8 will apply.
- 8.17 The term ‘CDR consumer’ is discussed in [Chapter B – Key Concepts](#).

⁵ Including a body corporate with separate legal personality.

Conditions for disclosing CDR data to an overseas recipient

Disclosing CDR data to an overseas recipient who is an accredited person

- 8.18 An accredited data recipient may disclose CDR data to an overseas recipient if the person is an accredited person.
- 8.19 The term ‘accredited person’ is discussed in [Chapter B – Key Concepts](#).
- 8.20 The Consumer Data Rules require that an individual or company must apply to be an accredited person under the Competition and Consumer Act. Accredited persons will be added to the Register of Accredited Persons if their application is successful.
- 8.21 The Consumer Data Rules and the draft [ACCC’s Accreditation Guidelines](#) provide more information about the requirements and process for accreditation.
- 8.22 Accreditation is considered sufficient protection to ensure compliance with the privacy safeguards.⁶

Disclosing CDR data after taking ‘reasonable steps’ to ensure an overseas recipient does not contravene the privacy safeguards

- 8.23 The requirement in Privacy Safeguard 8 to ensure that an overseas recipient does not breach the Privacy Safeguards is qualified by a ‘reasonable steps’ test.

What are ‘reasonable steps’?

- 8.24 It is generally expected that an accredited data recipient will enter into an enforceable contractual arrangement with the overseas recipient that requires the recipient to handle the CDR data in accordance with the Privacy Safeguards.
- 8.25 Consideration of whether an accredited data recipient has taken reasonable steps to ensure the overseas recipient can comply with the CDR regime may include:
- 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)

⁶ Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019, section 1.348.

- the possible adverse consequences for a CDR consumer if the CDR data is mishandled by the overseas recipient. More rigorous steps may be required as the risk of adversity increases
- existing technical and operational safeguards 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 Consumer Data Rules). More rigorous steps will be required where the recipient has limited existing safeguards in place
- the practicability, 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

‘on behalf of’

- 8.26 Privacy Safeguard 8 contemplates management or handling of CDR data undertaken on behalf of an overseas recipient. This may include employees, directors, officers, consultants, or subcontractors of an overseas recipient.
- 8.27 The Privacy Safeguards apply to the acts or omissions of an overseas recipient (or an individual or entity acting on behalf of the overseas recipient) as though the overseas recipient was the accredited data recipient who disclosed the CDR data for the purposes of the obligations of an accredited data recipient under Privacy Safeguard 8.

Risk point: An accredited data recipient will be liable under CDR legislation for the acts and omissions of an overseas recipient (and the acts or omissions of the subcontractors of the overseas recipient), where an accredited data recipient relies on the “reasonable steps” exception in Privacy Safeguard 8.

Privacy tip: It is advisable that an accredited person ensures 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.

Example

KTelco Ltd outsources its customer contact centre services function to HelpsHere Pty Ltd, an Australian-based entity. HelpsHere Pty Ltd uses a subcontractor located overseas to ensure HelpsHere Pty Ltd can meet a service commitment to its customers.

KTelco Ltd and HelpsHere Pty Ltd have a contract capturing their CDR outsourcing arrangement, which is compliant with the Consumer Data Rules. Under this contract, HelpsHere Pty Ltd and its subcontractors must comply with the CDR regime.

The subcontractor breaches its contract with HelpsHere Pty Ltd by accidentally disclosing CDR data to a third party. Under the Privacy Safeguards, KTelco Ltd is liable for the breach by their subcontractor.

Disclosing CDR data with a ‘reasonable belief’ the overseas recipient is subject to a substantially similar law (and the consumer can enforce that law)

What is ‘reasonable belief’?

- 8.28 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 protections to the Privacy Safeguards and that a CDR consumer will be able to enforce the protections provided by that law or binding scheme.
- 8.29 An accredited data recipient must have a reasonable basis for the belief, which is an objective test and not merely a genuine or subjective belief. It is the responsibility of the entity to be able to justify its reasonable belief.

What is a ‘law or binding scheme’?

- 8.30 An overseas recipient may be subject to a law or binding scheme, where, for example, it is:
- bound by 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 scheme, 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.
- 8.31 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’?

- 8.32 A substantially similar law or binding scheme would provide a comparable, or a higher level of privacy protection to that provided by the privacy safeguards. 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.
- 8.33 Whether there is substantial similarity is a question of fact.
- 8.34 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
- the law or scheme includes a right to access and seek correction of consumer data

When can a CDR consumer enforce the protections?

- 8.35 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 is substantially similar to the CDR regime.
- 8.36 An enforcement mechanism should meet two key requirements:
- it should be accessible to the individual, and
 - it should have effective powers to enforce the consumer data protections in the law or binding scheme.
- 8.37 A range of mechanisms may satisfy those requirements, ranging from a regulatory body similar to the OAIC, to an accredited dispute resolution scheme, an independent tribunal or a court with judicial functions and powers. Factors that may be relevant in deciding whether there is an accessible and effective enforcement mechanism 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
 - has 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
 - is required to operate according to principles of procedural fairness.
- 8.38 The mechanism may be a single mechanism or a combination of mechanisms. It may be established by the law or binding scheme that contains the consumer data protections, or by another law or binding scheme. Alternatively, the mechanism may take effect through the operation of cross-border enforcement arrangements between the OAIC and an appropriate regulatory authority in the foreign jurisdiction.

Conditions specified in the Consumer Data Rules

- 8.39 Privacy Safeguard 8 permits an overseas disclosure where conditions specified in the Consumer Data Rules are met.
- 8.40 The Consumer Data Rules do not currently provide any conditions for overseas disclosure and therefore this basis for disclosure is not available.

When is an accredited person accountable for the acts or omission of an overseas recipient?

8.41 Privacy Safeguard 8 provides that an accredited person is 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, and
- the accredited person does not reasonably believe that the overseas recipient is bound by a law or scheme that is similar to the CDR regime and that a consumer will be able to enforce protections provided by that law or scheme, or
- the conditions in the Consumer Data Laws are not met, and
- the overseas recipient contravenes the privacy safeguards⁷ and/or does not have a CDR policy.⁸

8.42 In these circumstances, the act or omission is taken to have been done by the accredited data recipient. The accredited data recipient is taken to have contravened the Privacy Safeguards.

8.43 Where an accredited data recipient takes reasonable steps to ensure the overseas recipient complies with the Privacy Safeguards, but the overseas recipient nevertheless contravenes a relevant Privacy Safeguard, the accredited data recipient is liable for that contravention (notwithstanding the fact it complied with its Privacy Safeguard 8 obligations).

8.44 As noted above, the conditions in the Consumer Data Rules relate to disclosures to outsourced service providers and stipulate the requirements that must be met by the accredited data recipient in doing so.

8.45 Importantly, Consumer Data Rule 7.6(2) provides that the accredited data recipient will be liable for the acts or omissions of the outsourced service provider (or its subcontractors), whether or not they were in accordance with the arrangement or not.

8.46 Therefore, it would be prudent for an accredited data recipient to consider maintaining policies in relation to the nature of the entities it engages under a CDR outsourcing arrangement. Those entities that:

- are accredited persons, or
- are located in jurisdictions in which they are bound by a law or scheme that is substantially similar to the CDR regime.

⁷ The relevant Privacy Safeguards are the privacy safeguard penalty provisions in defined in s56EU (Privacy Safeguards 3 – 13 inclusive, and the requirement to have a CDR policy in Privacy Safeguard 1).

⁸ 56EK(2).

Chapter 9:

Privacy Safeguard 9 —

Adoption or disclosure of government related identifiers by accredited data recipients

Consultation draft, October 2019

Contents

Key points	3
What does Privacy Safeguard 9 say?	3
Why is it important?	3
Who does Privacy Safeguard 9 apply to?	3
How Privacy Safeguard 9 interacts with the Privacy Act	4
Summary of application of Privacy Safeguard 9 by CDR entity	4
Meaning of government related identifier	4
‘Identifiers’	5
‘Government related identifier’	5
Adopting, using or disclosing a government related identifier	6
‘Adopt’	6
‘Use’	6
‘Disclose’	7
Exceptions	7
Interaction with other Privacy Safeguards	8
Privacy Safeguard 4	8

Key points

- Privacy Safeguard 9 sets out a prohibition on accredited data recipients adopting, using or disclosing government related identifiers unless required or authorised:
 - under another Australian law or
 - as prescribed by regulations made under the 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.
- An individual cannot consent to the adoption, use or disclosure of their government related identifier.

What does Privacy Safeguard 9 say?

- 9.1 Privacy Safeguard 9 prohibits an accredited data recipient that has collected CDR data which includes a government related identifier of a CDR consumer for the CDR data, from:
- adopting the government related identifier as its own identifier of the CDR 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 Consumer Data Rules, or
 - Australian Privacy Principle (APP) 9.3, which allows an entity to adopt, use or disclose a government related identifier of an individual as prescribed by regulations.
- 9.2 Privacy Safeguard 9 only concerns government related identifiers of individuals.
- 9.3 In this Chapter, a government related identifier of a CDR consumer included with the CDR 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 CDR consumer may not agree with or expect.

Who does Privacy Safeguard 9 apply to?

- 9.5 Privacy Safeguard 9 applies to accredited data recipients. It does not apply to data holders or designated gateways.

How Privacy Safeguard 9 interacts with the Privacy Act

- 9.6 It is important to understand how Privacy Safeguard 9 interacts with the *Privacy Act 1988* (Privacy Act) and the APPs.¹
- 9.7 Like Privacy Safeguard 9, APP 9 prohibits an APP entity from adopting, using or disclosing a government related identifier unless an exception applies.

Summary of application of Privacy Safeguard 9 by CDR entity

CDR entity	Privacy principle that applies to CDR data
Accredited data recipient	<p>Privacy Safeguard 9</p> <p>Privacy Safeguard 9 applies instead of APP 9,² meaning APP 9 will not apply to government related identifiers adopted, used or disclosed under the CDR regime.</p> <p>All accredited data recipients are subject to the Privacy Act and the APPs for their handling of personal information that is not CDR data. This is because all accredited data recipients are subject to the Privacy Act and the APPs for any personal information, even if it is not CDR data.³</p> <p>APP 9 will continue to apply to any government related identifier of an individual where collected in the entity's capacity as an APP entity.</p>
Designated gateway	<p>Australian Privacy Principle 9</p> <p>Privacy Safeguard 9 does not apply to a designated gateway.</p>
Data holder	<p>Australian Privacy Principle 9</p> <p>Privacy Safeguard 9 does not apply to a data holder.</p>

Meaning of government related identifier

- 9.8 'Government related identifier' has the meaning given to it in the Privacy Act⁴.
- 9.9 Privacy Safeguard 9 only concerns government related identifiers of individuals.
- 9.10 This only applies to CDR consumers who are natural persons (including individuals, sole trader or the partner of a partnership but not to corporations). For example, the Australian

¹ The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies.

² 56EC(4)(a). Section 56EC(4) provides that the APPs do not apply to an accredited data recipient of CDR data in relation to the CDR data. An accredited person who holds CDR data that was disclosed to the person under the Consumer Data Rules falls within the definition of 'accredited data recipient' for that data (unless they are a data holder or designated gateway for the data) (see s 56AK).

³ See s 6E(1D) of the Privacy Act.

⁴ 56EL(1)(b); 56EL(2)(b).

Business Number (ABN) of a body corporate would not be subject to Privacy Safeguard 9 (and note that the ABN of an individual is not an ‘identifier’ under s 6(1) of the Privacy Act).

‘Identifiers’

9.11 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.

9.12 The following are explicitly excluded from the definition of identifier:

- an individual’s name,
- an individual’s ABN
- anything else prescribed by the regulations made under the Privacy Act.⁵ 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’

9.13 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 agency⁶
- a State or Territory authority⁷
- 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,⁸ or a State contract,⁹ acting in its capacity as contracted service provider for that contract.

9.14 The following are examples of government related identifiers:

- Medicare numbers,
- Centrelink Reference numbers,
- driver licence numbers issued by State and Territory authorities and
- Australian passport numbers.

⁵ See the Federal Register of Legislation <<https://www.legislation.gov.au>> for up-to-date versions of the regulations made under the Privacy Act.

⁶ ‘Agency’ is defined in s 6(1) of the Privacy Act.

⁷ ‘State or Territory authority’ is defined in s 6C(3) of the Privacy Act.

⁸ ‘Commonwealth contract’ is defined in s 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.

⁹ ‘State contract’ is defined in s 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.

9.15 Some government related identifiers are regulated by other laws that restrict the way that entities can collect, use or disclose the particular identifier and related personal information. Examples include tax file numbers and individual healthcare identifiers.¹⁰

Adopting, using or disclosing a government related identifier

9.16 An accredited data recipient must not adopt a CDR consumer government related identifier as its own identifier of the CDR consumer, or otherwise use a government related identifier, unless an exception applies.¹¹ In addition, an accredited data recipient must not include the government related identifier when it discloses CDR data unless an exception applies.

‘Adopt’

9.17 The term ‘adopt’ is not defined in the Competition and Consumer Act and so it is appropriate to refer to its ordinary meaning.

9.18 An accredited data recipient ‘adopts’ a CDR consumer government related identifier if it collects CDR data that includes a government related identifier of the CDR consumer and organises the CDR data that it holds about that individual with reference to that identifier.

Example

Saul, an accountant and accredited data recipient, receives a CDR consumer’s driver licence number when it is disclosed to Saul in response to a consumer data request. Saul then uses the identifier to refer to that consumer in his own identification system.

Saul has adopted a CDR consumer government related identifier in breach of Privacy Safeguard 9.

‘Use’

9.19 The term ‘use’ is discussed in Chapter B (Key Concepts).

9.20 Examples of when an accredited data recipient will ‘use’ a CDR consumer government identifier include where the entity refers to a consumer by that identifier, organises records

¹⁰ For more information about the legislative regimes, visit the OAIC’s Tax File Numbers page and Healthcare Identifiers page <<https://www.oaic.gov.au>>.

¹¹ 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.

and documents pertaining to that consumer by reference to that identifier, or otherwise attributes that identifier to the CDR data of the consumer for reference purposes.

‘Disclose’

- 9.21 The term ‘disclose’ is discussed in Chapter B (Key Concepts)
- 9.22 An accredited data recipient or designated gateway ‘discloses’ CDR data where it makes it accessible to others outside the entity and releases the subsequent handling of the information from its effective control.

Exceptions

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

- 9.23 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.¹²
- 9.24 The meaning of ‘required or authorised by or under an Australian law or a court/tribunal order’ is discussed in Chapter B (Key concepts).
- 9.25 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,
 - the particular circumstances in which they may adopt, use or disclose it.

Prescribed by regulations

- 9.26 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.¹³
- 9.27 Regulations may be made under the Privacy Act to prescribe these matters.¹⁴

Example

Accredited data recipient, Data Dump Pty Ltd, uses a third party service provider, Bale. Ian, a CDR consumer, authorises a data holder of his CDR data to disclose his CDR data to Data Dump. The data holder discloses Ian’s passport number with the data.

¹² 56EL(1)(c).

¹³ 56EL(1)(d) and APP 9.3.

¹⁴ See the Federal Register of Legislation <<https://www.legislation.gov.au>> for up-to-date versions of regulations made under the Privacy Act.

Data Dump discloses CDR data collected from the data holder of Ian's CDR data to Bale pursuant to Consumer Data Rule 7.5(1)(d). Bale then uses the CDR data to provide data analytics services. Data Dump's systems are set up so that all CDR data collected is sent over a secure link to Bale, where the data is then within Bale's control.

When Ian's passport number is sent to Bale along with Ian's other CDR data, Data Dump has included the government related identifier in a disclosure in breach of Privacy Safeguard 9.

Risk point: An accredited data recipient may unknowingly use a CDR consumer government related identifier if there are not processes in place to prevent this.

Privacy tip: Accredited data recipient may frame consumer data requests made to data holders to specifically exclude any government related identifiers to reduce the risk that such identifiers will be included in the disclosure.

Interaction with other Privacy Safeguards

Privacy Safeguard 4

- 9.28 Privacy Safeguard 9 does not specifically address the collection of government related identifiers. However, if an accredited data recipient collects a government related identifier that is considered to be CDR data, the accredited data recipient 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

Consultation draft, October 2019

Contents

Key points	3
What does Privacy Safeguard 10 say?	3
Why is it important?	3
Who does Privacy Safeguard 10 apply to?	3
Who must be notified?	4
How must notification be given?	4
When must notification be given?	4
What matters must be included in the notification?	5
What CDR data was disclosed	5
When the CDR data was disclosed	5
The accredited data recipient of the CDR data	6
Other notification requirements under the Consumer Data Rules	6
Disclosure to a designated gateway	6
Interaction with other Privacy Safeguards	6

Key points

- Where a data holder discloses CDR data to an accredited person, the data holder must notify the consumer by updating the consumer dashboard.
- The Consumer Data Rules set out the matters that must be included in this notification.

What does Privacy Safeguard 10 say?

- 10.1 Where a data holder is required or authorised under the Consumer Data Rules to disclose CDR data, they must notify the consumer by taking the steps identified in the Consumer Data Rules.¹
- 10.2 Where an accredited data recipient discloses CDR data, they must notify the consumer by taking the steps identified in the Consumer Data Rules.²
- 10.3 The notification must:
- be given to those consumers that the Consumer Data Rules require to be notified,
 - cover the matters set out in the Consumer Data Rules, and
 - be given at or before the time specified in the Consumer Data Rules.

Why is it important?

- 10.4 Notification of disclosure of CDR data is an integral element of the Consumer Data Right (CDR) regime, as it provides confirmation to consumers that their CDR data has been disclosed in response to a consumer data request.
- 10.5 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?

- 10.6 Privacy Safeguard 10 applies to data holders and accredited data recipients. It does not apply to designated gateways.
- 10.7 Although Privacy Safeguard 10 applies to accredited data recipients, there are currently no Consumer Data Rules requiring accredited data recipients to notify consumers about the disclosure of CDR data.³
- 10.8 Accredited persons, accredited data recipients and designated gateways must ensure they are adhering to their obligations under the *Privacy Act 1988* (Cth) (Privacy Act) and the Australian Privacy Principles (APPs), including APP 6, when disclosing personal information.

¹ Section 56EM(1). For further information on 'required or authorised to use or disclose CDR data under the Consumer Data Rules', refer to Chapter B (Key Concepts).

² Section 56EM(2).

³ This is because accredited data recipients are generally not permitted to disclose CDR data unless the disclosure is directly to the consumer or to an outsourced service provider (Consumer Data Rule 7.5). On that basis, an accredited data recipient does not currently have notification obligations under Privacy Safeguard 10.

Who must be notified?

- 10.9 The data holder must notify each of the consumers for the CDR data that has been disclosed.⁴
- 10.10 There may be more than one consumer for the CDR data. In the banking sector, a key example is CDR data relating to a joint account. In this case, the data holder must notify both the requesting and non-requesting joint account holders. However, a data holder will not be required to notify the non-requesting joint account holder/s where the data holder considers this necessary to prevent physical or financial harm or abuse.⁵
- 10.11 This exception to notification is to accommodate existing procedures a data holder may have to protect consumers, for example particular account arrangements relating to consumers that may be experiencing family violence.

How must notification be given?

- 10.12 A data holder must update the consumer dashboard⁶ for a consumer as soon as practicable after CDR data relating to that consumer is disclosed.⁷
- 10.13 Further guidance about the consumer dashboard is set out in Chapter B (Key concepts).

When must notification be given?

- 10.14 A data holder must notify the consumer/s as soon as practicable after the CDR data is disclosed.⁸
- 10.15 Notification should generally occur in as close to real time as possible (i.e. as close to the time of first disclosure as possible).
- 10.16 However, whether the notification occurs ‘as soon as practicable’ will depend on the circumstances, and the following factors may be relevant:
- time and cost involved
 - technical matters
 - individual needs of the consumer (for example, additional steps required to make the content accessible).
- 10.17 It is the responsibility of the data holder to be able to justify any delay in notification.

⁴ Section 56EM(1)(b) and Consumer Data Rule 7.9. The Consumer Data Rules may also set requirements for other consumers that must be notified when CDR data is disclosed. There are currently no additional requirements in the Consumer Data Rules, other than in relation to joint account holders in the banking industry.

⁵ Rule 7.9 and clause 4.6 of Schedule 3, Consumer Data Rules.

⁶ A data holder’s consumer dashboard is an online service that can be used by each consumer to manage authorisations to disclose CDR data in response to consumer data requests. The service must also notify the consumer of information related to CDR data disclosed pursuant to an authorisation. The requirements for a data holder’s consumer dashboard are set out in Consumer Data Rule 1.14. The Consumer Experience Guidelines contain best practice recommendations for the data holder consumer dashboard.

⁷ Consumer Data Rule 7.9.

⁸ Consumer Data Rule 7.9.

10.18 A data holder is not excused from providing notification by reason only that it would be inconvenient, time consuming or costly to do so.

What matters must be included in the notification?

10.19 The minimum matters that need to be noted in a consumer's consumer dashboard are:

- what CDR data was disclosed
- when the CDR data was disclosed, and
- the accredited data recipient of the CDR data.⁹

What CDR data was disclosed

10.20 The data holder should ensure that the CDR data is described with sufficient specificity to allow the consumer to easily understand what CDR data was disclosed.

10.21 A data holder should have regard to the Data Language Standards when implementing this requirement.¹⁰ This will aid consumer comprehension by ensuring consistency between how CDR data was described in the authorisation-seeking process and how CDR data is described in the consumer dashboard.

When the CDR data was disclosed

*Where the CDR data was disclosed on a 'one-off' basis:*¹¹

10.22 The data holder should include the date on which the CDR data was disclosed.

10.23 Where CDR data was disclosed at different times, the data holder should include the date on which each dataset was disclosed.

*Where the CDR data was disclosed and will continue to be disclosed over a period of time:*¹²

10.24 The data holder should include the date range between which CDR data will be disclosed, with the starting date being the date on which the CDR data was first disclosed.

10.25 The data holder should, in addition to stating the time period for disclosure, note the frequency of data disclosure for ongoing disclosure.

⁹ Consumer Data Rule 7.9.

¹⁰ The Data Language Standards can be found within the Consumer Experience Guidelines. They provide descriptions of the types of data to be used by data holders when making and responding to requests. Adherence to the Data Language Standards will help ensure there is a consistent interpretation and description of the consumer data that will be shared in the CDR regime.

¹¹ 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.

¹² 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.

- 10.26 The data holder should have regard to the Consumer Experience Guidelines when implementing this requirement.¹³

The accredited data recipient of the CDR data

- 10.27 The data holder must indicate to whom the CDR data was disclosed.
- 10.28 A data holder should have regard to the Consumer Experience Guidelines relating to consumer dashboards when implementing this requirement.

Other notification requirements under the Consumer Data Rules

- 10.29 In addition to the Privacy Safeguard 10 notification requirements in relation to disclosure, the data holder must update a consumer's consumer dashboard as soon as practicable after the information required to be contained on the dashboard changes.¹⁴

Disclosure to a designated gateway

Note: *There are currently no designated gateways in the CDR regime.*

- 10.30 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 Consumer Data Rules.¹⁵
- 10.31 There are currently no Consumer Data Rules made for this circumstance.

Interaction with other Privacy Safeguards

- 10.32 CDR participants must comply with Privacy Safeguard 1 by taking reasonable steps to implement practices, procedures and systems that will ensure they comply with the CDR regime, including Privacy Safeguard 10. See Chapter 1 (Privacy Safeguard 1).
- 10.33 Privacy Safeguard 11 mandates the steps by which a data holder must advise a consumer where the data holder has disclosed CDR data that was incorrect. See Chapter 11 (Privacy Safeguard 11).

¹³ See the examples of implementation of the data holder dashboard regarding 'data sharing arrangement' in the Consumer Experience Guidelines.

¹⁴ Consumer Data Rule 4.27.

¹⁵ Consumer Data Rules may be made in relation to the notification requirements for that disclosure.

Chapter 11: Privacy Safeguard 11 — Quality of CDR data

Consultation draft, October 2019

Contents

Key points	3
What does Privacy Safeguard 11 say?	3
Why is it important?	3
Who does Privacy Safeguard 11 apply to?	4
How does Privacy Safeguard 11 interact with the Privacy Act?	4
Summary of application of Privacy Safeguard 11	4
What are the quality considerations?	5
Accurate	6
Up to date	6
Complete	6
Taking reasonable steps to ensure the quality of CDR data	7
When must an entity take reasonable steps?	7
What constitutes ‘reasonable steps’?	7
Examples of reasonable steps	8
Advising a CDR consumer when disclosed CDR data is incorrect	8
Data holders	9
Accredited data recipients	11
Disclosing corrected CDR data to the original recipient	11
When must an entity disclose corrected CDR data to the original recipient?	11
Record keeping requirements	12
How does Privacy Safeguard 11 interact with the other Privacy Safeguards?	13
Privacy Safeguard 1	13
Privacy Safeguard 5	13
Privacy Safeguard 10	13
Privacy Safeguard 12	14
Privacy Safeguard 13	14

Key points

- Privacy Safeguard 11, together with Consumer Data Rule 7.10, sets out obligations for data holders and accredited data recipients to:
 - ensure the quality of disclosed CDR data
 - inform CDR consumers in the event incorrect CDR data is disclosed, and
 - disclose corrected CDR data to the original recipient where requested by the affected CDR consumer.

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 Consumer Data Rules, and
- accredited data recipients who are disclosing CDR data when authorised or required under the Consumer Data 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 CDR consumer in accordance with the Consumer Data 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 CDR consumer to disclose corrected CDR data to the original recipient.

11.2 Privacy Safeguard 11 provides that holding CDR data so that it can be disclosed as required under the Consumer Data Rules is not a purpose when working out the purposes for which the CDR data is or was held.

11.3 Consumer Data Rule 7.10 requires a data holder who has disclosed incorrect CDR data to an accredited person to provide the CDR consumer with a written notice that identifies the accredited person and the incorrect CDR data, states the date of the disclosure, and states that the data holder must disclose the corrected data to that accredited person if the consumer requests them to do so.

Why is it important?

11.4 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 regime.

11.5 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 correct any inaccuracies in their data after it is shared.

- 11.6 This allows consumers to enjoy the benefits of the CDR regime, 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?

- 11.7 Privacy Safeguard 11 applies to data holders and accredited data recipients. It does not apply to designated gateways.

How does Privacy Safeguard 11 interact with the Privacy Act?

- 11.8 It is important to understand how Privacy Safeguard 11 interacts with the Privacy Act 1988 (the Privacy Act) and Australian Privacy Principles (APPs).¹
- 11.9 Like Privacy Safeguard 11, APP 10 requires APP entities to take reasonable steps to ensure the quality of personal information in certain circumstances.
- 11.10 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.
- 11.11 Although Privacy Safeguard 11 applies only in relation to the *disclosure* of CDR data, good practices and procedures to 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 regime.

Summary of application of Privacy Safeguard 11

CDR entity	Privacy principle that applies to CDR data
Accredited person	Australian Privacy Principle 10 APP 10 applies to any personal information held by accredited persons who are not yet accredited data recipients. ²
Accredited data recipient	Privacy Safeguard 11 Privacy Safeguard 11 applies instead of APP 10, ³ meaning APP 10 will not apply to CDR data that has been received by an accredited data recipient through the CDR regime. APP 10 will continue to apply to any personal information collected by the accredited person that is not CDR data. ⁴

¹ The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies (APP entities).

² An accredited person will become an accredited data recipient of CDR data upon being disclosed CDR data under the Consumer Data Rules (unless they are a data holder or designated gateway for the data) (see s 56AK).

³ 56EC(4)(a).

⁴ All accredited persons are subject to the Privacy Act and the APPs in relation to information that is personal information but is not CDR data. This means that non-CDR personal information handling by accredited persons is covered by the

CDR entity	Privacy principle that applies to CDR data
Data holder	<p>Privacy Safeguard 11</p> <p>Privacy Safeguard 11 applies instead of APP 10 for a disclosure of CDR data,⁵ meaning APP 10 will not apply to CDR data that a data holder is authorised or required to disclose under the Consumer Data Rules.</p> <p>However, APP 10 continues to apply to data holders in respect of the collection and use of CDR data that is also personal information, and in respect of CDR data that is also personal information which is disclosed otherwise than under the Consumer Data Rules (for instance, to a third party service provider).</p> <p>This means that APP 10 continues to apply to all personal information (and CDR data that is also personal information) that a data holder collects, uses or discloses where the entity is not required or authorised to disclose the data under the Consumer Data Rules.</p>
Designated gateway	<p>Australian Privacy Principle 10</p> <p>Privacy Safeguard 11 does not apply to a designated gateway, meaning the obligation to ensure the quality of personal information in APP 10 will continue to apply to a designated gateway that is an APP entity.</p>

What are the quality considerations?

- 11.12 The three quality considerations under Privacy Safeguard 11 are ‘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**.
- 11.13 When working out the purpose for which the CDR data is or was held, entities should disregard the purpose of holding the CDR data so that it can be disclosed as required under the Consumer Data Rules. 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 regime. ‘Purpose’ is discussed further in Chapter B (Key Concepts).
- 11.14 The three terms listed in Privacy Safeguard 11, ‘accurate’, ‘up to date’, and ‘complete’, are not defined in the Competition and Consumer Act or the Privacy Act.⁶ The following analysis of each term draws on the ordinary meaning of the terms and the APP Guidelines.⁷ As the analysis indicates, there is overlap in the meaning of the terms.

Privacy Act and the APPs, while the handling of CDR data is covered by the CDR regime and the Privacy Safeguards. See s 6E(1D) of the Privacy Act.

⁵ 56EC(4)(b).

⁶ 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 CDR consumer to correct the CDR data (see Chapter 13 (Privacy Safeguard 13)).

⁷ See OAIC, Australian Privacy Principles Guidelines (22 July 2019), Chapter 10 APP 10 — Quality of personal information.

Accurate

- 11.15 CDR data is inaccurate if it contains an error or defect or is misleading. An example is incorrect factual information about a CDR consumer's income, assets, loan repayment history or employment status.
- 11.16 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. 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). For instance, an accredited data recipient may use an algorithm to determine a CDR consumer's projected 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, it will not be inaccurate because, for instance, the consumer believes their income will be higher or lower during the projected period.

Up to date

- 11.17 CDR data is not up to date if it contains information that is no longer current. An example is a statement that a CDR consumer has an active account with a certain bank, where the consumer has since closed that account. Another example is an assessment that a consumer has a certain ability to meet a loan repayment obligation, where in fact the consumer's ability has since changed.⁸
- 11.18 For example, CDR data about a past event may have been accurate 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.

Complete

- 11.19 CDR data is incomplete if it presents a partial or misleading picture, rather than a true or full picture.
- 11.20 An example is data from which it can be inferred that a CDR 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.

⁸ Such an assessment will likely be 'materially enhanced information' under section 10 of the Designation Instrument and therefore not 'required consumer data' under the Consumer Data Rules.

Taking reasonable steps to ensure the quality of CDR data

When must an entity take reasonable steps?

- 11.21 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 Consumer Data Rules
 - **for accredited data recipients**, at the time the entity discloses CDR data when required or authorised under the Consumer Data Rules.
- 11.22 At other times, regular reviews of the quality of CDR data held by the entity may also ensure the CDR data is accurate, up-to-date and complete at the time it is disclosed.
- 11.23 Entities should also be aware that Privacy Safeguard 11 only requires an accredited data recipient to take reasonable steps when disclosing CDR data under the Consumer Data 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 consumer data rules’ is discussed in Chapter B (Key Concepts).
- 11.24 The obligation to take reasonable steps to ensure the quality of CDR data applies to accredited data recipients when disclosing CDR data:
- to the CDR consumer under Consumer Data Rules 7.5(1)(c) or 7.5(3), and
 - to an outsourced service provider under Consumer Data Rule 7.5(1)(d).

Risk point: If a data holder only takes steps to ensure the quality of CDR data at the time of the disclosure or authorisation, there is a greater risk that the data will be incorrect.

Privacy tip: While the obligation to ensure the quality of CDR data under Privacy Safeguard 11 only applies 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 and use for the purposes of APP 10.

What constitutes ‘reasonable steps’?

- 11.25 The requirement to ensure the quality of CDR data is qualified by a ‘reasonable steps’ test.
- 11.26 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.** An entity should consider the sensitivity of the data and possible adverse consequences for the consumer concerned if the CDR data is not correct. If a data holder is required or authorised to disclose data that is highly sensitive, the data holder would be required to take more extensive steps to ensure the quality of that data.
- **The possible adverse consequences for a consumer if the quality of CDR data is not ensured.** More rigorous steps may be required as the risk of adversity increases.
- **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.

11.27 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, it may be reasonable to take no steps to ensure the quality of that data. It is the responsibility of the entity to be able to justify that this is reasonable.

Examples of reasonable steps

11.28 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 reasonable steps to ensure the quality of CDR data the entity is authorised or required to disclose.
- 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 (such as algorithms) are operating appropriately and are fit for purpose, and not creating biased, inaccurate, discriminatory or unjustified results. This is because data derived from CDR data collected by an accredited data recipient continues to be ‘CDR data’.

Advising a CDR consumer when disclosed CDR data is incorrect

11.29 Consumer Data Rule 7.10 sets out the notice requirements with which a data holder must comply after disclosing incorrect CDR data to an accredited person. These notice requirements are summarised in paragraphs 11.31-11.42 below.

11.30 Consumer Data Rule 7.10 does not apply to accredited data recipients. There is no Consumer Data Rule in relation to accredited data recipients advising CDR consumers that disclosed CDR data was incorrect.

Data holders

When must a data holder advise a CDR consumer that disclosed CDR data was incorrect?

11.31 A data holder must advise a CDR consumer that some or all of the CDR data was incorrect if the entity⁹

- has disclosed CDR data after being required or authorised to do so under the Consumer Data Rules, and
- then becomes aware that the CDR data, when disclosed, was not accurate, up to date and complete, having regard to the purpose for which the data was held.

11.32 When considering whether to advise the consumer that incorrect CDR data was disclosed, it is not relevant whether the entity failed to take reasonable steps outlined in paragraph 11.25-11.27 of this chapter. It is sufficient that the CDR data was not accurate, up to date and complete when disclosed.

What information must a data holder provide to the consumer when incorrect CDR data has been disclosed?

11.33 Consumer Data Rule 7.10 requires a data holder that has disclosed incorrect CDR data to an accredited person to provide the consumer with a written notice that:

- identifies the accredited person,
- states the date of the disclosure,
- identifies which CDR data was incorrect, and
- states that the data holder must disclose the corrected data to that accredited person if the consumer requests that they do so.

11.34 A notice may deal with one or more disclosures of incorrect CDR data.

How must a notice be provided?

11.35 Consumer Data Rule 7.10 requires a data holder to notify the consumer by electronic means after disclosing incorrect data.

11.36 The requirement for this notice to be given by electronic means will be satisfied if the notice is given over email or over the CDR consumer's consumer dashboard.

11.37 The written notice may, for instance, be in the body of an email or in an electronic file attached to an email.

⁹ 56EN(3).

How quickly must data holders give notification to the consumer?

- 11.38 Data holders must provide notices to the consumer as soon as practicable, but no more than five business days after the data holder becomes aware that some or all of the disclosed data was incorrect.
- 11.39 The term ‘as soon as practicable’ is discussed in Chapter B (Key Concepts).
- 11.40 The test of practicability is an objective test. The data holder should be able to justify that it is not practicable to give notification promptly after becoming aware of the disclosure of incorrect CDR data.¹⁰
- 11.41 In adopting a timetable that is ‘practicable’ an entity can take technical and resource considerations into account. However, it is the responsibility of the data holder to be able to justify any delay in providing the notice.
- 11.42 The maximum time of five 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 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 CDR consumers.

Example

Free Bank Ltd is a data holder for a large number of CDR consumers. It is authorised by Yulia to disclose her CDR data relating to her residential mortgage product to an accredited person, Credibility Pty Ltd. Soon after the data is disclosed on 1 July, Credibility queries whether the variable interest rate relating to Yulia’s repayments is correct.

Free Bank then becomes aware that some of the disclosed data was incorrect when disclosed, because the applicable variable interest rate was not correct for a certain period. Within a number of hours, Free Bank is practicably able to provide a notice to Yulia over her consumer dashboard which states that:

- incorrect CDR data was given to Credibility on 1 July
- the data relating to her mortgage repayments was incorrect due to a mistake in the rate contained in the data, and
- Free Bank is required to disclose corrected data to Credibility if Yulia requests that they do so.

Free bank has electronically provided Yulia with the notice required under Consumer Data Rule 7.10 and Privacy Safeguard 11, as soon as practicable.

Free Bank then realises that the error is systemic and has caused Free Bank to have disclosed incorrect CDR data in respect of all similar disclosures to accredited persons since the variable rate change a number of months ago.

¹⁰ 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 CDR 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.

Free Bank hires external counsel and other experts to undertake an urgent review of its CDR disclosures and determine the extent of the error. It takes Free Bank almost five business days before it is in a position to send all affected CDR consumers a notice similar to the one given to Yulia.

Although Free Bank has taken almost 5 business days to send the affected CDR consumers the notices required by Consumer Data Rule 7.10 and Privacy Safeguard 11, it has done so as soon as practicable.

Accredited data recipients

Does an accredited data recipient need to advise CDR consumers if disclosed CDR data was incorrect?

11.43 For accredited data recipients, there is no Consumer Data Rule in relation to advising CDR consumers that disclosed CDR data was incorrect. This is because an accredited data recipient may only disclose CDR data if required or authorised under another Australian law or court/tribunal order,¹¹ or under the Consumer Data Rules to the consumer or an outsourced service provider.

11.44 If an accredited data recipient discloses CDR data:

- to the consumer, or an outsourced service provider in accordance with the Consumer Data Rules; or
- as required or authorised under another Australian law or court/tribunal order,

and that data is incorrect, the requirement to advise the CDR consumer does not apply as there are no Consumer Data Rules for the entity to follow.

Disclosing corrected CDR data to the original recipient

When must an entity disclose corrected CDR data to the original recipient?

11.45 Privacy Safeguard 11 requires a data holder to disclose corrected CDR data to the original recipient¹² of the disclosure if:¹³

- the entity has advised the CDR consumer that some or all of the CDR data was incorrect when the entity disclosed it, and

¹¹ 56EI(1)(c).

¹² The original recipient may be the CDR consumer where the data holder disclosed the CDR data to the consumer in response to a valid consumer request in accordance with Consumer Data Rule 3.4(2) or (3).

¹³ 56EN(4). Note that although this subsection is also expressed to apply to accredited data recipients, as there are no Consumer Data Rules for such entities to advise CDR consumers of disclosures of incorrect data under 56EN(3), the obligation in 56EN(4) does not currently apply to those entities.

- the CDR consumer requests the entity to disclose the corrected CDR data.
- 11.46 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.
- 11.47 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 under in accordance with s 56EP(3)(a)(i), and
 - for which a qualifying statement has been included in accordance with s 56EP(3)(a)(ii).
- 11.48 This means that if a data holder includes a qualifying statement with CDR data rather than correcting it in response to a request from the CDR consumer to correct the data, and the CDR data had been disclosed to an accredited person before the qualifying statement was included, Privacy Safeguard 11 requires the data holder to re-disclose that CDR data, which now includes the qualifying statement, to that accredited person.

Example

SuperGas Ltd is a data holder for CDR data. On 1 May, SuperGas discloses Gudny’s CDR data to an accredited person in response to Gudny’s valid request. The CDR data includes readings from a gas meter at Gudny’s residence that, for reasons outside SuperGas’ control, is faulty.

After receiving her latest gas bill, Gudny realises that the gas meter is faulty and notifies SuperGas through the customer service portal on its website. SuperGas arranges for the meter to be fixed.

SuperGas determines that the gas usage data it holds for Gudny is inaccurate, given that it is held for the purposes of billing Gudny under her gas contract and allowing Gudny to track her usage, among other things.

SuperGas notifies Gudny over her consumer dashboard in compliance with Consumer Data Rule 7.10. The notice states that the gas usage data disclosed to the accredited person was incorrect, due to the faulty readings.

Gudny requests SuperGas to disclose corrected data to the recipient.

This example is continued below.

Record keeping requirements

- 11.49 If an entity discloses corrected CDR data in accordance with Privacy Safeguard 11,¹⁴ the entity (and, if the data is disclosed to an accredited person, the recipient) should ensure that they comply with the record keeping requirements under Consumer Data Rule 9.3.
- 11.50 For data holders, Consumer Data Rule 9.3(1) 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.¹⁵ If corrected data is disclosed, the data holder must

¹⁴ 56EN(4).

¹⁵ Consumer Data Rule 9.3(1)(d).

keep and maintain a record of both the initial disclosure in which incorrect CDR was disclosed, and the subsequent disclosure in which the corrected data was disclosed. This is because both disclosures are made in response to the original consumer data request.

- 11.51 For accredited data recipients, Consumer Data Rule 9.3(2) requires the recipient to keep and maintain various records relating to CDR data, including records of the types of CDR data collected under the Consumer Data Rules.¹⁶ There is no requirement for an accredited data recipient to keep and maintain a record of the collection of the corrected data. However, the accredited data recipient is required to notify the consumer of the collection (see 11.54 below).

How does Privacy Safeguard 11 interact with the other Privacy Safeguards?

Privacy Safeguard 1

- 11.52 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 11.

Privacy Safeguard 5

- 11.53 Privacy Safeguard 5 requires an accredited data recipient to notify a CDR consumer of the collection of their CDR data by updating the CDR consumer's consumer dashboard.
- 11.54 Where an accredited data recipient has collected CDR data, and then collects corrected data after the data holder complies with the consumer's requests 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

- 11.55 Privacy Safeguard 10 requires data holders to notify a CDR consumer of the disclosure of their CDR data by updating the CDR consumer's consumer dashboard.
- 11.56 Where a data holder has disclosed CDR data, and then discloses corrected data as the result of the consumer's requests to correct and disclose corrected data under Privacy Safeguards 11 and 13, the data holder must notify that consumer under Privacy Safeguard 10 in respect of both disclosures.

Example

Phoney Phones Ltd, a data holder, discloses Satoko's CDR data to accredited person, Bill Balancer Pty Ltd, in response to a consumer data request made on Satoko's behalf.

Phoney Phones updates Satoko's consumer dashboard under Privacy Safeguard 10 and Consumer Data Rule 7.9, and Bill Balancer updates Satoko's consumer dashboard under Privacy Safeguard 5 and Consumer Data Rule 7.4.

¹⁶ Consumer Data Rule 9.3(2)(e).

Phoney Phones, through its own inquiries, then becomes aware that the data was incorrect when disclosed.

Pursuant to Privacy Safeguard 11 and Consumer Data Rule 7.10, Phoney Phones advises Satoko that incorrect data was disclosed, through her consumer dashboard.

Satoko requests Phoney Phones to disclose corrected CDR data to Bill Balancer under Privacy Safeguard 11.¹⁷

Phoney Phones corrects the CDR data in accordance with Privacy Safeguard 13 and Consumer Data Rule 7.15.

Phoney Phones complies with Satoko's request to disclose corrected CDR data. Both Bill Balancer and Phoney Phones update Satoko's consumer dashboards accordingly.

Privacy Safeguard 12

- 11.57 Where an accredited data recipient amends or creates an updated copy of 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 redundant data that it holds (for example a copy of that information).

Privacy Safeguard 13

- 11.58 Privacy Safeguard 13 requires data holders and accredited data recipients to respond to a CDR consumer request for correction of their CDR data including by taking steps to correct the CDR data or by including a qualifying statement with the CDR data to ensure its accuracy.¹⁸
- 11.59 A data holder that corrects CDR data or includes a qualifying statement with the data in accordance with Privacy Safeguard 13 should consider whether the CDR consumer must be advised of any previous disclosures of the CDR data where the data may have been incorrect when it was disclosed, in accordance with Privacy Safeguard 11. In such circumstances the data holder will be on notice that CDR data was likely incorrect when disclosed.

Example

This example follows the example under the heading 'When must an entity disclose corrected CDR data to the original recipient?', above.

SuperGas receives Gudny's request to disclose her corrected CDR data. A SuperGas customer service officer promptly sends Gudny an email acknowledging receipt of her request.

This request is necessarily also a request under Privacy Safeguard 13 to correct the data. SuperGas determines that it cannot correct the CDR data as there is no method of determining Gudny's actual gas usage for the period in which the gas meter was faulty.

¹⁷ As explained in 13.50 of Chapter 13 (Privacy Safeguard 13), a request under section 56EN(4) is necessarily a request for the data holder to correct the CDR data under 56EP(1).

¹⁸ 56EP(3)(a).

SuperGas therefore includes a statement with the CDR data that, for the particular period, there was a fault with the gas meter which recorded the data and the exact gas usage cannot be accurately determined. SuperGas also attaches an electronic link to its digital record of the data.

SuperGas then sends Gudny both an email and a message through her consumer dashboard explaining that SuperGas has included the statement with her data, as correction of the data was not possible, and sets out the complaint mechanisms available to her.

SuperGas then re-discloses the data, which now includes the qualifying statement, to the accredited person.

Chapter 12:

Privacy Safeguard 12 —

Security of CDR data, and destruction or de-identification of redundant CDR data

Consultation draft, October 2019

Contents

Key points	3
What does Privacy Safeguard 12 say?	3
Why is it important?	3
Who does Privacy Safeguard 12 apply to?	4
Accreditation guidelines on information security	4
How Privacy Safeguard 12 interacts with the Privacy Act	4
Summary of application of Privacy Safeguard 12 by CDR entity	5
PART A: Security of CDR data	6
What do security measures need to protect against?	6
What steps does an entity need to take to secure CDR data?	7
Notifiable Data Breach (NDB) scheme	16
PART B: Treatment of redundant data (destruction and de-identification)	18
Overview of the process for treating redundant data	18
What is ‘redundant CDR data’?	18
Deciding how to deal with redundant data	19
Steps to destroy redundant data	21
Steps to de-identify redundant data	23
Other relevant security obligations	24
Privacy Safeguards	24

Key points

- Securing CDR data is an integral element of the Consumer Data Right (CDR) regime.
- Privacy Safeguard 12 places requirements on accredited data recipients 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.
- In addition, if an accredited data recipient or a designated gateway no longer needs the CDR data for purposes permitted by privacy safeguards or the Consumer Data Rules, then the data is considered 'redundant data' and will need to be destroyed 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 regime.

What does Privacy Safeguard 12 say?

- 12.1 Accredited data recipients and designated gateways must take the steps in the Consumer Data Rules to protect the CDR data from misuse, interference and loss, as well as unauthorised access, modification and disclosure.
- 12.2 Accredited data recipients and designated gateways must also take the steps set out in the Consumer Data Rules to destroy or de-identify any CDR data that is no longer needed for:
- the purposes permitted under the Consumer Data 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. Accredited data recipients 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 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 or designated gateway is a party.

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 OAIC’s long-running [national community attitudes to privacy survey](#), privacy protection contributes to an individual’s trust in an entity.¹ If an entity is perceived to be handling data contrary to community expectations, individuals may seek out alternative products and services.

Who does Privacy Safeguard 12 apply to?

12.7 Privacy Safeguard 12 applies to accredited data recipients and designated gateways. It does not apply to data holders.

Note: *Currently, there are no designated gateways in the CDR regime responsible for facilitating the transfer of information between data holders and accredited persons (see Chapter B: Key Concepts for the meaning of designated gateway).*

Accreditation guidelines on information security

12.8 This chapter provides guidance on the steps for securing CDR data and managing redundant CDR data in compliance with Privacy Safeguard 12.

12.9 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 regime.

12.10 Accredited persons should refer to the [Draft Supplementary Accreditation Guidelines on Information Security](#) by the Australian Competition and Consumer Commission (ACCC) for specific guidance on the:

- information security obligations under Privacy Safeguard 12 applicants must satisfy for accreditation under the CDR regime, 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

12.11 It is important to understand how Privacy Safeguard 12 interacts with the *Privacy Act 1988* (Cth) (Privacy Act) and Australian Privacy Principles (APPs).²

12.12 Like Privacy Safeguard 12, 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

² The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies (APP entities). See also Chapter B: Key Concepts of the APP guidelines.

² The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies (APP entities). See also Chapter B: Key Concepts of the APP guidelines.

retain this personal information (see [Chapter 11: APP 11 – Security of personal information of the APP Guidelines](#)).

Summary of application of Privacy Safeguard 12 by CDR entity

CDR entity	Security principle that applies to CDR data
Accredited data recipient	<p>Privacy Safeguard 12</p> <p>Privacy Safeguard 12 will apply to CDR data an accredited data recipient has received through the CDR regime.</p> <p>However, the Privacy Act and APP 11 will continue to apply to any personal information handled by the accredited data recipient that is not CDR data.³</p> <p>All accredited data recipients are subject to the Privacy Act and the APPs in relation to information that is personal information but is not CDR data.</p>
Designated gateways	<p>Privacy Safeguard 12</p> <p>Privacy Safeguard 12 applies instead of APP 11, meaning APP 11 will not apply to CDR data that a designated gateway is the gateway for under the CDR regime.</p> <p>APP 11 will continue to apply to any personal information handled by the designated gateway that is not CDR data.</p>
Data holders	<p>Australian Privacy Principle 11</p> <p>Privacy Safeguard 12 does not apply to data holders, meaning the security obligations in APP 11 will continue to apply to data holders.</p>

³ All accredited data recipients are subject to the Privacy Act and the APPs in relation to information that is personal information but is not CDR data. This means that non-CDR personal information handling by accredited data recipients is covered by the Privacy Act and the APPs, while the handling of CDR data is covered by the CDR regime and the Privacy Safeguards. See s 6E(1D) of the Privacy Act.

PART A: Security of CDR data

What do security measures need to protect against?

- 12.13 An accredited data recipient is required to put in place specific information security measures to protect the CDR data they receive from misuse, interference and loss, as well as unauthorised access, modification and disclosure.
- 12.14 A designated gateway of CDR data is required to put in place information security measures to protect that CDR data from misuse, interference and loss, as well as unauthorised access, modification and disclosure.
- 12.15 The terms ‘misuse’, ‘interference’, ‘loss’ and ‘unauthorised access’ are not defined in the CDR regime. 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 to include an exhaustive list of examples.
- **Misuse** occurs where CDR data is used for a purpose not permitted by the CDR. For example, misuse would occur if an employee of a CDR entity browses consumer statements to discover information about someone they know.⁴
 - **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 unauthorised access or disclosure. Examples of loss include physical loss by leaving data in a public place, failing to keep adequate backups in the event of systems failure or as a result of natural disasters.⁵
 - **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 access 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 and releases that information from its effective control in a

⁴ Privacy Safeguard 6 sets out when an accredited data recipient of CDR data or a designated gateway of CDR data is permitted to use that CDR data (see Chapter 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 and 9). ‘Use’ is discussed in more detail in Chapter B (Key concepts).

⁵ Loss does not apply to intentional destruction or de-identification of CDR data undertaken in accordance with the Consumer Data Rules.

way that is not permitted by the CDR regime. 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.

- 12.16 Information security not only covers cybersecurity (the protection of your networks and information systems from attack), but also physical and organisational security measures.

What steps does an entity need to take to secure CDR data?

- 12.17 Privacy Safeguard 12 requires an accredited data recipient and designated gateway to take the steps in the Consumer Data 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 Consumer Data Rules.

- 12.18 The Consumer Data 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.

- 12.19 Broadly, the steps to manage the information security of CDR data are:

- **Step 1:** define and implement security governance in relation to CDR data.
- **Step 2:** define the boundaries of the CDR data environment.
- **Step 3:** have and maintain an information security capability (including minimum security controls set out in Part 2 of Schedule 2 of the Consumer Data Rules).
- **Step 4:** implement a formal controls assessment program.
- **Step 5:** manage and report security incidents.

- 12.20 This section summarises what is required by these steps and provides guidance on how accredited data recipients may implement them.

- 12.21 The five 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.

Steps for managing the information security of CDR data



Define and implement security governance



Define the boundaries of the CDR data environment



Have and maintain an information security capability



Implement a formal controls assessment program



Manage and report security incidents



Step 1: Define and implement security governance in relation to CDR Data

Information security governance framework

- 12.22 The Consumer Data Rules require an accredited data recipient to establish and maintain a formal governance framework⁶ for managing information security risks relating to CDR data.
- 12.23 An accredited data recipient may leverage their existing information security governance structure and extend it to their CDR data environment.⁷ An accredited data recipient may also utilise existing frameworks, requirements and models in developing their information security governance framework and defining security areas.⁸
- 12.24 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.
- 12.25 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

⁶ A formal governance framework refers to policies, processes, roles and responsibilities required to facilitate the oversight and management of information security.

⁷ For further information, see the ACCC's [Draft Supplementary Accreditation Guidelines on Information Security](#).

⁸ The ACCC's [Draft Supplementary Accreditation Guidelines on 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.

- 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.

12.26 Accredited data recipients are subject to audit requirements set out in the ACCC's [Draft Supplementary Accreditation Guidelines on 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 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

- 12.27 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.⁹
- 12.28 Accredited data recipients may choose to document these practices and procedures as part of the information security policy required by the Consumer Data Rules (see paragraphs 12.32–12.36 below) or as a separate document.
- 12.29 Senior management will have ultimate responsibility for the management of information security.¹⁰ Senior management should implement the necessary practices, procedures, resources and training to allow the accredited data recipient to effectively discharge its responsibilities under the Consumer Data Rules.¹¹
- 12.30 An accredited data recipient should establish formal security governance structures, such as committees and forums, to oversee the security of CDR data.¹² These committees or forums should include membership from across key business areas, particularly where the entity's CDR data environment is large or complex,¹³ so information is an integrated component of the accredited data recipient's entire business and not left to the compliance or ICT area alone.
- 12.31 An accredited data recipient's formal security should have clear procedures for oversight and accountability, and clear lines of authority for decisions regarding the security of CDR data.

⁹ sub-clause 1.3(2) of Schedule 2 of the [Consumer Data Rules](#).

¹⁰ 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 is an associated person (i.e. a person who makes or participates in making, or would (if the other person were an accredited person) make or participate in making, decisions that affect the management of CDR data by the other person) of the accredited data recipient: sub-clause 1.2 of Schedule 2 of the Consumer Data Rules.

¹¹ The ACCC's [Draft Supplementary Accreditation Guidelines on Information Security](#).

¹² The ACCC's [Draft Supplementary Accreditation Guidelines on Information Security](#).

¹³ The ACCC's [Draft Supplementary Accreditation Guidelines on 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
- 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 (e.g. committees and forums).

Information security policy

12.32 Accredited data recipients must have and maintain an information security policy that governs information security across its organisation.¹⁴

12.33 The information security policy must include information about¹⁵:

- its information security risk posture (that is, the exposure and potential harm to an 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.

12.34 The information security policy should be internally and externally enforceable. Compliance with the policy should also be monitored.¹⁶

12.35 Accredited data recipients 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.

¹⁴ sub-clause 1.3(3) of Schedule 2 of the Consumer Data Rules.

¹⁵ sub-clause 1.3(3) of Schedule 2 of the Consumer Data Rules.

¹⁶ The term 'enforceable' is defined in the ACCC's [Draft Supplementary Accreditation Guidelines on Information Security](#) as both internally and externally, 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 construal requirements and ongoing third party monitoring processes.

- 12.36 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

- 12.37 The accredited data recipient must review and update the Information Governance framework for appropriateness:
- a. in response to material changes to both the extent and nature of threats to its CDR data environment and its operating environment, or
 - b. where no such material changes occur—at least annually.¹⁷

What is a material change?

A material change is one that significantly changes the scope of the CDR data environment, such as the introduction of a new system, the migration of data onto new infrastructure, introduction of a new outsourced service provider, or a change to the terms and conditions of the services provided by an existing outsourced service provider.¹⁸

Step 2: Define the boundaries of the CDR data environment

- 12.38 An accredited data recipient must assess, define and document its CDR data environment. 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 outsourced service provider or third party.¹⁹
- 12.39 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 privacy, procedures and systems are up to date.

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 disclosed to outsourced service providers. The documented analysis should generally include information about:

¹⁷ Sub-clause 1.3(4) of Schedule 2 of the Consumer Data Rules.

¹⁸ The ACCC’s [Draft Supplementary Accreditation Guidelines on Information Security](#).

¹⁹ The ACCC’s [Draft Supplementary Accreditation Guidelines on Information Security](#).

People: Who will have access to CDR data? Who will authorise access?

Technology: Such as information systems, storage systems (including whether it 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, thereby increasing the risk of unauthorised disclosure or access.

12.40 This can either be documented through a data flow diagram or a written statement.²⁰

12.41 Accredited data recipients need to review their CDR data environment for completeness and accuracy:

- as soon as practicable when they become aware of material changes²¹ 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

12.42 The Consumer Data 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 Consumer Data 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, 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.

12.43 The accredited data recipient must review and adjust its information security capability.

²⁰ For further information see the Supplementary accreditation guidelines: information security.

²¹ A material change is one that significantly changes the scope of the CDR data environment, such as the introduction of a new system, the migration of data onto new infrastructure, introduction of a new outsourced service provider, or a change to the terms and conditions of the services provided by an existing outsourced service provider.

Information security controls

- 12.44 The Consumer Data 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 of the Consumer Data Rules.
- 12.45 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.
- 12.46 Compliance with Privacy Safeguard 12 requires the implementation of these controls across the CDR environment.
- 12.47 The information security controls in Part 2, Schedule 2 of the Consumer Data 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.
- 12.48 Further information regarding the minimum information security controls is contained in the ACCC's [Draft Supplementary Accreditation Guidelines on Information Security](#).

Additional security controls required to respond to risks to information security

- 12.49 In addition to the information security controls set out in Part 2 Schedule 2 of the Consumer Data 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.
- 12.50 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.

Outsourced service provider information security capability

- 12.51 Where an accredited data recipient uses an outsourced service provider to provide goods or services to a consumer, the accredited data recipient must ensure their contract with the

outsourced service provider requires them to take the steps outlined in Schedule 2 as if the outsourced service provider were an accredited data recipient.²²

12.52 To comply with this requirement, accredited data recipients may consider the following when engaging an outsourced provider:

- assessing whether the information security capabilities of the outsourced service provider, 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 the Consumer Data Rules and the security controls set out in Part 2 of the Consumer Data Rules
- requesting and reviewing information from the outsourced service provider such as vulnerability and penetration testing reports, internal audit reports, and other information security assessments and questionnaires
- including contractual provisions regarding security capability reflecting the definition of a CDR outsourcing arrangement in the Consumer Data Rules.²³

Reviewing security capability

12.53 Under the Consumer Data 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.²⁴

12.54 Where changes in the operations of the accredited data recipient could lead to changes in its risk posture (e.g. 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 the accredited data recipient’s information security risks.

Step 4: implement a formal controls assessment program

Assessing the effectiveness of controls

12.55 An accredited data recipient must establish and implement a testing program to review and assess the effectiveness of its information security capability.

12.56 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

²² Consumer Data Rule 1.10(2)(b)(i).

²³ Consumer Data Rule 1.10(2).

²⁴ sub-clause 1.5(2) of Schedule 2 of the Consumer Data Rules

- 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.²⁵
- 12.57 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.²⁶
- 12.58 In order to maintain accreditation under the CDR framework, an accredited person must also provide regular attestation statements and assurance reports to the Data Recipient Accreditor.²⁷ More information can be found in the ACCC’s [Draft Supplementary Accreditation Guidelines on Information Security](#).
- 12.59 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 regime obligations and the control requirements in Part 2 of Schedule 2 of the Consumer Data Rules.²⁸
- 12.60 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.²⁹
- 12.61 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.³⁰
- 12.62 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 its CDR data environment — as soon as practicable, or
 - b. where no such material changes occur — at least annually.³¹

Step 5: Manage and report security incidents

- 12.63 An accredited data recipient must have procedures and practices in place to detect, record, and respond to information security incidents as soon as practicable.³² More detail about maintaining these practices can be found in ACCC’s [Draft Supplementary Accreditation Guidelines on Information Security](#).

²⁵ sub-clause 1.6(1)(a) of Schedule 2 of the Consumer Data Rules.

²⁶ sub-clause 1.6(1)(b) of Schedule 2 of the Consumer Data Rules.

²⁷ sub-clause 2.1(2) of Schedule 1 of the Consumer Data Rules.

²⁸ sub-clause 1.6(2) of Schedule 2 of the Consumer Data Rules.

²⁹ sub-clause 1.6(3) of Schedule 2 of the Consumer Data Rules.

³⁰ sub-clause 1.6(4) of Schedule 2 of the Consumer Data Rules.

³¹ sub-clause 1.6(4) of Schedule 2 of the Consumer Data Rules.

³² sub-clause 1.7(1) of Schedule 2 of the Consumer Data Rules.

- 12.64 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.³³
- 12.65 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; and
 - b. notifying CDR data security breaches to the Information Commissioner and to consumers as required under Part IIIC of the *Privacy Act 1988*,³⁴ 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.
- 12.66 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 its 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.³⁵

Notifiable Data Breach (NDB) scheme

- 12.67 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'.³⁶
- 12.68 Under the NDB scheme, accredited data recipients are required to notify affected individuals and the Information Commissioner in the event of an 'eligible data breach' under the NDB scheme.³⁷
- 12.69 A data breach is eligible if it is likely to result in serious harm to any of the individuals 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.
- 12.70 For more information, see the OAIC's [Notifiable Data Breaches scheme webpage](#).

³³ sub-clause 1.7(2) of Schedule 2 of the Consumer Data Rules.

³⁴ See the 'Notifiable Data Breach (NDB) scheme' section further below in this Chapter.

³⁵ sub-clause 1.7(4) of Schedule 2 of the Consumer Data Rules.

³⁶ 56ES.

³⁷ See Part IIIC, Division 3 of the Privacy Act. See generally the OAIC's [Notifiable Data Breaches scheme webpage](#) for further information.

The OAIC has developed the [Data breach preparation and response guide – A guide to managing data breaches in accordance with the Privacy Act 1988 \(Cth\)](#) 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 data breach preparation and response guide are useful and applicable to CDR data security breaches.³⁸

³⁸ The notifiable data breaches provisions of the Privacy Act apply in CDR as if personal information was ‘CDR data’ (see s 56ES).

PART B: Treatment of redundant data (destruction and de-identification)

Overview of the process for treating redundant data

- 12.71 An accredited data recipient must destroy or de-identify CDR data that has become ‘redundant’. This means that, if the accredited data recipient no longer has a reason to keep the CDR data, it must destroy it or de-identify it.
- 12.72 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 Consumer Data Rules and explained under the heading ‘Deciding how to deal with redundant data’ below. Whether a consumer has made an election to delete will be relevant to this decision.
- 12.73 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 Consumer Data Rules and outlined under the headings ‘Steps to destroy redundant data’ and ‘Steps to de-identify redundant data’ below.
- 12.74 Where the de-identification process does not apply or cannot result in de-identified information in accordance with the Consumer Data Rules, the destruction process must be followed as outlined under the heading ‘Steps to destroy redundant data’ below.

What is ‘redundant CDR data’?

- 12.75 ‘Redundant data’ is CDR data that:
- an accredited data recipient or designated gateway no longer needs for a purpose permitted under the Consumer Data Rules, or for any purpose for which it is allowed to be used or disclosed under the Privacy Safeguards
 - an accredited data recipient or designated gateway is not required to retain by or under an Australian law or a court/tribunal order, and
 - does not relate to any current or anticipated legal proceedings or dispute resolution proceedings to which the accredited data recipient or designated gateway is a party.
- 12.76 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, or³⁹
 - where a consumer withdraws their consent.⁴⁰
- 12.77 The terms ‘purpose’ (in the context of redundant CDR data) and ‘required by or under an Australian law or court/tribunal order’ are discussed in more detail in Chapter B (Key concepts).

³⁹ Consumer Data Rule 5.23(4)

⁴⁰ Consumer Data Rule 4.14(1)(a)

12.78 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 by external dispute resolution schemes.

Risk point: Entities risk keeping CDR data longer than they need to.

Privacy tip: Where laws prevent de-identification or destruction of redundant CDR 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 degree of information needed.

Deciding how to deal with redundant data

Step 1: Notification to consumer of matters relating to redundant data

General policy for dealing with redundant data

12.79 When seeking consent from a consumer to collect and use their CDR data⁴¹, 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.⁴²

The consumer’s right to elect for their redundant data to be deleted

12.80 If an accredited person’s general policy is either de-identification or deciding between destruction and deidentification when the CDR data becomes redundant, then the accredited data recipient must allow the consumer to elect for their redundant CDR data to be deleted.

12.81 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).⁴³

12.82 See [Chapter B \(Key Concepts\)](#) for further guidance about the meaning of ‘derived data’.

Step 2: Consider whether the redundant CDR data must be destroyed

12.83 In many cases, an accredited data recipient will not have the option to de-identify under the Consumer Data Rules, and the CDR data must be destroyed.

⁴¹ Consumer Data Rule 4.11(3)

⁴² Consumer Data Rule 4.17(1)

⁴³ Consumer Data Rule 4.16. See also ‘reasonably identifiable’ in [Chapter B \(Key Concepts\)](#).

- 12.84 The Consumer Data Rules require redundant CDR data to be destroyed where either:
- the consumer has elected for their redundant CDR data to be deleted, or
 - 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 destroying redundant CDR data. Where an accredited data recipient advised the consumer of a general policy of destruction, the recipient **must destroy the CDR data**, even if their general policy has since changed.

Step 3: If destruction isn't required, choose between destruction and de-identification

- 12.85 If there is 'no election to delete' in place and the entity did not advise the consumer that it has a general approach of destroying the CDR data, then the entity **can decide between destroying or de-identifying the CDR data** using the steps and processes contained in the Consumer Data Rules and outlined below.

Step 4: Destroying redundant data

- 12.86 If the accredited data recipient chooses under Step 3 (paragraph 12.85) to destroy the redundant CDR data, then they must proceed to destroy the data in accordance with the 'CDR data deletion process' set out in the Consumer Data Rules.⁴⁴ 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

- 12.87 Once an accredited data recipient has determined the de-identification process could apply and the 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 Consumer Data Rules.
- 12.88 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.⁴⁵
- 12.89 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 de-identification.

⁴⁴ Consumer Data Rule 1.18

⁴⁵ Consumer Data Rule 1.17(1)

- 12.90 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 released into an open environment, or what controls and safeguards apply to the data access environment).⁴⁶
- 12.91 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.
- 12.92 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 Consumer Data Rules. De-identification will generally only be appropriate where CDR data has been through an extremely robust de-identification process that ensures — with a very high degree of confidence — that no consumers are reasonably identifiable.
- 12.93 As a result, even if some CDR data is able to be sufficiently de-identified to this required extent, the utility of that data for many intended uses would likely be compromised.

De-identifying redundant CDR data (if de-identification is possible)

- 12.94 If, having taken the steps outlined above, the accredited data recipient determines that it is possible to de-identify the redundant CDR data, they can then proceed to de-identify the data in accordance with the ‘CDR data de-identification process’ set out in the Consumer Data Rules.⁴⁷ This process is explained further below under ‘Steps to de-identify redundant data’ in paragraph 12.106.

Destroying redundant CDR data (if de-identification is not possible)

- 12.95 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 Consumer Data Rules, and explained below under ‘Steps to destroy redundant data’ at paragraph 12.96.⁴⁸

Steps to destroy redundant data

- 12.96 The Consumer Data Rules set out the process to delete redundant data in the CDR data deletion process.⁴⁹
- 12.97 This process applies to both:
- the deletion of CDR data in response to a consumer’s election, and
 - where the entity otherwise chooses to delete the redundant data in order to comply with its Privacy Safeguard 12 obligations.

⁴⁶ Consumer Data Rule 1.17(2)(f)

⁴⁷ Consumer Data Rule 1.17

⁴⁸ Consumer Data Rule 1.17(4)

⁴⁹ Consumer Data Rule 1.18

Deleting the CDR data ‘to the extent reasonably practicable’

- 12.98 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.⁵⁰
- 12.99 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 outsourced service providers) — 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
 - the **practicability, including time and cost involved** — however an accredited data recipient is not excused from destroying 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 be deleted from backup systems?

- 12.100 The Consumer Data Rules recognise that irretrievable destruction of CDR data from a backup system is not always straightforward, and it may not be possible to achieve this immediately (for example, archived data that could be re-installed).
- 12.101 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, and⁵¹
 - commits to take reasonable steps to irretrievably destroy the personal information if, or when, this becomes possible.
- 12.102 It is important to note that the accredited data recipient must continue to take reasonable steps to work towards a solution to eventually destroy the CDR data.

⁵⁰ Consumer Data Rule 1.18(a)

⁵¹ This should go beyond the minimum access controls specified in the Consumer Data Rules.

Make a record to evidence the deletion

12.103 The accredited data recipient must also make a record to evidence the deletion.⁵²

12.104 Accredited data recipients should take care to ensure that the record does not include CDR data relating to a consumer.

12.105 The accredited data recipient must also direct any other person to which it has disclosed that CDR data to:

- delete, to the extent reasonably practicable, any copies of that CDR data, or any CDR data directly or indirectly derived from it, that it holds
- make a record to evidence the steps taken to delete the CDR data, and
- notify the person who gave the direction of the deletion.⁵³

Steps to de-identify redundant data

12.106 If the accredited data recipient determines that it is possible to de-identify the data, it must determine and apply the appropriate de-identification technique.⁵⁴

12.107 Specifically, the accredited data recipient must:

- determine the technique that is appropriate in the circumstances, and
- apply that technique 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 in order to ensure that no person is any longer identifiable or reasonably identifiable.⁵⁵

12.108 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
- any persons to whom the de-identified data is disclosed.

12.109 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 (see paragraph 12.95 above).

⁵² Consumer Data Rule 1.18(b)

⁵³ Consumer Data Rule 1.18(c)

⁵⁴ Consumer Data Rule 1.17(3)

⁵⁵ Consumer Data Rule 1.17(3)

Outsourced Service Providers

- 12.110 Accredited data recipients undertaking the de-identification process must also direct any outsourced service providers⁵⁶ to return or delete the redundant data.
- 12.111 An accredited data recipient must direct any outsourced service providers to either return the data to the accredited data recipient or delete it, as well as any data directly or indirectly derived from the CDR data.⁵⁷
- 12.112 Where the accredited data recipient receives redundant data from an outsourced service provider, it must then de-identify the data in accordance with the CDR de-identification process, as it would with any other redundant data.
- 12.113 The accredited data recipient is responsible for making these directions to any other person who has received the data. If the outsourced service provider has also disclosed the data to another person, the accredited data recipient must also direct that person to return or delete the data. If the person has also disclosed the data, the same obligations apply to the accredited data recipient, and so on.⁵⁸

Other relevant security obligations

Privacy Safeguards

- 12.114 Compliance with the Privacy Safeguards as a whole will promote security and reduce the risk of CDR data being accidentally or deliberately comprised. This is because the Privacy 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.
- 12.115 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.
- 12.116 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.
- 12.117 Privacy Safeguard 4 contains requirements to destroy information if it is unsolicited and not required to be retained by the entity. 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.

⁵⁶ For information on outsourced service providers, see [Chapter B \(Key Concepts\)](#).

⁵⁷ Consumer Data Rule 7.12(2)(b)

⁵⁸ Consumer Data Rule 7.12(2)(b)(ii)

Chapter 13:

Privacy Safeguard 13 —

Correction of CDR data

Consultation draft, October 2019

Contents

Key points	3
What does Privacy Safeguard 13 say?	3
Why is it important?	3
Who does Privacy Safeguard 13 apply to?	4
How Privacy Safeguard 13 interacts with the Privacy Act	4
Summary of application of Privacy Safeguard 13 by CDR entity	4
When must an entity correct CDR data?	5
Actioning and responding to correct requests	6
Acknowledging receipt of correction requests	6
Taking action to correct, or qualify, the CDR data	6
When action is not necessary in response to a request	7
How must a correction notice be provided to consumers?	8
What must be included in a correction notice to consumers?	8
What are the correction considerations?	9
Accurate	9
Up to date	10
Complete	10
Not misleading	10
Charges to correct CDR data	11
Interaction with other Privacy Safeguards	11
Privacy Safeguard 5	11
Privacy Safeguard 10	11
Privacy Safeguard 11	11
Privacy Safeguard 12	12

Key points

- Privacy Safeguard 13, together with Consumer Data Rules 7.14 and 7.15, sets out obligations for data holders and accredited data recipients to:
 - respond to correction requests made by CDR consumers in respect of CDR data, and to take certain steps to correct or include a qualifying statement in respect of the data, and
 - give the CDR consumer notice of any correction or statement made in response to their request, or reasons why a correction or statement is unnecessary or inappropriate.

What does Privacy Safeguard 13 say?

13.1 Privacy Safeguard 13 requires data holders and accredited data recipients who:

- receive a request from a CDR consumer to correct CDR data, and
- in the case of data holders, were earlier required or authorised under the Consumer Data Rules to disclose the CDR data,¹

to respond to the request by taking the relevant steps set out in the Consumer Data Rules.

13.2 Consumer Data Rule 7.15 requires an entity to acknowledge receipt of the request as soon as practicable and sets out how the entity must, to the extent it considers appropriate:

- correct the CDR data, or
- qualify the data by including a statement with it, and
- give the consumer a notice setting out how the entity responded to the request as well as the complaint mechanisms available to the consumer.

13.3 Consumer Data Rule 7.14 prohibits charging a fee for responding to or actioning a correction request.

Why is it important?

13.4 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 regime.

13.5 For consumers to have proper control over their data, they must be given the power to require the entities that have disclosed or collected their data to correct inaccuracies in that data.

13.6 Privacy Safeguard 13 does this by ensuring entities are required to correct inaccurate CDR data in certain circumstances when requested to do so by the consumer.

13.7 This allows consumers to enjoy the benefits of the CDR regime, such as receiving competitive offers from other service providers, as the data made available to sector participants can be relied upon.

¹ The reason for this requirement in respect of data holders is that a Consumer Data Rule can only affect a data holder and relate to the accuracy of CDR data if the rule also relates to the disclosure of the CDR data under the Consumer Data Rules (s 56BD(3)(b)).

Who does Privacy Safeguard 13 apply to?

- 13.8 Privacy Safeguard 13 applies to data holders and accredited data recipients for the CDR data. It does not apply to designated gateways.
- 13.9 Importantly, Privacy Safeguard 13 only applies to the CDR data a data holder was required or authorised to disclose under the Consumer Data Rules.²

How Privacy Safeguard 13 interacts with the Privacy Act

- 13.10 It is important to understand how Privacy Safeguard 13 interacts with the *Privacy Act 1988* (the Privacy Act) and Australian Privacy Principles (APPs).³
- 13.11 Like Privacy Safeguard 13, APP 13 requires an APP entity to correct personal information held by the entity in certain circumstances.

Summary of application of Privacy Safeguard 13 by CDR entity

CDR entity	Privacy principle that applies to CDR data
Accredited person	<p>Australian Privacy Principle 13</p> <p>APP 13 applies to any personal information held by accredited persons who are not yet accredited data recipients.⁴</p>
Accredited data recipient	<p>Privacy Safeguard 13</p> <p>Privacy Safeguard 13 applies instead of APP 13,⁵ meaning APP 13 will not apply to CDR data that has been received by an accredited data recipient through the CDR regime.</p> <p>APP 13 will continue to apply to any personal information collected by the accredited person that is not CDR data.⁶</p>

² 56EP(1)(c).

³ The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies (APP entities).

⁴ An accredited person will become an accredited data recipient of CDR data following receipt of CDR data under the Consumer Data Rules (unless they are a data holder or designated gateway for the data) (see s 56AK).

⁵ 56EC(4)(a).

⁶ All accredited persons are subject to the Privacy Act and the APPs in relation to information that is personal information but is not CDR data. This means that non-CDR personal information handling by accredited persons is covered by the Privacy Act and the APPs, while the handling of CDR data is covered by the CDR regime and the Privacy Safeguards. See s 6E(1D) of the Privacy Act.

CDR entity	Privacy principle that applies to CDR data
Data holder	<p>Australian Privacy Principle 13 and Privacy Safeguard 13 (depending on the circumstances)</p> <p>APP 13 applies to CDR data that is also personal information unless a consumer requests the data holder to correct CDR data.</p> <p>Where a consumer requests the data holder correct CDR data:</p> <ul style="list-style-type: none"> • Privacy Safeguard 13 applies instead of APP 13⁷ for CDR data disclosed under the Consumer Data Rules • APP 13 applies for CDR data which was disclosed otherwise than under the Consumer Data Rules⁸, where that CDR data is personal information. <p>This means that APP 13 continues to apply to all personal information (and CDR data that is personal information):</p> <ul style="list-style-type: none"> • where a data holder has not received a correction request, and • that a data holder discloses otherwise than under the Consumer Data Rules.
Designated gateway	<p>Australian Privacy Principle 13</p> <p>Privacy Safeguard 13 does not apply to a designated gateway.</p>

When must an entity correct CDR data?

13.12 Privacy Safeguard 13 and Consumer Data Rule 7.15 require an entity to correct or include a qualifying statement with CDR data after the CDR consumer has requested their CDR data be corrected, unless the entity does not consider a correction or statement to be appropriate.⁹

Example

Kiefer requests his bank, Money Mattress Ltd, a data holder of his CDR data, to correct his recent transaction data after he becomes a victim of credit card fraud. The request is made over the phone.

The Money Mattress phone operator acknowledges receipt of the request immediately, over the phone, and arranges for Keifer's consumer dashboard to be updated to reflect that the request was made. Money Mattress' systems show that the bank was earlier required to disclose the data to accredited person, Safer Money Pty Ltd, under Consumer Data Rule 4.6(4).

⁷ 56EC(4)(b).

⁸ For instance, to a third party service provider.

⁹ For data holders, this obligation only arises if the entity was required or authorised under the Consumer Data Rules to disclose the CDR data.

Money Mattress determines that for one month, incorrect as well as correct transaction data is recorded. In order to correct the data, Money Mattress considers the appropriate course is to delete the incorrect data and retain the correct data.

Actioning and responding to correct requests

Acknowledging receipt of correction requests

- 13.13 When a consumer makes a request to correct their CDR data, Consumer Data Rule 7.15(a) requires the entity to acknowledge receipt of a correction request as soon as practicable.
- 13.14 An entity should acknowledge they have 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.
- 13.15 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.
- 13.16 The concept, ‘as soon as practicable’ is discussed in Chapter B (Key Concepts). 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 be able to justify any delay in acknowledging receipt of the request.

Taking action to correct, or qualify, the CDR data

- 13.17 Consumer Data Rule 7.15 requires an entity that receives a correction request to either:
- correct the CDR data, or
 - 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,
- to the extent that the entity considers appropriate.
- 13.18 An entity must first consider the extent to which it considers it appropriate to act to correct or qualify the information. Once it determines this, it must undertake either to correct the data or to include a qualifying statement with the data. Such corrections or qualifying statements must make the data accurate, up to date, complete and not misleading (to the best of the entity’s knowledge).
- 13.19 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.
- 13.20 An entity should also be prepared in an appropriate case 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

- 13.21 An entity may consider that it is not appropriate to make any correction or qualifying statement at all, because (for instance) the CDR data as it exists is accurate, up to date, complete and not misleading.
- 13.22 In such circumstances the entity must give the CDR consumer a notice in accordance with Consumer Data Rule 7.15(c) detailing the reasons why it considered that no correction or statement was necessary or appropriate and setting out the available complaint mechanisms.¹⁰
- 13.23 Reasons for not correcting CDR data or including a qualifying statement with the data may include:
- 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
 - the entity is an accredited data recipient of the data and the request is in respect of data the entity has collected from a data holder (rather than data the entity may have derived from collected data), or
 - the CDR data has already been corrected, or a qualifying statement already included with the data, on a previous occasion.

Example

Dolly defaults on her credit card repayments with data holder, BankaLot Ltd. Dolly authorises BankaLot to disclose her CDR data to accredited person, CreditCardFinder Pty Ltd, which gives BankaLot a consumer data request on Dolly's behalf. Shortly after Dolly is notified that the data has been collected, Dolly requests CreditCardFinder to correct her repayment history to show that no default was made with BankaLot.

CreditCardFinder acknowledges receipt of the request the following business day through the 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 Dolly a notice through her consumer dashboard that states that no correction or statement was made in relation to her CDR data, because CreditCardFinder did not think it appropriate for it to make such a correction or qualifying statement in relation to data it collected from BankaLot, and that if Dolly wishes the data be corrected, she should request BankaLot to make the relevant correction.

¹⁰ 56EP(3)(b).

The notice also sets out the complaint mechanisms available to Dolly, which are in line with the corresponding section in CreditCardFinder's CDR policy.

How must a correction notice be provided to consumers?

- 13.24 Consumer Data Rule 7.15(c) 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.
- 13.25 The requirement for written notices to be given by electronic means will be satisfied if the notice is given over email or over the CDR consumer's consumer dashboard.
- 13.26 The written notice may be in the body of an email or in an electronic file attached to an email.
- 13.27 While SMS is an electronic means of communicating notice, practically it is unlikely to be appropriate as the number of matters that the written notice must address under Rule 7.15(c) would likely make the SMS very long.

What must be included in a correction notice to consumers?

- 13.28 The correction notice to the consumer must set out:
- what the entity did in response to the request, and
 - complaint mechanisms available to the consumer.
- 13.29 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.
 - 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,¹¹ and any external dispute resolution schemes recognised by the Australian Competition and Consumer Commission under s 56DA(1).
- 13.30 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 Consumer Data Rules, they have a right to bring an action for damages in a court of competent jurisdiction under s 56EY of the Competition and Consumer Act.

¹¹ 56ET(4).

Example

This example follows the example under paragraph 13.12 above.

After Money Mattress corrects Kiefer's CDR data, Money Mattress sends Kiefer a notice over the consumer dashboard within the required 10 business day period. The notice states that Money Mattress has corrected the data by deleting the incorrect data relating to fraudulent transactions and retaining the correct data, and sets out the complaint mechanisms available to Kiefer.

What are the correction considerations?

- 13.31 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'.
- 13.32 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**. Privacy Safeguard 13 requires that holding the CDR data so that it can be disclosed as required under the Consumer Data Rules is not a purpose when working out the purposes for which the data is or was held.¹² 'Purpose' is discussed further in Chapter B (Key Concepts).
- 13.33 These four terms are not defined in the Competition and Consumer Act or the Privacy Act.¹³ The following analysis of each term draws on the ordinary meaning of the terms, APP Guidelines and Part V of the Freedom of Information Act 1982.¹⁴ As the analysis indicates, there is overlap in the meaning of the terms.

Accurate

- 13.34 CDR data is inaccurate if it contains an error or defect or is misleading. An example is incorrect factual information about a CDR consumer's income, assets, loan repayment history or employment status.
- 13.35 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. 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). For instance, an accredited data recipient may use an algorithm to determine a CDR consumer's projected 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, it will not be inaccurate because, for instance, the consumer believes their income will be higher or lower during the projected period.

¹² 56EP(4).

¹³ These 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 – Quality of CDR data for further information.

¹⁴ See OAIC, Australian Privacy Principles Guidelines (22 July 2019), Chapter 10 APP 10 – Quality of personal information.

Up to date

- 13.36 CDR data is not up to date if it contains information that is no longer current. An example is a statement that a CDR consumer has an active account with a certain bank, where the consumer has closed that account. Another example is an assessment that a consumer has a certain ability to meet a loan repayment obligation, where in fact the consumer's ability has since changed.¹⁵
- 13.37 For example, CDR data about a past event may have been accurate 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.

Complete

- 13.38 CDR data is incomplete if it presents a partial or misleading picture rather than a true or full picture.
- 13.39 An example is data from which it can be inferred that a CDR 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.

Not misleading

- 13.40 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.
- 13.41 Data may also be misleading if other relevant information is not included. An example is a statement that a CDR consumer is involved in litigation to recover a debt, without including the fact that the consumer is the plaintiff rather than the defendant in the action.

Example

Accredited person, XYZ Solutions Pty Ltd (**XYZ**), has consent from Zorro to collect his CDR data from data holder, Good Faith Banking and Insurance Ltd (**GFBI**). Zorro has consented to XYZ collecting and using the data for the purposes of providing Zorro with recommendations for various insurance products (for which XYZ does not receive commissions and does not promote).

Zorro had earlier spoken with GFBI employee, Bert, about insurance products offered by GFBI and mistakenly advised that he has mortgage protection when he does not. Bert had recorded, as part of Zorro's CDR data, that Zorro has mortgage protection insurance.

¹⁵ Such an assessment will likely be by 'materially enhanced information' under section 10 of the Designation Instrument and therefore not 'required consumer data' under the Consumer Data Rules.

If Zorro requests XYZ or GFBI to correct his CDR data, the entity may include a statement with the data that Zorro does not have the insurance product. The inclusion of such a statement would render the data no longer inaccurate or misleading.

Charges to correct CDR data

13.42 Consumer Data Rule 7.14 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

13.43 Privacy Safeguard 5 requires an accredited data recipient to notify a CDR consumer of the collection of their CDR data by updating the CDR consumer's consumer dashboard.

13.44 Where an accredited person has collected CDR data, and then collects corrected data after the data holder 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

13.45 Privacy Safeguard 10 requires a data holder to notify a CDR consumer of the disclosure of their CDR data by updating the CDR consumer's consumer dashboard.

13.46 Where a data holder has disclosed CDR data and then discloses corrected data as the result of the consumer's requests to correct and disclose corrected data under Privacy Safeguards 11 and 13, the data holder must notify that consumer under Privacy Safeguard 10 in respect of both disclosures.

Privacy Safeguard 11

13.47 Privacy Safeguard 13 does not apply where an entity knows CDR information is incorrect, but the CDR consumer has not made a correction request.

13.48 However, data holders and accredited data recipients will still have obligations under Privacy Safeguard 11 to take reasonable steps to ensure the quality of CDR data they are required or authorised to disclose under the Consumer Data Rules.

13.49 This includes an obligation for accredited data recipients and data holders to advise CDR consumers that some or all of their CDR data disclosed was incorrect if, at the time of disclosure, the data was not accurate, up to date and complete, having regard to the purposes for which the data was held.

13.50 An entity that corrects CDR data or includes a qualifying statement with it in accordance with Privacy Safeguard 13 must consider whether the CDR consumer must be advised of any previous disclosures of the CDR data where the data was incorrect when it was disclosed, in accordance with Privacy Safeguard 11.¹⁶ The CDR consumer may then request the entity disclose corrected CDR data to the recipient of the earlier disclosure, in accordance with Privacy Safeguard 11.¹⁷

Risk point: If a data holder only corrects CDR data in response to CDR consumer requests, rather than taking reasonable steps under Privacy Safeguard 11 to ensure the quality of CDR data they are required or authorised to disclose under the Consumer Data Rules, the entity may breach Privacy Safeguard 11 when disclosing the CDR data.

Privacy tip: Data holders should ensure that whenever they become aware that CDR data is incorrect, steps are taken to correct the data or include a qualifying statement with the data.

Privacy Safeguard 12

13.51 Where an accredited data recipient amends or creates new 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 redundant data that it holds (for example a copy of that information).

Example

Accredited data recipient of Morpheus' CDR data, NRGZ Pty Ltd, receives a correction request from Morpheus.

Data holder, Energetica Ltd was earlier required to disclose Morpheus' CDR data to NRGZ in response to a consumer data request.¹⁸

Morpheus's request is in respect of his energy usage data for the past year. The data is in respect of a shared house in which Morpheus lived with 5 other housemates, where the energy plan with Energetica was in Morpheus' name alone but payment of the bills was split among the housemates.

Morpheus requests his energy data be corrected to reflect this fact, or to be deleted from his CDR data held by NRGZ.

NRGZ considers that, as the service requested by Morpheus requires NRGZ to ascertain his individual energy usage over a certain period of time, and it is not possible to ascertain the usage from the data collected from Energetica, the data is not needed for this purpose and is not required to be retained under an Australian law or court/tribunal order. NRGZ determines that the data is redundant and should be destroyed under Privacy Safeguard 12.

NRGZ sends Morpheus a notice over his consumer dashboard indicating that NRGZ did not think it appropriate to correct or qualify it.

¹⁶ See section 56EN(3).

¹⁷ See section 56EN(4).

¹⁸ under Consumer Data Rule 4.6(4).