



Australian Government

Office of the Australian Information Commissioner



**Consumer  
Data Right**

# Privacy Safeguard Guidelines

Version 3.0 June 2021

OAIC

# Contents

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

## General matters

Chapter A: Introductory matters

Chapter B: Key concepts

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

## Part 1 — Consideration of CDR data privacy

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

Chapter 2: Privacy Safeguard 2 — Anonymity and pseudonymity

## Part 2 — Collecting CDR data

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

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

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

## Part 3 — Dealing with CDR data

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

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

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

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

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

## Part 4 — Integrity of CDR data

Chapter 11: Privacy Safeguard 11 — Quality of CDR data

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

## Part 5 — Correction of CDR data

Chapter 13: Privacy Safeguard 13 — Correction of CDR data

# Chapter A:

# Introductory matters

Version 3.0, June 2021

# Contents

<b>Purpose</b>	<b>3</b>
<b>About the consumer data right</b>	<b>4</b>
<b>About the privacy safeguards</b>	<b>4</b>
<b>Who must comply with the privacy safeguards?</b>	<b>6</b>
<b>Which privacy protections apply in the CDR context?</b>	<b>7</b>
<b>Do the privacy safeguards apply instead of the Privacy Act and the APPs?</b>	<b>7</b>
Accredited persons and accredited data recipients	8
Data holders	8
Designated gateways	8
<b>What happens if an entity breaches the privacy safeguards?</b>	<b>9</b>
<b>Where do I get more information?</b>	<b>9</b>

# Purpose

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

---

<sup>1</sup> Section 56EQ(5) of the Competition and Consumer Act.

## About the consumer data right

- A.7 The CDR aims to provide greater choice and control for Australians over how their data is used and disclosed. It allows consumers to access particular data in a usable form and to direct a business to securely transfer that data to an accredited person.
- A.8 Individual consumers and small, medium and large business consumers are able to exercise the CDR in relation to data that is covered by the CDR regime.
- A.9 The CDR has commenced in the banking sector (known as ‘Open Banking’). Next, CDR will be implemented in the energy sector.<sup>2</sup> It will then be introduced sector by sector across the broader economy as designated by the Minister.

## About the privacy safeguards

- A.10 The privacy safeguards are legally binding statutory provisions, which ensure the security and integrity of the CDR regime. The specific requirements for certain privacy safeguards are set out in the CDR Rules.
- A.11 The privacy safeguards set out standards, rights and obligations in relation to collecting, using, disclosing and correcting CDR data for which there are one or more consumers:
- Privacy Safeguard 1: Open and transparent management of CDR data
  - Privacy Safeguard 2: Anonymity and pseudonymity
  - Privacy Safeguard 3: Seeking to collect CDR data from CDR participants
  - Privacy Safeguard 4: Dealing with unsolicited CDR data from CDR participants
  - Privacy Safeguard 5: Notifying of the collection of CDR data
  - Privacy Safeguard 6: Use or disclosure of CDR data by accredited data recipients or designated gateways
  - Privacy Safeguard 7: Use or disclosure of CDR data for direct marketing by accredited data recipients or designated gateways
  - Privacy Safeguard 8: Overseas disclosure of CDR data by accredited data recipients
  - Privacy Safeguard 9: Adoption or disclosure of government related identifiers by accredited data recipients
  - Privacy Safeguard 10: Notifying of the disclosure of CDR data
  - Privacy Safeguard 11: Quality of CDR data
  - Privacy Safeguard 12: Security of CDR data, and destruction or de-identification of redundant CDR data
  - Privacy Safeguard 13: Correction of CDR data

---

<sup>2</sup> The energy sector was designated by the Treasurer on 26 June 2020. See the *Consumer Data Right (Energy Sector) Designation 2020*.

- A.12 The privacy safeguards only apply to CDR data for which there are one or more ‘CDR consumers’.<sup>3</sup> A CDR consumer can be an individual or a business enterprise.<sup>4</sup>
- A.13 There are a number of factors that determine whether CDR data has a ‘CDR consumer’.<sup>5</sup> In particular, for CDR data to have a CDR consumer, at least one person needs to be identifiable or reasonably identifiable from the CDR data or other information held by the relevant entity.<sup>6</sup> See paragraphs B.42 to B.66 in [Chapter B \(Key concepts\)](#) of the CDR Privacy Safeguard Guidelines for the full meaning of ‘CDR consumer’.
- A.14 The privacy safeguards do not apply where there is no CDR consumer<sup>7</sup> because, for example, there is no person that is identifiable or reasonably identifiable from the data. Product data is an example of CDR data for which there is no CDR consumer.
- A.15 The privacy safeguards are structured to reflect the CDR data lifecycle. They are grouped into five subdivisions within Division 5 of Part IVD of the Competition and Consumer Act:
- Subdivision B — Consideration of CDR data privacy (Privacy Safeguards 1 and 2)
  - Subdivision C — Collecting CDR data (Privacy Safeguards 3, 4 and 5)
  - Subdivision D — Dealing with CDR data (Privacy Safeguards 6, 7, 8, 9 and 10)
  - Subdivision E — Integrity of CDR data (Privacy Safeguards 11 and 12)
  - Subdivision F — Correction of CDR data (Privacy Safeguard 13)
- A.16 The requirements in each of these privacy safeguards interact with and complement each other.

## How to use these guidelines

- A.17 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.18 The number of the chapter corresponds to the number of the privacy safeguard.
- A.19 Chapter B contains guidance on general matters, including an explanation of key concepts that are used throughout the privacy safeguards and the Privacy Safeguard guidelines.
- A.20 Chapter C contains guidance on consent, which is the primary basis for collecting, using and disclosing CDR data under the CDR regime.
- A.21 These guidelines should be read together with the full text of Division 5 of Part IVD of the Competition and Consumer Act and the CDR Rules.

---

<sup>3</sup> Section 56EB(1) of the Competition and Consumer Act.

<sup>4</sup> Section 56AI(3) of the Competition and Consumer Act; Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019, paragraphs 1.100 and 1.101. See also s 2C of the *Acts Interpretation Act 1901* (Cth), which provides that in any Act (including the references to ‘person’ in s 56AI(3) of the Competition and Consumer Act), expressions used to denote persons generally include a body politic or corporate as well as an individual.

<sup>5</sup> Section 56AI(3) of the Competition and Consumer Act.

<sup>6</sup> Section 56AI(3)(c) of the Competition and Consumer Act. The ‘relevant entity’ here is the data holder, accredited data recipient, or person holding data on their behalf: s 56AI(3)(c)(ii) referencing 56AI(3)(b) of the Competition and Consumer Act.

<sup>7</sup> Section 56AI(3)(c) of the Competition and Consumer Act.

## Who must comply with the privacy safeguards?

- A.22 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:** persons who have been granted accreditation by the Australian Competition and Consumer Commission to receive data through the CDR regime<sup>8</sup>
  - **accredited data recipients:** accredited persons who have collected the CDR data from a data holder or another accredited data recipient<sup>9</sup>
  - **data holders:** the holders of the original data that the transfer of data applies to,<sup>10</sup> and
  - **designated gateways:** entities designated by the Minister as responsible for facilitating the transfer of information between data holders and accredited persons.<sup>11</sup>
- A.23 Each of these types of entities are defined in the Competition and Consumer Act and discussed further in [Chapter B \(Key concepts\)](#).
- A.24 Each privacy safeguard chapter specifies the type of entity to which it applies.
- A.25 The privacy safeguards extend to acts, omissions, matters and things outside Australia.<sup>12</sup>
- A.26 In respect of CDR data held within Australia, the privacy safeguards apply to all persons, including foreign persons.<sup>13</sup>
- A.27 In respect of an act or omission relating to CDR data held outside Australia, the privacy safeguards only apply if the act or omission:<sup>14</sup>
- 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.

---

<sup>8</sup> For specific requirements, see section 56CA of the Competition and Consumer Act.

<sup>9</sup> For specific requirements, see s 56AK of the Competition and Consumer Act.

<sup>10</sup> For specific requirements, see s 56AJ of the Competition and Consumer Act.

<sup>11</sup> For specific requirements, see s 56AL(2) of the Competition and Consumer Act.

<sup>12</sup> Section 56AO(1) of the Competition and Consumer Act.

<sup>13</sup> Section 56AO(2) of the Competition and Consumer Act.

<sup>14</sup> Section 56AO(3) of the Competition and Consumer Act.



## Which privacy protections apply in the CDR context?

CDR entity	Privacy safeguards that apply in the CDR context	APPs that apply in the CDR context
<b>Accredited person</b>	Privacy safeguards 1–4 <sup>15</sup>	None. Privacy Safeguards 1–4 apply instead of the corresponding APPs. <sup>16</sup>
<b>Accredited data recipient<sup>17</sup></b>	Privacy safeguards 1, 2 and 5–13	None. The APPs do not apply to an accredited data recipient of a consumer's CDR data in relation to that data.
<b>Data holder</b>	Privacy safeguards 1, 10, 11 and 13	All APPs (1–13)  APPs 10 and 13 are replaced by Privacy Safeguards 11 and 13 once the data holder is required or authorised to disclose the CDR data under the CDR Rules
<b>Designated gateway</b>	Privacy safeguards 1, 6, 7 and 12	APPs 1–5, 8–10 and 12–13

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

- A.28 Section 56EC(4) of the Competition and Consumer Act sets out when a privacy safeguard applies instead of an Australian Privacy Principle (APP) under the *Privacy Act 1988* (Privacy Act).
- A.29 The privacy safeguards apply only to CDR data for which there are one or more CDR consumers.<sup>18</sup>

<sup>15</sup> See ss 56EC(4), 56ED, 56EE(1)(b), 56EF and 56EG of the Competition and Consumer Act.

<sup>16</sup> **Note:** If Privacy Safeguards 1 – 4 do not apply, the corresponding APP may continue to apply to other handling of the individual's personal information where the accredited person is an APP entity (see s 56EC(4) and (5)(aa)) of the Competition and Consumer Act. Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See s 6E(1D) of the Privacy Act.

<sup>17</sup> An accredited person becomes an accredited data recipient for CDR data when:

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

<sup>18</sup> Section 56EB(1) of the Competition and Consumer Act.

- A.30 As set out in paragraph A.13 above, for there to be a CDR consumer, at least one person must be identifiable or reasonably identifiable from the CDR data or other information held by the relevant entity. As such, where the consumer is an individual, CDR data protected by the privacy safeguards will contain information about an identified or reasonably identifiable individual, and will therefore also be ‘personal information’ under the Privacy Act.
- A.31 To work out when the privacy safeguards apply, an entity needs to consider what capacity they are acting in – as a data holder, accredited person/accredited data recipient, or designated gateway.
- A.32 In each chapter in these guidelines, the interaction between the privacy safeguard and corresponding APP is discussed.

## Accredited persons and accredited data recipients

- A.33 For an accredited person or accredited data recipient of CDR data, the privacy safeguards apply instead of the APPs in relation to the handling of the CDR data within the CDR system.<sup>19</sup>

## Data holders

- A.34 For data holders, the APPs will apply to CDR data that is also personal information with the exception of APPs 10 (quality of personal information) and 13 (correction of personal information). These two APPs are replaced by Privacy Safeguards 11 (quality of CDR data) and 13 (correction of CDR data) once the data holder is required or authorised to disclose the CDR data under the CDR Rules. Privacy Safeguard 10 does not have an APP equivalent and applies to data holders in addition to all other privacy protections.
- A.35 Data holders must also comply with both APP 1 and Privacy Safeguard 1 which relate to open and transparent management of personal information and CDR data respectively. As explained above, these obligations apply concurrently and the obligations in Privacy Safeguard 1 do not displace the APP 1 obligations.

## Designated gateways

- A.36 The APPs will continue to apply to designated gateways for CDR data that is personal information except in relation to the use and disclosure of CDR data, including for direct marketing purposes, for which Privacy Safeguards 6 (use or disclosure of CDR data) and 7 (direct marketing) apply instead of APP 6 and APP 7, and the security of the CDR data, for which Privacy Safeguard 12 (security of CDR data) applies instead of APP 11.
- A.37 Further, designated gateways must comply with Privacy Safeguard 1 (open and transparent management of CDR data) in addition to APP 1. As explained above, these obligations apply concurrently and the obligations in Privacy Safeguard 1 do not displace the APP 1 obligations.

---

<sup>19</sup> The APPs do not apply to an accredited data recipient of CDR data, in relation to that CDR data - s 56EC(4)(a) of the Competition and Consumer Act. However, s 56EC(4) does not affect how the APPs apply to accredited persons and accredited data recipients who are APP entities, in relation to the handling of personal information outside the CDR system. (Note: Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See s 6E(1D) of the Privacy Act.) Section 56EC(4) also does not affect how the APPs apply to an accredited person who does not become an accredited data recipient of the CDR data (other than for Privacy Safeguards 1 – 4). See s 56EC(5)(aa) of the Competition and Consumer Act.

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

## What happens if an entity breaches the privacy safeguards?

- A.38 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.39 Where a consumer makes a complaint, the Information Commissioner will generally attempt to conciliate the complaint.
- A.40 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,<sup>20</sup> for example the power to make a determination,<sup>21</sup> 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.<sup>22</sup>
- A.41 The Australian Competition and Consumer Commission (ACCC) also have a strategic enforcement role where there are repeated or serious breaches. The Office of the Australian Information Commissioner (OAIC) and the ACCC have published a joint [Compliance and Enforcement Policy](#) for the CDR intended to help consumers and CDR entities understand the approach that the OAIC and ACCC will take to encourage compliance with the CDR Rules, legislation (including privacy safeguards and Consumer Data Standards) and how they will respond to breaches of the regulatory framework. The OAIC has also published a [CDR Regulatory Action Policy](#) which sets out the OAIC's priorities, goals and principles in regulating the CDR, and complements the joint Compliance and Enforcement Policy.

## Where do I get more information?

- A.42 The OAIC has further information about the CDR and its role on the OAIC website, see [www.oaic.gov.au/consumer-data-right](http://www.oaic.gov.au/consumer-data-right).

---

<sup>20</sup> Section 56ET(4) of the Competition and Consumer Act 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.

<sup>21</sup> Section 52 of the Privacy Act.

<sup>22</sup> Section 56EU of the Competition and Consumer Act. All privacy safeguards contain civil penalty provisions except for Privacy Safeguard 2.

# Chapter B:

# Key concepts

Version 3.0 June 2021

# Contents

<b>About this Chapter</b>	<b>4</b>
<b>Accredited data recipient</b>	<b>6</b>
<b>Accredited person</b>	<b>7</b>
<b>Authorise, Authorisation</b>	<b>7</b>
<b>CDR data</b>	<b>8</b>
Derived CDR data	8
<b>CDR participant</b>	<b>8</b>
<b>CDR policy</b>	<b>8</b>
<b>CDR receipt</b>	<b>9</b>
<b>CDR regime</b>	<b>9</b>
<b>Collect</b>	<b>9</b>
<b>Consent</b>	<b>9</b>
Collection consent	10
Use consent	10
AP disclosure consent	10
Direct marketing consent	10
De-identification consent	11
<b>Consumer, CDR consumer or ‘eligible’ CDR consumer</b>	<b>11</b>
Reasonably identifiable	12
Relates to	13
Associate	13
Eligible CDR consumer	14
<b>Consumer dashboard, or dashboard</b>	<b>15</b>
<b>Consumer data request</b>	<b>15</b>
Direct request service	16
Accredited person request service	16
Valid request	16
<b>CDR Rules</b>	<b>17</b>
<b>Current</b>	<b>17</b>
Current consent	17
Current authorisation	18
<b>Consumer Experience Guidelines</b>	<b>18</b>
<b>Data holder</b>	<b>19</b>
Earliest holding day	20
<b>Data minimisation principle</b>	<b>20</b>

<b>Data standards</b>	<b>21</b>
Consumer Experience Standards	21
<b>Designated gateway</b>	<b>22</b>
<b>Designation instrument</b>	<b>22</b>
<b>Disclosure</b>	<b>22</b>
<b>Eligible</b>	<b>23</b>
<b>General research</b>	<b>23</b>
<b>Holds</b>	<b>23</b>
<b>Outsourced service provider</b>	<b>24</b>
CDR outsourcing arrangement	24
<b>Purpose</b>	<b>25</b>
<b>Reasonable, Reasonably</b>	<b>25</b>
<b>Reasonable steps</b>	<b>26</b>
<b>Redundant data</b>	<b>26</b>
<b>Required consumer data</b>	<b>26</b>
<b>Required or authorised by an Australian law or by a court/tribunal order</b>	<b>27</b>
Australian law	27
Court/tribunal order	27
Required	27
Authorised	28
<b>Required or authorised to use or disclose CDR data under the CDR Rules</b>	<b>28</b>
Required	28
Authorised	29
<b>Required product data</b>	<b>29</b>
<b>Service data</b>	<b>29</b>
<b>Use</b>	<b>30</b>
<b>Voluntary consumer data</b>	<b>30</b>
<b>Voluntary product data</b>	<b>31</b>

## About this Chapter

- B.1 This Chapter outlines some key words and phrases that are used in the privacy safeguards and consumer data rules (CDR Rules).
- B.2 The example below outlines a key information flow in the CDR regime and demonstrates the operation of several key concepts in the CDR regime.
- B.3 Further information regarding the underlined terms can be found within this Chapter under the corresponding heading.

### Key concepts in the CDR regime explained



#### Accredited persons

Meadow Bank wants to receive CDR data to provide products or services to consumers under the CDR regime, so it applies to the ACCC (the Data Recipient Accreditor)<sup>1</sup> to become accredited. The ACCC is satisfied that Meadow Bank meets the accreditation criteria under the CDR Rules and grants accreditation. Meadow Bank is therefore an **accredited person** and is allowed to receive CDR data under the CDR regime.



#### CDR data

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

*cont*

<sup>1</sup> See paragraph B.9.

<sup>2</sup> Section 56AI(1) of the Competition and Consumer Act. The Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019 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.



### Data holders

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

- Carly's CDR data is within a class of information specified in the designation instrument for the banking sector
- Carly's CDR data is held by Sunny Bank on or after the earliest holding day<sup>3</sup>
- Sunny Bank is not a designated gateway for the data, and
- Sunny Bank is an authorised deposit-taking institution (one of the categories specified in s 56AJ(1)(d) of the Competition and Consumer Act).<sup>4</sup>



### CDR consumers

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

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

*cont*

<sup>3</sup> For the banking sector, 1 January 2017 is the 'earliest holding day' specified in the designation instrument: s 5(3) of the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019. See paragraphs B.103 to B.104 for further information.

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

<sup>5</sup> See paragraph B.43 for further information.

<sup>6</sup> Section 56AI(3) of the Competition and Consumer Act.





### Accredited data recipients

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

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

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

- is an accredited person
- has been disclosed CDR data from a data holder (Sunny Bank) under the CDR Rules
- holds that CDR data, and
- does not hold that CDR data as a data holder or designated gateway.<sup>7</sup>



### Consumer dashboards

Given that Meadow Bank has made a consumer data request on Carly's behalf, Meadow Bank provides Carly with a **consumer dashboard**.<sup>8</sup> A consumer dashboard is an online service that allows Carly to manage and view details about her consent.

Upon receiving the consumer data request from Meadow Bank, Sunny Bank also provides Carly with a consumer dashboard that will allow Carly to manage and view details about her authorisation.<sup>9</sup>

## Accredited data recipient

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

- is an accredited person (see paragraphs B.7 to B.11 below)
- was disclosed CDR data from a CDR participant under the CDR Rules<sup>10</sup>
- holds that CDR data (or has another person hold that CDR data on their behalf), and

<sup>7</sup> Section 56AK of the Competition and Consumer Act.

<sup>8</sup> CDR Rule 1.14(1)(a).

<sup>9</sup> CDR Rule 1.15(1)(a).

<sup>10</sup> If an accredited person is disclosed CDR data otherwise than in accordance with the CDR Rules (for instance, outside the CDR system), they will not become an 'accredited data recipient' for that CDR data.

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

- does not hold that CDR data as a data holder or designated gateway.<sup>11</sup>
- B.5 Accredited persons should be aware that where they are seeking consent from a consumer to collect, use or disclose CDR data, and the CDR data is yet to be collected, they are not yet an accredited data recipient of the CDR data.
- B.6 For an illustration of how and when an accredited person becomes an accredited data recipient of CDR data, see the example under paragraph B.3.

## Accredited person

- B.7 An ‘accredited person’ is a person who has been granted accreditation by the Data Recipient Accreditor.<sup>12</sup>
- B.8 In the banking sector, an example of an accredited person could be a bank, a FinTech or other business that wishes to provide a good or service using CDR data from the banking sector. This is demonstrated by the example under paragraph B.3.
- B.9 The Data Recipient Accreditor is the Australian Competition and Consumer Commission (ACCC).<sup>13</sup>
- B.10 To be granted an accreditation, the person must satisfy the accreditation criteria in Part 5 of the CDR Rules.
- B.11 A data holder may be accredited under the CDR system, and therefore be both a data holder and an accredited person.

## Authorise, Authorisation

- B.12 An authorisation must meet the requirements set out in the CDR Rules, and be sought in accordance with the data standards.<sup>14</sup>
- B.13 Data holders must ask the consumer to authorise the disclosure of their CDR data to an accredited person before disclosing CDR data to the relevant accredited person.
- B.14 For the banking sector, for requests that relate to joint accounts, in some cases, the data holder might need to seek an authorisation (known as an ‘approval’) from the other joint account holder/s.<sup>15</sup>
- B.15 For further information, see the [Guide to privacy for data holders](#). See also the example under paragraph B.3 to understand at which point a data holder must seek authorisation from the consumer to disclose CDR data.

---

<sup>11</sup> Section 56AK of the Competition and Consumer Act.

<sup>12</sup> Section 56CA(1) of the Competition and Consumer Act.

<sup>13</sup> The ACCC has been appointed as the Data Recipient Accreditor by the Minister under s 56CG of the Competition and Consumer Act.

<sup>14</sup> CDR Rule 4.5. See Division 4.4 of the CDR Rules for the requirements for asking a consumer to give or amend an authorisation.

<sup>15</sup> Depending on which ‘disclosure option’ (i.e. pre-approval or co-approval option) has been selected by the joint account holders through the joint account management service: cl 4.5 and 4.6 of Schedule 3 to the CDR Rules. See subdivision 4.3.2 of Schedule 3 to the CDR Rules, which sets out how consumer data requests to data holders that relate to joint accounts are handled in the CDR regime.

## CDR data

B.16 'CDR data' is information that is:

- within a class of information specified in the designation instrument for each sector,<sup>16</sup> or
- derived from the above information ('derived CDR data').<sup>17</sup>

### Derived CDR data

B.17 'Derived CDR data' is data that has been wholly or partly derived from CDR data, or data derived from previously derived data.<sup>18</sup> This means data derived from 'derived CDR data' is also 'derived CDR data'.

B.18 'Derived' takes its ordinary meaning. This is because 'derived' is not defined in the Competition and Consumer Act or the *Privacy Act 1988* (the Privacy Act).

## CDR participant

B.19 A 'CDR participant' is a data holder, or an accredited data recipient, of CDR data.<sup>19</sup>

## CDR policy

B.20 A 'CDR policy' is a document that provides information to consumers about how CDR data is managed and how they can make an inquiry or a complaint. The policy must be developed and maintained by entities in accordance with Privacy Safeguard 1 and CDR Rule 7.2.

B.21 The CDR policy must be a separate document to an entity's privacy policy. For further information on the suggested process for developing a CDR policy and the minimum requirements for what must be included, see [Chapter 1 \(Privacy Safeguard 1\)](#) and the [Guide to developing a CDR policy](#).

---

<sup>16</sup> Section 56AI(1) of the Competition and Consumer Act. The Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019 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](#).

<sup>17</sup> Section 56AI(1) of the Competition and Consumer Act. The Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019 (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 (available [here](#)) as well as the explanation of 'voluntary consumer data' in this Chapter.

<sup>18</sup> Section 56AI(2) of the Competition and Consumer Act.

<sup>19</sup> Section 56AL(1) of the Competition and Consumer Act.

## CDR receipt

- B.22 A 'CDR receipt' is a notice given by an accredited person to a CDR consumer who has provided, amended or withdrawn a consent.<sup>20</sup>
- B.23 CDR receipts must be given in accordance with CDR Rule 4.18.

## CDR regime

- B.24 The 'CDR regime' was enacted by the *Treasury Laws Amendment (Consumer Data Right) Act 2019* to insert a new Part IVD into the Competition and Consumer Act.
- B.25 The CDR regime includes the CDR Rules, privacy safeguards, data standards, designation instruments, and any regulations made in respect of the provisions in the Competition and Consumer Act.

## Collect

- B.26 'Collect' is not defined in the Competition and Consumer Act or the Privacy Act.
- B.27 Under the CDR regime 'collect' has its ordinary, broad meaning (as it does under the Privacy Act). The concept of 'collection' applies broadly, and includes gathering, acquiring or obtaining CDR data by any means including from individuals and other entities.
- B.28 Section 4(1) of the Competition and Consumer Act, provides that a person 'collects' information only if the person collects the information for inclusion in:
- a record (within the meaning of the Privacy Act), or
  - a generally available publication (within the meaning of the Privacy Act).<sup>21</sup>

## Consent

- B.29 Consent is the:
- only basis on which an accredited person may collect CDR data,<sup>22</sup> and
  - primary basis on which an accredited data recipient of particular CDR data may use and disclose CDR data.<sup>23</sup>

---

<sup>20</sup> CDR Rule 4.18(1).

<sup>21</sup> 'Record' is defined in s 6(1) of the Privacy Act to include a document or an electronic or other device, with certain exclusions. 'Generally available publication' is defined in s 6(1) of the Privacy Act to include certain publications that are, or will be, generally available to members of the public whether or not published in print, electronically or any other form and whether or not available on the payment of a fee.

<sup>22</sup> See Chapter 3 (Privacy Safeguard 3) for information on seeking to collect of CDR data.

<sup>23</sup> See Chapter 6 (Privacy Safeguard 6), Chapter 7 (Privacy Safeguard 7), Chapter 8 (Privacy Safeguard 8) and Chapter 9 (Privacy Safeguard 9) for information regarding use or disclosure of CDR data.

- B.30 The CDR regime sets out specific categories of consents that an accredited person may seek from a consumer. These are set out in CDR Rule 1.10A and outlined below in paragraphs B.33-B.41.
- B.31 Consent must meet the requirements set out in the CDR Rules.<sup>24</sup>
- B.32 For further information, including the requirements which an accredited person must comply with when asking a consumer to give or amend a consent, see [Chapter C \(Consent\)](#).

## Collection consent

- B.33 A collection consent is a consent given by a consumer for an accredited person to collect particular CDR data from a data holder or accredited data recipient of that CDR data.<sup>25</sup>

## Use consent

- B.34 A use consent is a consent given by a consumer for an accredited data recipient of particular CDR data to use that CDR data in a particular way, for example to provide goods or services requested by the consumer.<sup>26</sup>
- B.35 A use consent includes a direct marketing consent for an accredited data recipient to use CDR data for the purposes of direct marketing, and a de-identification consent (as outlined in paragraph B.40 below).

## AP disclosure consent

- B.36 An AP disclosure consent is a consent given by a consumer for an accredited data recipient of particular CDR data to disclose that CDR data to an accredited person in response to a consumer data request.<sup>27</sup>

## Direct marketing consent

- B.37 A direct marketing consent is a consent given by a consumer for an accredited data recipient of particular CDR data to use or disclose CDR data for the purposes of direct marketing.<sup>28</sup>
- B.38 A direct marketing consent for an accredited data recipient to use CDR data for the purposes of direct marketing is a form of 'use consent'.

---

<sup>24</sup> The requirements that an accredited person must comply with when asking for consent are contained in Division 4.3 of the CDR Rules. The specific requirements differ depending on which type of consent is being sought.

<sup>25</sup> CDR Rules 1.10A(1)(a) and 1.10A(2)(a).

<sup>26</sup> CDR Rules 1.10A(1)(b) and 1.10A(2)(b).

<sup>27</sup> CDR Rules 1.10(1)(c)(i) and 1.10A(2)(e). CDR Rule 7.5A prohibits an accredited person from disclosing CDR data to another accredited person under an AP disclosure consent until the earlier of 1 July 2021 or the making of a relevant consumer experience data standard. In practice, there is limited utility in seeking an AP disclosure consent until disclosures under AP disclosure consents are authorised in the CDR regime.

<sup>28</sup> CDR Rules 1.10A(1)(d) and 1.10A(2)(c).

- B.39 A direct marketing consent for an accredited data recipient to disclose CDR data to an accredited person for the purposes of direct marketing is a form of ‘disclosure consent’.<sup>29</sup>

## De-identification consent

- B.40 A de-identification consent is a consent given by a consumer for an accredited data recipient of particular CDR data to de-identify some or all of that CDR data in accordance with the CDR data de-identification process<sup>30</sup> and:
- use the de-identified data for ‘general research’ (see paragraph B.126), and/or
  - disclose (including by selling) the de-identified data.<sup>31</sup>
- B.41 A de-identification consent is a form of ‘use consent’.

## Consumer, CDR consumer or ‘eligible’ CDR consumer

- B.42 The ‘CDR consumer’ is the person who has the right to:
- access the CDR data held by a data holder, and
  - direct that the CDR data be disclosed to them or to an accredited person.<sup>32</sup>
- B.43 A person is a ‘CDR consumer’ for CDR data if each of the following four conditions are met:<sup>33</sup>
- the CDR data ‘relates to’<sup>34</sup> the person because of the supply of a good or service to the person or an associate<sup>35</sup> of the person<sup>36</sup>
  - the CDR data is held by another person who is:
    - a data holder of the CDR data
    - an accredited data recipient of the CDR data, or
    - holding<sup>37</sup> the data on behalf of a data holder or accredited data recipient of the CDR data<sup>38</sup>

---

<sup>29</sup> CDR Rule 1.10A(1)(c)(ii). A ‘disclosure consent’ includes an AP disclosure consent, as well as a consent for an accredited data recipient to disclose CDR data to an accredited person for the purposes of direct marketing.

<sup>30</sup> See CDR Rule 1.17 and Chapter 12 (Privacy Safeguard 12) for further information on the CDR data de-identification process.

<sup>31</sup> CDR Rules 1.10A(1)(e) and 1.10A(2)(d).

<sup>32</sup> Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019, paragraph 1.100.

<sup>33</sup> Section 56AI(3) of the Competition and Consumer Act.

<sup>34</sup> See paragraphs B.51 to B.57 for the meaning of ‘relates to’.

<sup>35</sup> See paragraphs B.58 to B.63 for the meaning of ‘associate’.

<sup>36</sup> Section 56AI(3)(a) of the Competition and Consumer Act. 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.

<sup>37</sup> See paragraphs B.127 to B.128 for the meaning of ‘holds’.

<sup>38</sup> Section 56AI(3)(b) of the Competition and Consumer Act.

- the person is identifiable, or reasonably identifiable,<sup>39</sup> from the CDR data or other information held by the other person (the data holder, accredited data recipient, or person holding data on their behalf),<sup>40</sup> and
- none of the conditions (if any) prescribed by the regulations apply to the person in relation to the CDR data.

B.44 A CDR consumer can be an individual or a business enterprise.<sup>41</sup>

B.45 Section 4B(1) of the Competition and Consumer Act does not apply for the purposes of determining whether a person is a ‘CDR consumer’.<sup>42</sup> This section explains when a person is taken to have acquired particular goods or services as a consumer, outside of the CDR regime.

B.46 These guidelines use the term ‘consumer’ to refer to ‘CDR consumer’.

## Reasonably identifiable

B.47 As outlined in paragraph B.43, for a person to be a ‘CDR consumer’ that person must be identifiable, or ‘reasonably identifiable’, from the CDR data or other information held by the relevant entity (i.e. the data holder, accredited data recipient, or person holding data on their behalf).<sup>43</sup>

B.48 For the purpose of determining whether a person is a ‘CDR consumer’ for CDR data, ‘reasonably identifiable’ is an objective test that has practical regard to the relevant context. This can include consideration of:

- the nature and amount of information
- other information held by the entity (see paragraphs B.127 to B.128 for a discussion on the meaning of ‘held’), and
- whether it is practicable to use that information to identify the person.

B.49 Where it is unclear whether a person is ‘reasonably identifiable’, an entity should err on the side of caution and act as though the person is ‘reasonably identifiable’ from the CDR data or other information held by the entity. In practice, this generally means treating the person as a ‘CDR consumer’ – the entity would need to handle CDR data which relates to the consumer in accordance with the privacy safeguards.

B.50 See B.138 to B.141 for a discussion on the meaning of ‘reasonably’.

---

<sup>39</sup> See paragraphs B.47 to B.50 for the meaning of ‘reasonably identifiable’.

<sup>40</sup> Section 56AI(3)(c) of the Competition and Consumer Act.

<sup>41</sup> Section 56AI(3) of the Competition and Consumer Act; Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019, paragraphs 1.100 and 1.101. See also s 2C of the *Acts Interpretation Act 1901* (Cth), which provides that in any Act (including the references to ‘person’ in s 56AI(3) of the Competition and Consumer Act), expressions used to denote persons generally include a body politic or corporate as well as an individual.

<sup>42</sup> Section 56AI(4) of the Competition and Consumer Act.

<sup>43</sup> Section 56AI(3)(c) of the Competition and Consumer Act.

## Relates to

- B.51 As outlined in paragraph B.43, for a person to be a ‘CDR consumer’ the CDR data must ‘relate to’ that person.<sup>44</sup>
- B.52 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.<sup>45</sup> The relevant context in the CDR regime is the Competition and Consumer Act and the Privacy Act.
- B.53 The Competition and Consumer Act states that the CDR data must ‘relate to’ the person because of the supply of a good or service to them or an associate of theirs, or because of circumstances of a kind prescribed by the CDR Rules.<sup>46</sup>
- B.54 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.55 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.58 to B.63 below).
- B.56 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.<sup>47</sup>
- B.57 By using the broad phrase ‘relates to’, the CDR regime captures meta-data.<sup>48</sup>

## Associate

- B.58 As outlined in paragraph B.43, for a person to be a CDR consumer the CDR data must relate to that person because of the supply of a good or service to the person or one or more of that person’s ‘associates’.<sup>49</sup>
- B.59 This means a person can be a ‘CDR consumer’ for CDR data relevant to goods or services used by one of their associates, such as a partner, family member or related body corporate.<sup>50</sup>

---

<sup>44</sup> Section 56AI(3)(a) of the Competition and Consumer Act.

<sup>45</sup> *PMT Partners Pty Ltd (in liq) v Australian National Parks and Wildlife Service* (1995) 184 CLR 301, 331 (Toohey and Gummow JJ).

<sup>46</sup> Section 56AI(3)(a) of the Competition and Consumer Act.

<sup>47</sup> Explanatory Memorandum, *Treasury Laws Amendment (Consumer Data Right) Bill 2019*, section 1.108.

<sup>48</sup> This includes meta-data of the type found not to be ‘about’ an individual for the purpose of the Privacy Act in *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFA 4: Explanatory Memorandum, *Treasury Laws Amendment (Consumer Data Right) Bill 2019*, section 1.106.

<sup>49</sup> Section 56AI(3)(a) of the Competition and Consumer Act.

<sup>50</sup> In the banking sector, a key example of this is where CDR data relates to a joint account.



B.60 In this context, ‘associate’ has the same meaning as in the *Income Tax Assessment Act 1936* (ITA Act).<sup>51</sup> Section 318 of the ITA Act defines ‘associates’ with respect to natural persons, companies, trustees and partnerships.<sup>52</sup>

B.61 For natural persons, an associate is:

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

B.62 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.63 The ITA Act does not define ‘associate’ with respect to a government entity. This means that a government entity that is not a company cannot be a CDR consumer if the CDR data relates to the entity because of the supply of a good or service to one or more of the entity’s ‘associates’, because the entity does not have any ‘associates’ as defined in the ITA Act.

## Eligible CDR consumer

B.64 While ‘CDR consumer’ is defined in the Competition and Consumer Act, only ‘eligible’ CDR consumers may make consumer data requests to access or transfer their CDR data under the CDR Rules.

B.65 A consumer for the banking sector is ‘eligible’ if, at that time:<sup>53</sup>

- for any consumer – the consumer is an account holder or a secondary user<sup>54</sup> for an account with the data holder that is open and set up in such a way that it can be accessed online by that consumer
- for a consumer that is an individual – the consumer is 18 years or older, and

---

<sup>51</sup> Section 56AI(3) of the Competition and Consumer Act.

<sup>52</sup> For the purposes of the CDR regime, associates of partnerships are not directly relevant, as a partnership is not a ‘person’.

<sup>53</sup> Clause 2.1 of Schedule 3 to the CDR Rules.

<sup>54</sup> A person is a ‘secondary user’ for an account with a data holder if the person has ‘account privileges’ in relation to the account, and the account holder has given the data holder an instruction to treat the person as a secondary user for the purposes of the CDR Rules (CDR Rule 1.7). ‘Account privileges’ for the banking sector are defined in clause 2.2 of Schedule 3 to the CDR Rules.

Any provisions in the CDR Rules which impose obligations on data holders in relation to secondary users only apply to initial data holders in respect of NAB, CBA, ANZ, Westpac branded products on and from 1 November 2021 (and for all other data holders, on and from 1 November 2022): see cl 6.7 of Schedule 3 to the CDR Rules.

- for a consumer that is a partner in a partnership for which there is partnership account<sup>55</sup> with the data holder – the partnership account is open and set up in such a way that it can be accessed online.<sup>56</sup>

B.66 For guidance regarding ‘consumers’ and ‘CDR consumers’, see paragraphs B.42 to B.46.

## Consumer dashboard, or dashboard

- B.67 Each accredited person and each data holder must provide a ‘consumer dashboard’ for CDR consumers.
- B.68 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 they have given to the accredited person (for example, to withdraw such consents).
  - The service must also provide the consumer with certain details of each consent.
- B.69 The requirements for an accredited person’s consumer dashboard are set out in CDR Rule 1.14. For more information, see [Chapter C \(Consent\)](#).
- B.70 A data holder’s consumer dashboard is an online service that can be used by each CDR consumer to manage authorisations to disclose CDR data in response to consumer data requests (for example, to withdraw such authorisations). The service must also notify the consumer of information related to CDR data disclosed pursuant to an authorisation.
- B.71 The requirements for a data holder’s consumer dashboard are set out in CDR Rule 1.15. For more information, see the [Guide to privacy for data holders](#).
- B.72 These guidelines use the term ‘dashboard’ and ‘consumer dashboard’ interchangeably.

## Consumer data request

- B.73 A ‘consumer data request’ is either:
- a request made directly by a CDR consumer to a data holder,<sup>57</sup> or
  - a request made by an accredited person to a data holder<sup>58</sup> or accredited data recipient<sup>59</sup> 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.

---

<sup>55</sup> A ‘partnership account’ means an account with a data holder that is held by or on behalf of the partnership or the partners in a partnership: CDR Rule 1.7.

<sup>56</sup> Any provisions in the CDR Rules which impose obligations on data holders in relation to partnerships only apply to initial data holders in respect of NAB, CBA, ANZ, Westpac branded products on and from 1 November 2021 (and for all other data holders, on and from 1 November 2022): see cl 6.7 of Schedule 3 to the CDR Rules.

<sup>57</sup> CDR Rule 3.3. For the banking sector, a data holder’s obligations under Part 3 of the CDR Rules (regarding consumer data requests made by consumers) do not commence until 1 November 2021: clause 6.6 of Schedule 3 to the CDR Rules.

<sup>58</sup> CDR Rule 4.4.

<sup>59</sup> CDR Rule 4.7A.

- B.74 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.<sup>60</sup>
- B.75 A request from an accredited person to a data holder 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.<sup>61</sup>
- B.76 A request from an accredited person to a data holder or accredited data recipient must comply with the data minimisation principle.<sup>62</sup>
- B.77 Refer to [Chapter 3 \(Privacy Safeguard 3\)](#) and [Chapter C \(Consent\)](#) for further information.

## Direct request service

- B.78 A data holder's 'direct request service' is an online service that allows eligible CDR consumers to make consumer data requests directly to the data holder in a timely and efficient manner.<sup>63</sup>
- B.79 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.80 This service must conform with the data standards.

## Accredited person request service

- B.81 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.<sup>64</sup>
- B.82 It also allows accredited persons to receive requested data in machine-readable form.
- B.83 This service must conform with the data standards.

## Valid request

- B.84 A 'valid' request is defined in the CDR Rules in Part 3 (Consumer data requests made by eligible CDR consumers) and Part 4 (Consumer data requests made by accredited persons).
- B.85 Under Part 3, 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.<sup>65</sup>
- B.86 An 'eligible' consumer for the banking sector is discussed above at paragraphs B.64 to B.66.

---

<sup>60</sup> CDR Rule 3.3(1). For the banking sector, a data holder's obligations under Part 3 of the CDR Rules (regarding consumer data requests made by consumers) do not commence until 1 November 2021: clause 6.6 of Schedule 3 to the CDR Rules.

<sup>61</sup> CDR Rule 4.4(3). There are no equivalent requirements under CDR Rule 4.7A for how an accredited person makes a consumer data request to an accredited data recipient.

<sup>62</sup> CDR Rules 4.4(1) and 4.7A(1).

<sup>63</sup> CDR Rule 1.13(2). For the banking sector, a data holder's obligations under Part 3 of the CDR Rules (regarding consumer data requests made by consumers) do not commence until 1 November 2021: clause 6.6 of Schedule 3 to the CDR Rules.

<sup>64</sup> CDR Rule 1.13(3).

<sup>65</sup> CDR Rule 3.3(3). For the banking sector, a data holder's obligations under Part 3 of the CDR Rules (regarding consumer data requests made by consumers) do not commence until 1 November 2021: clause 6.6 of Schedule 3 to the CDR Rules.

B.87 Under Part 4 of the CDR Rules, 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 to collect the CDR data and use it in order to provide those goods or services
- the accredited person has asked the consumer to give their consent for the person to collect their CDR data from a CDR participant and use that CDR data in order to provide those goods or services and
- the CDR consumer has given a collection consent and a use consent in response to the accredited person’s request (and that consent has not been withdrawn).<sup>66</sup>

B.88 Refer to [Chapter 3 \(Privacy Safeguard 3\)](#) for further information regarding valid requests, and [Chapter C \(Consent\)](#) for information regarding collection and use consents.

## CDR Rules

B.89 The consumer data rules (CDR Rules) refer to the *Competition and Consumer (Consumer Data Right) Rules 2020*.

B.90 The Minister has the power to make rules to determine how the CDR functions in each sector.<sup>67</sup> CDR Rules may be made on aspects of the CDR regime (as provided in Part IVD the Competition and Consumer Act) including the privacy safeguards,<sup>68</sup> accreditation of data recipients and the disclosure, collection, use, accuracy, storage, security or deletion of CDR data for which there are one or more CDR consumers.<sup>69</sup>

## Current

### Current consent

B.91 A consent is ‘current’ if it has not expired under CDR Rule 4.14.<sup>70</sup>

B.92 CDR Rule 4.14 provides that a consent expires:

- if it is withdrawn
- at the end of the period of consent
- once 12 months has passed after consent was given or last amended
- for a collection consent, when the accredited person is notified by the data holder of the withdrawal of authorisation
- for a collection consent, when the accredited person is notified by the accredited data recipient of the expiry of the AP disclosure consent

---

<sup>66</sup> CDR Rule 4.3.

<sup>67</sup> Section 56BA(1) of the Competition and Consumer Act.

<sup>68</sup> Part IVD, Division V of the Competition and Consumer Act.

<sup>69</sup> Section 56BB of the Competition and Consumer Act.

<sup>70</sup> CDR Rule 1.7(1) (Definitions).

- for an AP disclosure consent, when the accredited data recipient is notified by the accredited person of the expiry of the collection consent
- if the accredited person's accreditation is revoked or surrendered, when this revocation or surrender takes effect
- upon an accredited person becoming a data holder of particular CDR data (in this situation, each of the accredited person's consents that relate to the CDR data would expire), or
- if another CDR Rule provides that consent expires.

B.93 For further information on when a consent expires, see [Chapter C \(Consent\)](#).

## Current authorisation

B.94 Authorisation to disclose particular CDR data to an accredited person is 'current' if it has not expired under CDR Rule 4.26.<sup>71</sup>

B.95 CDR Rule 4.26 provides that authorisation expires:

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

B.96 For further information on when an authorisation expires, see the [Guide to privacy for data holders](#).

## Consumer Experience Guidelines

B.97 The Consumer Experience Guidelines set out guidelines for best practice design patterns to be used by entities seeking consent and/or authorisation from consumers under the CDR regime.

B.98 The Consumer Experience Guidelines are made by the Data Standards Body and cover matters including:

---

<sup>71</sup> CDR Rule 1.7.

- 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.99 The Consumer Experience Guidelines contain supporting examples illustrating how a range of key CDR Rules can be implemented.

B.100 The Consumer Experience Guidelines are available on the Data Standards Body website, [consumerdatastandards.gov.au](https://consumerdatastandards.gov.au).

## Data holder

B.101 A person is a data holder of CDR data if:<sup>72</sup>

- the CDR data falls within a class of information specified in the designation instrument for the relevant sector<sup>73</sup>
- the CDR data is held by (or on behalf of) the person on or after the earliest holding day<sup>74</sup>
- the CDR data began to be held by (or on behalf of) the person before that earliest holding day, is of continuing use and relevance (e.g. a current account number),<sup>75</sup> and is not about the provision of a product or service by (or on behalf of) the person before the earliest holding day<sup>76</sup> (e.g. a transaction on an account)<sup>77</sup>
- the person is not a designated gateway for the CDR data, and
- any of the three cases below apply:
  - **First case – person is also specified in the designation instrument:** The person is specified or belongs to a class of persons specified in a designation instrument

---

<sup>72</sup> Section 56AJ of the Competition and Consumer Act.

<sup>73</sup> For the banking sector, the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019 sets out matters including the classes of information that are subject to the CDR regime. The designation instrument for the banking sector is available [here](#). See also s 56AC(2)(a) of the Competition and Consumer Act.

<sup>74</sup> Being the earliest holding date specified in the designation instrument for the relevant sector. 1 January 2017 is the ‘earliest holding day’ specified in the designation instrument for the banking sector: s 5(3) of the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019.

<sup>75</sup> Explanatory Memorandum, Treasury Laws Amendment (2020 Measures No. 6) Bill 2020, [2.35].

<sup>76</sup> For a product or service that the person began providing before the earliest holding day and continued providing after that day, the person will:

- not be the data holder of CDR data about the person’s provision of the product or service before that day, but
- will be the data holder of CDR data about the person’s provision of the product or service on or after the earliest holding day (provided all the other criteria in s 56AJ of the Competition and Consumer Act, as discussed at paragraphs B.101 are met by the entity): see Note 2 to s 56AJ of the Competition and Consumer Act.

<sup>77</sup> Explanatory Memorandum, Treasury Laws Amendment (2020 Measures No. 6) Bill 2020, [2.35].

and neither the CDR data, nor any other CDR data from which the CDR data was directly or indirectly derived, was disclosed to the person under the CDR Rules.<sup>78</sup>

- **Second case – reciprocity arising from the person being disclosed other CDR data under the CDR Rules:** Neither the CDR data, nor any other CDR data from which the CDR data was directly or indirectly derived, was disclosed to the person under the CDR Rules, and the person is an accredited data recipient of other CDR data.<sup>79</sup>
- **Third case – conditions in the CDR Rules are met:** The CDR data or any other CDR data from which the CDR data was directly or indirectly derived was disclosed to the person under the CDR Rules, the person is an accredited person and the conditions specified in the CDR Rules are met.<sup>80</sup>

B.102 For further information on the privacy obligations for data holder, see the [Guide to privacy for data holders](#).

## Earliest holding day

- B.103 A designation instrument must specify the ‘earliest holding day’ for a particular sector. This is the earliest day applicable to the sector for holding the designated information.<sup>81</sup>
- B.104 Under the designation instrument for the banking sector, the earliest holding day is 1 January 2017.<sup>82</sup>

## Data minimisation principle

- B.105 The data minimisation principle limits the scope and amount of CDR data an accredited person may collect and use.
- B.106 An accredited person collects and uses CDR data in compliance with the data minimisation principle if:<sup>83</sup>
- a. when making a consumer data request on behalf of a 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 needed in order to provide the goods or services requested by the consumer, and

---

<sup>78</sup> 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 CDR Rule 1.10.

<sup>79</sup> Section 56AJ(3) of the Competition and Consumer Act. 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. Although under the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019 only authorised deposit-taking institutions (ADIs) are designated as persons who hold the specified classes of information for the purposes of s 56AC(2)(b), a non-ADI accredited person may become a data holder in respect of certain CDR data if this circumstance applies.

<sup>80</sup> The conditions for the banking sector are contained in clause 7.2 of Schedule 3 to the CDR Rules.

<sup>81</sup> Section 56AC(2)(c) of the Competition and Consumer Act.

<sup>82</sup> Section 5(3) of the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019.

<sup>83</sup> CDR Rule 1.8.

- 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 or to fulfill any other purpose consented to by the consumer.

## Data standards

B.107 A 'data standard' is a standard made by the Data Standards Chair of the Data Standards Body under section 56FA of the Competition and Consumer Act.

B.108 Data standards are about:

- the format and description of CDR data
- the disclosure of CDR data
- the collection, use, accuracy, storage, security and deletion of CDR data
- de-identifying CDR data, or
- other matters prescribed by regulations.<sup>84</sup>

B.109 The current data standards are available on Consumer Data Standards website, [consumerdatastandards.gov.au](https://consumerdatastandards.gov.au) and include the following:

- API Standards
- Information Security Standards, and
- Consumer Experience Standards.

## Consumer Experience Standards

B.110 The 'Consumer Experience Standards' are data standards<sup>85</sup> regarding:

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

B.111 The Consumer Experience Standards are available on Consumer Data Standards website, [consumerdatastandards.gov.au](https://consumerdatastandards.gov.au).

---

<sup>84</sup> Section 56FA of the Competition and Consumer Act and CDR Rule 8.11.

<sup>85</sup> Section 56FA of the Competition and Consumer Act and CDR Rule 8.11.



## Data Language Standards

- B.112 The ‘Data Language Standards’ are data standards<sup>86</sup> regarding the types of CDR data and descriptions of those types to be used by CDR participants in making and responding to requests.
- B.113 The Data Language Standards form part of the Consumer Experience Standards and are available on the Consumer Data Standards website, [consumerdatastandards.gov.au](https://consumerdatastandards.gov.au).

## Designated gateway

- B.114 A ‘designated gateway’ is a person specified as a gateway in a legislative instrument made under s 56AC(2) of the Competition and Consumer Act.<sup>87</sup>
- B.115 There is no designated gateway for the banking sector.

## Designation instrument

- B.116 A ‘designation instrument’ is a legislative instrument made by the Minister under section 56AC(2) of the Competition and Consumer Act.
- B.117 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.118 The designation instrument for the banking sector is the [Consumer Data Right \(Authorised Deposit-Taking Institutions\) Designation 2019](#), dated 4 September 2019.

## Disclosure

- B.119 ‘Disclosure’ is not defined in the Competition and Consumer Act or the Privacy Act.
- B.120 Under the CDR regime ‘disclose’ takes its ordinary, broad meaning.
- B.121 An entity discloses CDR data when it makes the data accessible or visible to others outside the entity.<sup>88</sup> 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.<sup>89</sup>
- B.122 For example, an entity discloses CDR data when it transfers a copy of the data in machine-readable form to another entity.

---

<sup>86</sup> Section 56FA of the Competition and Consumer Act and CDR Rule 8.11.

<sup>87</sup> See s 56AL of the Competition and Consumer Act for the definition of ‘designated gateway’.

<sup>88</sup> Information will be ‘disclosed’ under the CDR regime regardless of whether an entity retains effective control over the data.

<sup>89</sup> For a similar approach to interpreting ‘disclosure’, see *Pratt Consolidated Holdings Pty Ltd v Commissioner of Taxation* [2011] AATA 907, [112]–[119].

B.123 Where an accredited data recipient engages a third party to perform services on its behalf, the provision of CDR data to that third party will in most circumstances be a disclosure (see paragraphs B.172 to B.173 for the limited circumstances where it will be a ‘use’).

B.124 ‘Disclosure’ is a separate concept from:

- ‘Unauthorised access’ which is addressed in [Chapter 12 \(Privacy Safeguard 12\)](#). An entity is not taken to have disclosed CDR data where a third party intentionally exploits the entity’s security measures and gains unauthorised access to the information. Examples include unauthorised access following a cyber-attack or a theft, including where the third party then makes that data available to others outside the entity.
- ‘Use’ which is discussed in paragraphs B.170 to B.173 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.125 ‘Eligible’ CDR consumers are discussed at paragraphs B.64–B.66.

## General research

B.126 ‘General research’ is defined in CDR Rule 1.7 to mean research undertaken by an accredited data recipient with CDR data de-identified in accordance with the CDR Rules that does not relate to the provision of goods or services to any particular CDR consumer. An example is product or business development.<sup>90</sup>

## Holds

B.127 Section 4(1) of the Competition and Consumer Act provides that a person ‘holds’ information if they have possession or control of a record (within the meaning of the Privacy Act)<sup>91</sup> that contains the information.<sup>92</sup> This definition is comparable to the definition of ‘holds’ in the Privacy Act.<sup>93</sup>

B.128 The term ‘holds’ extends beyond physical possession of a record to include a record that a CDR entity has the right or power to deal with. Whether a CDR entity ‘holds’ a particular item of CDR data may therefore depend on the particular data collection, management and storage arrangements it has adopted. For example, a CDR entity ‘holds’ CDR data where:

- it physically possesses a record containing the CDR data and can access that data physically or by use of an electronic device (such as decryption software)

<sup>90</sup> Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020* at [21].

<sup>91</sup> ‘Record’ is defined in s 6(1) of the Privacy Act.

<sup>92</sup> Section 4(1) of the Competition and Consumer Act.

<sup>93</sup> Section 6(1) of the Privacy Act.

- it has the right or power to deal with the CDR data, even if it does not physically possess or own the medium on which the CDR data is stored. For example, the entity has outsourced the storage of CDR data to a third party but it retains the right to deal with it, including to access and amend that data.

## Outsourced service provider

B.129 The CDR Rules provide that an ‘outsourced service provider’ is a person:

- who is accredited and collects CDR data from a CDR participant on behalf of an accredited person under a CDR outsourcing arrangement, and/or
- to whom an accredited person discloses CDR data under a CDR outsourcing arrangement for the purpose of the provider providing goods or services to the accredited person.<sup>94</sup>

B.130 For the meaning of ‘collects’, refer to B.26 to B.28 above.

B.131 For the meaning of ‘discloses’, refer to B.119 to B.124 above.

## CDR outsourcing arrangement

B.132 A CDR outsourcing arrangement is a written contract between an accredited person (the ‘principal’) and an outsourced service provider (the ‘provider’). Under this arrangement a provider will collect CDR data on behalf of the principal (if the provider is an accredited person) and/or provide goods or services to the principal using CDR data disclosed to it by the principal.<sup>95</sup>

B.133 The CDR outsourcing arrangement must require the provider to:

- take the steps in Schedule 2 to the CDR Rules to protect service data, as if it were an accredited data recipient
- not use or disclose service data other than in accordance with the contract
- not disclose service data to another person otherwise than under a further CDR outsourcing arrangement, and if it does so, to ensure that the other person complies with the requirements of the CDR outsourcing arrangement
- if directed by the principal:
  - provide access to any service data that it holds
  - return any CDR data that the principal disclosed to it
  - delete (in accordance with the CDR data deletion process) any service data disclosed to it by the principal
  - provide to the principal 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, and

---

<sup>94</sup> CDR Rules 1.7(1) (Definitions) and 1.10.

<sup>95</sup> CDR Rules 1.7(1) (Definitions) and 1.10.

- where the provider is to collect CDR data on the principal's behalf, not further outsource that collection.

B.134 For information on the meaning of 'service data' in relation to a CDR outsourcing arrangement, see B.169 below.

## Purpose

B.135 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.<sup>96</sup>

B.136 The purpose of an act is the reason or object for which it is done.

B.137 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.<sup>97</sup> 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.138 'Reasonable' and 'reasonably' are used in the privacy safeguards and CDR Rules to qualify a test or obligation. For example, for CDR data to have a 'CDR consumer', at least one person must be identifiable or 'reasonably' identifiable from the CDR data or other information held by the relevant entity.<sup>98</sup>

B.139 '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.140 What is reasonable is a question of fact in each individual case. It is an objective test that has regard to how a reasonable person, who is properly informed, would be expected to act in the circumstances. What is reasonable can be influenced by current standards and practices.<sup>99</sup>

B.141 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',<sup>100</sup> and 'involves an evaluation of the known facts, circumstances and considerations which may bear

---

<sup>96</sup> Section 4F(1)(b) of the Competition and Consumer Act.

<sup>97</sup> Section 4F of the Competition and Consumer Act.

<sup>98</sup> Section 56AI(3)(c) of the Competition and Consumer Act.

<sup>99</sup> 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).

<sup>100</sup> *George v Rockett* (1990) 170 CLR 104, 112.

rationally upon the issue in question'.<sup>101</sup> There may be a conflicting range of objective circumstances to be considered, and the factors in support of a conclusion should outweigh those against.

## Reasonable steps

- B.142 References to 'reasonable steps' are used in the privacy safeguards and CDR Rules. An example is in Privacy Safeguard 11, which includes a requirement for data holders and accredited data recipients to take reasonable steps to ensure the quality of disclosed CDR data.<sup>102</sup>
- B.143 The 'reasonable steps' test is an objective test and is to be applied in the same manner as 'reasonable' and 'reasonably'.
- B.144 An entity must be able to justify that reasonable steps were taken.

## Redundant data

- B.145 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 CDR Rules or for a purpose for which the entity may use or disclose it under Division 5, Part IVD of the Competition and Consumer Act.<sup>103</sup>
- B.146 For further information on redundant data, including how to meet the obligation under Privacy Safeguard 12 to delete or de-identify redundant data, see [Chapter 12 \(Privacy Safeguard 12\)](#).

## Required consumer data

- B.147 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 CDR Rule 3.4(3), or
  - an accredited person in response to a consumer data request under CDR Rule 4.6(4).
- B.148 'Required consumer data' for the banking sector is defined in clause 3.2 of Schedule 3 to the CDR Rules.<sup>104</sup>

---

<sup>101</sup> *McKinnon v Secretary, Department of Treasury* (2006) 228 CLR 423, 430 (Gleeson CJ & Kirby J).

<sup>102</sup> See [Chapter 11 \(Privacy Safeguard 11\)](#) for information about the obligations under Privacy Safeguard 11 (s 56EN of the Competition and Consumer Act).

<sup>103</sup> Section 56EO(2) of the Competition and Consumer Act. Note that this section also applies to designated gateways, however there are no designated gateways in the banking sector.

<sup>104</sup> Clause 3.2(3) of Schedule 3 to the CDR Rules sets out what CDR data will be neither required consumer data nor voluntary consumer data.

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

B.149 A number of the privacy safeguards and CDR Rules provide an exception if a CDR entity is ‘required or authorised by or under an Australian law or a court/tribunal order’ to act differently. For example, Privacy Safeguard 6 which prohibits the use or disclosure of CDR data by an accredited data recipient unless, for example, the use or disclosure is required or authorised by or under another Australian law or a court/tribunal order.<sup>105</sup>

### Australian law

B.150 ‘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
- a rule of common law or equity.<sup>106</sup>

### Court/tribunal order

B.151 ‘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.<sup>107</sup>

B.152 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.153 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.154 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.155 The obligation will usually be indicated by words such as ‘must’ or ‘shall’ and may be accompanied by a sanction for non-compliance.

---

<sup>105</sup> And the accredited data recipient makes a written note of the use or disclosure. Section 56EI(1)(c) of the Competition and Consumer Act. See [Chapter 6 \(Privacy Safeguard 6\)](#) for further information.

<sup>106</sup> Section 6(1) of the Privacy Act.

<sup>107</sup> Section 6(1) of the Privacy Act.

## Authorised

- B.156 A person who is ‘authorised’ under an Australian law or a court/tribunal order has discretion as to whether they will handle data in a particular way. The person is permitted to take the action but is not required to do so. The authorisation may be indicated by a word such as ‘may’ but may also be implied rather than expressed in the law or order.
- B.157 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.158 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 committed<sup>108</sup> 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.159 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.<sup>109</sup>

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

- B.160 For data holders, certain regulatory provisions refer to situations where the data holder is or was ‘required or authorised’ to disclose the CDR data under the CDR Rules. For example, the requirement in Privacy Safeguard 13 to respond to a correction request applies where the data holder was ‘earlier required or authorised under the CDR Rules’ to disclose the CDR data.<sup>110</sup>
- B.161 For accredited data recipients, certain regulatory provisions refer to situations where the accredited data recipient is ‘required or authorised’ under the CDR Rules to use or disclose CDR data. For example, Privacy Safeguard 6 provides that an accredited data recipient must not use or disclose CDR data unless, for example, the use or disclosure is required or authorised under the CDR Rules.<sup>111</sup>

## Required

- B.162 A data holder is ‘required’ to disclose required consumer data<sup>112</sup> under the CDR Rules:
- in response to a valid consumer data request under CDR Rule 3.4(3), subject to CDR Rule 3.5, and

<sup>108</sup> For example, s 316(1) of the *Crimes Act 1900* (NSW).

<sup>109</sup> See *Coco v The Queen* (1994) 179 CLR 427.

<sup>110</sup> Section 56EP(1)(c) of the Competition and Consumer Act. See [Chapter 13 \(Privacy Safeguard 13\)](#) for further information.

<sup>111</sup> Section 56EI(1)(b) of the Competition and Consumer Act. See [Chapter 6 \(Privacy Safeguard 6\)](#) for further information.

<sup>112</sup> See paragraphs B.147 to B.148 for further information about ‘required consumer data’.

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

B.163 An accredited data recipient is never ‘required’ to use or disclose CDR data under the CDR Rules.

## Authorised

B.164 A data holder may be ‘authorised’ to disclose a consumer’s CDR data to an accredited person by the relevant CDR consumer.<sup>113</sup> Such an authorisation must be in accordance with Division 4.4 of the CDR Rules.

B.165 An accredited data recipient is ‘authorised’ to use or disclose CDR data under the CDR Rules in the circumstances outlined in CDR Rule 7.5. For information on the permitted uses or disclosures that do not relate to direct marketing, see [Chapter 6 \(Privacy Safeguard 6\)](#). For information on the permitted uses or disclosures that relate to direct marketing, see [Chapter 7 \(Privacy Safeguard 7\)](#).

## Required product data

B.166 In the banking sector, ‘required product data’ means CDR data for which there are no CDR consumers, and which is:<sup>114</sup>

- within a class of information specified in the banking sector designation instrument
- 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.167 The privacy safeguards do not apply to required product data.<sup>115</sup>

## Service data

B.168 ‘Service data’ refers to CDR data collected by or disclosed to an outsourced service provider under a CDR outsourcing arrangement, including any data directly or indirectly derived from such CDR data.<sup>116</sup>

B.169 For guidance regarding ‘outsourced service providers’ and ‘CDR outsourcing arrangements’, see B.129 to B.134.

---

<sup>113</sup> CDR Rule 4.5.

<sup>114</sup> Clause 3.1(1) of Schedule 3 to the CDR Rules.

<sup>115</sup> Section 56EB(1) of the Competition and Consumer Act.

<sup>116</sup> CDR Rule 1.10(4).



## Use

- B.170 ‘Use’ is not defined in the Competition and Consumer Act or the Privacy Act. ‘Use’ is a separate concept from disclosure, which is discussed at paragraphs B.119 to B.124 above.
- B.171 Generally, an entity ‘uses’ CDR data when it handles and manages that data within its effective control. Examples include the entity:
- accessing and reading the data
  - searching records for the data
  - making a decision based on the data
  - passing the data from one part of the entity to another
  - de-identifying data, and
  - deriving data from the data.
- B.172 In limited circumstances, providing CDR data to a third party (such as a cloud service provider) for limited purposes may be a use of data, rather than a disclosure (see paragraphs B.119 to B.124). However, such a provision of data will constitute a ‘use’ only if the data remains encrypted at all times, and the third party does not hold or have access to the decryption keys (on the basis that the third party would be technically unable to view or access the data at all times, and there would therefore be no disclosure).
- B.173 Whether the provision of CDR data constitutes a use or a disclosure needs to be considered carefully on a case-by-case basis, and depends on the specific technical arrangements in place with the third party. If the third party could access or view unencrypted data, for example, to maintain or provide its service, then the provision of data to that third party would constitute a disclosure, and a CDR outsourcing arrangement would be required (see paragraphs B.132 to B.134).

## Voluntary consumer data

- B.174 ‘Voluntary consumer data’ is CDR data a data holder may disclose to a CDR consumer under CDR Rule 3.4(2) or to an accredited person under CDR Rule 4.6(2).
- B.175 For the banking sector, ‘voluntary consumer data’ is CDR data for which there is a CDR consumer that is:
- not required consumer data, and
  - not specified in the CDR Rules as being neither required consumer data nor voluntary consumer data.<sup>117</sup>
- B.176 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

---

<sup>117</sup> Clause 3.2(2) of Schedule 3 to the CDR Rules. Clause 3.2(3) of Schedule 3 to the CDR Rule sets out what CDR data will be neither required consumer data nor voluntary consumer data.

instrument for the banking sector,<sup>118</sup> but may nonetheless be CDR data (as it is data derived from a specified class of information in the relevant designation instrument).

## Voluntary product data

B.177 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.<sup>119</sup>

B.178 The privacy safeguards do not apply to voluntary product data.<sup>120</sup>

---

<sup>118</sup> Section 10 of the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019 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.

<sup>119</sup> Clause 3.1(2) of Schedule 3 to the CDR Rules.

<sup>120</sup> Section 56EB(1) of the Competition and Consumer Act.

# Chapter C: Consent —

## The basis for collecting, using and disclosing CDR data

Version 3.0, June 2021

# Contents

<b>Key points</b>	<b>3</b>
<b>Why is it important?</b>	<b>3</b>
<b>How is consent in the CDR regime different to the Privacy Act?</b>	<b>3</b>
<b>How does consent fit into the CDR regime?</b>	<b>4</b>
<b>What are the different categories of consents in the CDR regime?</b>	<b>7</b>
<b>How must consent be sought?</b>	<b>8</b>
<b>Can consents be amended?</b>	<b>9</b>
<b>Requirements for asking a consumer to give or amend a consent</b>	<b>11</b>
General processes	11
Fees for disclosure	13
Name and accreditation number	14
Data minimisation principle	14
Outsourced service providers	15
Withdrawal of consent	15
Treatment of redundant data	16
De-identification consents	17
Amendment of consent	18
<b>Restrictions on seeking consents</b>	<b>18</b>
<b>How consents must be managed</b>	<b>19</b>
Consumer dashboards	19
Consumers may withdraw consent	21
Effect of withdrawing consent	23
When a consent expires	24
Notification requirements	26
<b>Authorisation</b>	<b>28</b>

## Key points

- An accredited person may only collect, use and disclose consumer data right (CDR) data with the consent of the consumer.
- The CDR regime sets out specific categories of consents that an accredited person may seek from a consumer. It further prohibits an accredited person from seeking a consent which does not fit into these categories.
- An accredited person must ask a consumer to give or amend a consent in accordance with the consumer data rules (CDR 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 a consumer to give or amend a consent must be compliant with the data standards (subject to the exceptions in CDR Rule 4.10(2)), and have regard to the Consumer Experience Guidelines.
- An accredited person must comply with the data minimisation principle when collecting or using CDR data.
- A data holder may disclose CDR data only with the authorisation of the relevant CDR consumers.

## Why is it important?

- C.1 The CDR regime places the value and control of consumer data in the hands of the consumer. This is achieved by requiring the consumer's consent for the collection, use and disclosure of their CDR data.
- C.2 Consumer consent is the bedrock of the CDR 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* (the Privacy Act).
- C.4 The CDR regime requires express consent from consumers for the collection, use and disclosure of their CDR data by accredited persons.<sup>1</sup> Consent must meet the requirements set out in the CDR Rules. A consumer can only give consent for a maximum period of 12

---

<sup>1</sup> Consent is the only basis on which an accredited person may collect CDR data. See [Chapter 3 \(Privacy Safeguard 3\)](#) for information on seeking to collect of CDR data.

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

months. Without express consent, the accredited person is not able to collect, use, or disclose CDR data.<sup>2</sup>

- C.5 However, under the Privacy Act, consent is not the primary basis upon which an entity may collect, use or disclose personal information.<sup>3</sup> In addition, where consent is involved, the consent can be either express or implied.<sup>4</sup>
- C.6 The CDR 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.

## How does consent fit into the CDR regime?

- C.8 Consent is the primary basis on which an accredited person may collect, use and disclose CDR data for which there are one or more consumers.<sup>5</sup>
- C.9 Where an accredited person:
  - offers a good or service through the CDR regime, and
  - needs to collect a consumer's CDR data from a data holder or accredited data recipient ('CDR participant') in order to use it to provide such goods or services,
 the accredited person may ask for the consumer's consent to the collection and use of their CDR data to provide the good or service.<sup>6</sup>
- C.10 In giving the above consents, the CDR consumer provides the accredited person with a 'valid request' to seek to collect the relevant CDR data.<sup>7</sup> An accredited person can only collect and use the CDR data if it has obtained these consents.
- 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 CDR participant of the CDR data. The accredited person collects this CDR data by making a 'consumer data request' to the relevant CDR participant/s.<sup>8</sup>

---

<sup>2</sup> Consent is the only basis on which an accredited person may collect CDR data, and the primary basis on which an accredited data recipient of CDR data may use and disclose that data. For further information, see footnote 1 above.

<sup>3</sup> 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 of the APP Guidelines](#) and [Chapter B: Key concepts of the APP Guidelines](#).

<sup>4</sup> See section 6(1) of the Privacy Act and [Chapter B: Key concepts of the APP Guidelines](#).

<sup>5</sup> An accredited person may make a product data request without the involvement of a consumer, for instance. In addition, while consent is the only basis on which an accredited person may collect CDR data, consent is a primary basis on which an accredited person may use and disclose CDR data. See [Chapter 6 \(Privacy Safeguard 6\)](#), [Chapter 7 \(Privacy Safeguard 7\)](#), [Chapter 8 \(Privacy Safeguard 8\)](#) and [Chapter 9 \(Privacy Safeguard 9\)](#) for further information regarding use and disclosure of CDR data.

<sup>6</sup> CDR Rule 4.3.

<sup>7</sup> CDR Rule 4.3(3).

<sup>8</sup> CDR Rules 4.4 and 4.7A. For information regarding 'valid requests' and 'consumer data requests', see [Chapter 3 \(Privacy Safeguard 3\)](#). See also the flow chart underneath paragraph C.15 which demonstrates the points at which a valid request is given by the consumer and consumer data request is made on behalf of the consumer by the accredited person.

- 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 or disclose CDR data under Privacy Safeguard 6 and Privacy Safeguard 7.
- C.14 The flow chart below paragraph C.105 demonstrates how consent fits in the key information flow between a consumer, accredited person and data holder.
- C.15 The flow chart following demonstrates the points at which a valid request is given by the consumer and a consumer data request is made on behalf of the consumer by the accredited person.

## Consent and collection process for accredited persons

### Obtaining consumer consent for the collection and use of CDR data

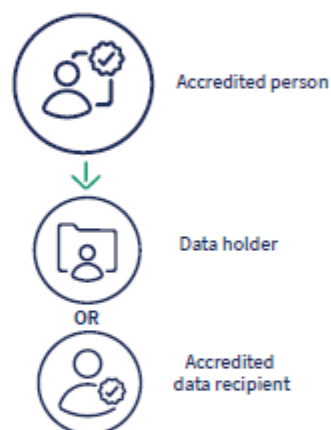
- Accredited person offers a good or service which requires CDR data
- Consumer wishes to be provided the good or service
- Accredited person asks the consumer to consent to the collection and use of their CDR data for this purpose, for up to 12 months
- Consumer provides their express consent to the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



The consumer has given the accredited person a valid request ✓

### Making a consumer data request on behalf of the consumer

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



CDR participant sends the consumer's CDR data to the accredited person after obtaining:

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



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

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

[2] Note: there are no equivalent requirements for how an accredited person must make a request to another accredited data recipient



# What are the different categories of consents in the CDR regime?

C.16 The CDR regime requires an accredited person to obtain different categories of consents from a consumer depending on what data-handling activity they propose to undertake.

C.17 The categories of consents that may be given by a consumer to an accredited person in the CDR regime are as follows:<sup>9</sup>

- **Collection consent** – a consent for an accredited person to collect particular CDR data from a data holder or accredited data recipient of that CDR data.<sup>10</sup>
- **Use consent** – a consent for an accredited data recipient of particular CDR data to use that CDR data in a particular way, for example to provide goods or services requested by the consumer.<sup>11</sup> A use consent includes a direct marketing consent for an accredited data recipient to use CDR data for the purposes of direct marketing, and a de-identification consent (as outlined below).
- **AP disclosure consent** – a consent for an accredited data recipient of particular CDR data to disclose that CDR data to another accredited person in response to a consumer data request.<sup>12</sup>
- **Direct marketing consent** – a consent for an accredited data recipient of particular CDR data to use or disclose that CDR data for the purposes of direct marketing.<sup>13</sup>
  - A direct marketing consent for an accredited data recipient to use CDR data for the purposes of direct marketing is a form of ‘use consent’.
  - A direct marketing consent for an accredited data recipient to disclose CDR data to another accredited person for the purposes of direct marketing is a form of ‘disclosure consent’.<sup>14</sup>

---

<sup>9</sup> Note: Each category of consent (except a ‘collection consent’) refers to an ‘accredited data recipient of particular CDR data’, rather than an ‘accredited person’. This is because, while the entity will be an ‘accredited person’ when seeking this category of consents, the entity would become an ‘accredited data recipient of particular CDR data’ in relation to that consumer upon collecting the relevant CDR data.

<sup>10</sup> CDR Rules 1.10A(1)(a) and 1.10A(2)(a).

<sup>11</sup> CDR Rules 1.10A(1)(b) and 1.10A(2)(b).

<sup>12</sup> CDR Rules 1.10(1)(c)(i) and 1.10A(2)(e). CDR Rule 7.5A prohibits an accredited data recipient from disclosing CDR data to another accredited person under an AP disclosure consent until the earlier of 1 July 2021 or the making of a relevant consumer experience data standard. In practice, there is limited utility in seeking an AP disclosure consent until disclosures under AP disclosure consents are authorised in the CDR regime.

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

<sup>13</sup> CDR Rules 1.10A(1)(d) and 1.10A(2)(c).

<sup>14</sup> CDR Rule 1.10A(1)(c)(ii). A ‘disclosure consent’ includes an AP disclosure consent, as well as a consent for an accredited data recipient to disclose CDR data to an accredited person for the purposes of direct marketing.

- **De-identification consent** – a form of ‘use consent’ for an accredited data recipient of particular CDR data to de-identify some or all of that CDR data in accordance with the CDR data de-identification process<sup>15</sup> and:
  - use the de-identified data for general research,<sup>16</sup> and/or
  - disclose (including by selling) the de-identified data.

- C.18 An accredited person is prohibited from seeking a consent that is not in the list above.<sup>17</sup>
- C.19 Each category of consent operates independently of each other. This means that an accredited person can ask for more than one category of consent, and that a consumer must be enabled by an accredited person to independently manage each category of consent.<sup>18</sup> For example, an accredited person may ask a consumer for a collection consent and use consent, and the consumer can (in future) choose to withdraw only the collection consent, if they wish.<sup>19</sup>
- C.20 The requirements that an accredited person must comply with when asking for a consent are contained in Division 4.3 of the CDR Rules. The specific requirements differ depending on which category of consent is being sought.
- C.21 The categories of consent are based off the ‘types’ of consents set out in the CDR Rules.<sup>20</sup>

## How must consent be sought?

- C.22 An accredited person must ask the consumer to give consent in accordance with Division 4.3 of the CDR Rules. Division 4.3 sets out the specific requirements for each consent outlined in the section above.<sup>21</sup>
- C.23 The requirements in Division 4.3 are outlined below under ‘Requirements for asking a consumer to give or amend a consent’, ‘Restrictions on seeking consents’ and ‘How consents must be managed’.

---

<sup>15</sup> See CDR Rule 1.17 and [Chapter 12 \(Privacy Safeguard 12\)](#) for further information on the CDR data de-identification process.

<sup>16</sup> ‘General research’ is defined in CDR Rule 1.7 to mean research undertaken by an accredited data recipient with CDR data de-identified in accordance with the CDR Rules that does not relate to the provision of goods or services to any particular CDR consumer.

<sup>17</sup> CDR Rule 4.12(3)(a).

<sup>18</sup> See the Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020* at [7].

<sup>19</sup> For example, where the consumer wishes to allow the accredited data recipient to keep using their CDR data so they may continue to receive the relevant good or service. Where a consumer withdraws both their collection consent and use consent, it is likely the CDR data would become redundant data that must be deleted or de-identified under Privacy Safeguard 12, unless an exception applies. For further information, see paragraphs C.81 to C.89 ‘Effect of withdrawing consent’.

<sup>20</sup> The ‘categories’ of consent are listed at CDR Rule 1.10A(2) and defined by reference to the ‘types’ of consents listed at CDR Rule 1.10A(1).

<sup>21</sup> Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020*, 13, which provides that an accredited person must ask for consent in accordance with Division 4.3 of the CDR Rules which now encompass provisions relating to all types and categories of consent. See also CDR Rule 4.3(2).

- C.24 The CDR Rules state that the objective of Division 4.3 is to ensure that consent given by a consumer is voluntary, express, informed, specific as to purpose, time limited and easily withdrawn.<sup>22</sup>
- C.25 In obtaining consent from a consumer, an accredited person must comply with requirements relating to:
- an accredited person's processes for asking for consent<sup>23</sup>
  - information to be presented to the consumer when asking for consent,<sup>24</sup> and
  - restrictions on seeking consent.<sup>25</sup>
- C.26 Where a consumer is not an individual 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.<sup>26</sup>

## Can consents be amended?

- C.27 An accredited person will be allowed to invite a consumer to amend their existing consent on and from 1 July 2021.<sup>27</sup> This includes allowing a consumer to change:
- the types of CDR data that can be collected and/or disclosed
  - what the CDR data can be used for
  - what accounts or data holders CDR data is to be collected from, and/or
  - the duration of the consent.<sup>28</sup>
- C.28 An invitation to amend a consent may be issued only where the amendment would:<sup>29</sup>
- better enable the accredited person to provide the goods or service requested by the consumer under the existing consent,<sup>30</sup> or
  - be consequential to an agreement between the accredited person and consumer to modify those goods or services, and enable the accredited person to provide the modified goods or services.

---

<sup>22</sup> CDR Rule 4.9. The Explanatory Statement to the CDR Rules, together with the Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020*, provides that the CDR Rules are intended to ensure that all consents sought in the CDR regime are transparent and that consumers understand the potential consequences of what they are consenting to.

<sup>23</sup> CDR Rule 4.10.

<sup>24</sup> CDR Rule 4.11.

<sup>25</sup> CDR Rule 4.12.

<sup>26</sup> A person is entitled, under section 128 of the *Corporations Act 2001*, to make the assumptions set out in section 129 of that Act when dealing with corporations, including that persons held out by the company as directors, officers and agents are duly appointed and have authority to exercise customary powers.

<sup>27</sup> CDR Rule 4.12B(5). See generally Subdivision 4.3.2A of the CDR Rules.

<sup>28</sup> See the Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020* at [6].

<sup>29</sup> CDR Rule 4.12B(3).

<sup>30</sup> That is, the goods or services requested by the consumer as part of their valid request in CDR Rule 4.3(1)(a).

- C.29 An invitation to amend an existing consent may be given via the consumer dashboard (if applicable)<sup>31</sup> or in writing to the consumer.<sup>32</sup> An invitation can only be given where the consent is current (i.e. has not expired).<sup>33</sup>
- C.30 Where an accredited person wishes to invite a consumer to amend the duration of their consent, the invitation must not be given:
- any earlier than a reasonable period before the existing consent expires, and
  - more than a reasonable number of times within this period.<sup>34</sup>

**Example:** A consumer has given a consent to an accredited data recipient in relation to CDR data for a period of three months. In the three weeks prior to expiry, the accredited person invites the consumer on two occasions to extend the duration of their existing consent. The accredited data recipient has decided, based on their circumstances, that they have provided the invitation within a reasonable period before the existing consent expires, and a reasonable number of times within that period.<sup>35</sup>

- C.31 Where the accredited person wishes to invite a consumer to extend the duration of their consent, they should first consider whether the invitation would constitute an offer to renew existing goods or services under CDR Rule 7.5(3)(a)(ii) (in which case a direct marketing consent would be required).<sup>36</sup>
- C.32 An accredited person cannot ask a consumer to extend the duration of an existing consent for longer than 12 months.<sup>37</sup>
- C.33 An accredited person must ask the consumer to give any amendments to their existing consent in the same manner that they asked the consumer to provide the existing consent (i.e. in accordance with Division 4.3 of the CDR Rules).<sup>38</sup> There are some exceptions, as outlined in the following section.<sup>39</sup>
- C.34 Where a consumer amends their collection consent, the accredited person must notify the relevant CDR participant/s that the consent has been amended.<sup>40</sup>

<sup>31</sup> It is optional for accredited persons to offer a consent amendment functionality in the consumer dashboard: see CDR Rules 4.12B(2)(a) and 1.14(2A).

<sup>32</sup> CDR Rule 4.12B(2).

<sup>33</sup> CDR Rule 4.12B(3). See paragraphs C.90 to C.96 and CDR Rule 4.14 for information on when consent expires.

<sup>34</sup> CDR Rule 4.12B(4).

<sup>35</sup> Example adapted from the Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020*, 15.

<sup>36</sup> Sending the consumer an offer to renew existing goods or services when they expire is direct marketing, and is only permitted if the accredited person has obtained a direct marketing consent from the consumer to send them information for these purposes. See s 56EJ(1) of the Competition and Consumer Act and CDR Rule 7.5(3)(a)(ii). For further information on this requirement, see [Chapter 7 \(Privacy Safeguard 7\)](#).

<sup>37</sup> This is as a result of CDR Rule 4.12(1), which provides that the duration of a consent cannot exceed 12 months.

<sup>38</sup> CDR Rule 4.12(C)(1).

<sup>39</sup> The exceptions are contained in CDR Rule 4.12(C)(2) and allow certain details of the existing consent to be presented as pre-selected options (namely, the details covered by CDR Rules 4.11(1)(a), (b) and (ba)). They also require additional information to be presented to the consumer to explain: the consequences of amending consent; and that the accredited person would be able to continue to use CDR data already disclosed to it to the extent allowed by the amended consent.

<sup>40</sup> CDR Rule 4.18C.

- where the CDR data is being collected from a data holder, in accordance with the data standards, and/or
- where the CDR data is being collected from an accredited data recipient, as soon as practicable. This notice should contain sufficient detail to enable the accredited data recipient to understand the types of CDR data to which the amended collection consent now applies.

C.35 An accredited person must also provide a consumer with certain notifications upon the amendment of a consent. These are outlined under ‘Notification requirements’ in paragraph C.97 of this Chapter.

C.36 An amendment of a consent takes effect when the consumer amends the consent.<sup>41</sup>

## Requirements for asking a consumer to give or amend a consent

### General processes

C.37 An accredited person’s processes for asking a consumer to give or amend a consent must:

- accord with any consumer experience data standards<sup>42</sup>
- for all consents, accord with any other data standards<sup>43</sup> (except in the case of a consent to collect CDR data from an accredited data recipient, or a disclosure consent),<sup>44</sup> and
- be as easy to understand as practicable, including by using concise language and, where appropriate, visual aids.<sup>45</sup>

C.38 In ensuring processes are easy to understand, an accredited person must also have regard to the Consumer Experience Guidelines.<sup>46</sup>

C.39 An accredited person must not:

- include or refer to the accredited person’s CDR policy or other documents in a way that would reduce consumer comprehension when seeking consent, or

---

<sup>41</sup> CDR Rule 4.12A. As per the note to this Rule, it is not possible for the consumer to specify a different date or time.

<sup>42</sup> CDR Rule 4.10. The consumer experience standards are data standards regarding the obtaining and withdrawal of consents, the collection and use of CDR data, and the types of CDR data and description of those types to be used by CDR participants when making requests. Further information is available in [Chapter B \(Key concepts\)](#).

<sup>43</sup> ‘CDR Rule 4.10(2) does not affect the application of other data standards in relation to any other processes for which an accredited person is responsible (for example data standards that may apply to encryption of data in transit in accordance with Schedule 2, Part 2 of the CDR Rules.)’: Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020*, 15. Other data standards include the API standards and information security standards, and are discussed in [Chapter B \(Key concepts\)](#).

<sup>44</sup> CDR Rule 4.10(2).

<sup>45</sup> CDR Rule 4.10.

<sup>46</sup> CDR Rule 4.10. The ‘Consumer Experience Guidelines’ provide best practice interpretations of several CDR Rules relating to consent and are discussed in [Chapter B \(Key concepts\)](#).

- bundle consents with other directions, agreements, consents or permissions.<sup>47</sup> This practice has the potential to undermine the voluntary nature of the consent.
- C.40 However, an accredited person may refer to its CDR policy when seeking consent, so long as doing so would not be likely to reduce consumer comprehension.<sup>48</sup>
- C.41 Each time an accredited person seeks a consumer's consent, they must allow the consumer to actively select or clearly indicate:
- for collection and disclosure consents,<sup>49</sup> the particular types of CDR data to which the consent will apply<sup>50</sup>
  - for all consents, whether the data will be:
    - collected and, if applicable, disclosed on a single occasion and used over a specified period of time (not exceeding 12 months), or
    - collected and, if applicable, disclosed on an ongoing basis and used over a specified period of time (not exceeding 12 months).<sup>51</sup>
  - for a use consent,<sup>52</sup> the specific uses of that CDR data,<sup>53</sup> and
  - for a disclosure consent,<sup>54</sup> the accredited person to whom the CDR data may be disclosed.<sup>55</sup>
- C.42 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.41 above,<sup>56</sup> and

---

<sup>47</sup> CDR Rule 4.10. Bundled consent refers to the 'bundling' together of multiple requests for consumer's consent to a wide range of collections, uses and/or disclosures of CDR data, without giving the consumer the opportunity to choose which collections, uses or disclosures they agree to and which they do not.

<sup>48</sup> Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020*, 14. Indeed, accredited persons are required to provide links to their CDR policy at certain points in the consent-seeking process, for example when providing information about outsourced service providers (CDR Rule 4.11(3)(f)(i) and (ii)) and general research (CDR Rule 4.15(c)).

<sup>49</sup> Including both an AP disclosure consent (as defined in CDR Rule 1.10A) and a direct marketing consent for an accredited data recipient of particular CDR data to disclose that CDR data to another accredited person for the purposes of direct marketing: CDR Rule 1.10A(1)(c)(ii).

<sup>50</sup> CDR Rules 4.11(1)(a)(i), 4.11(1)(c) and 4.11(2).

<sup>51</sup> CDR Rules 4.11(1)(b), 4.11(1)(c), 4.11(2) and 4.12(1).

<sup>52</sup> Including a de-identification consent (as defined in CDR Rule 1.10A) and a direct marketing consent for an accredited data recipient of particular CDR data to use that CDR data for the purposes of direct marketing (as per CDR Rule 1.10A).

<sup>53</sup> CDR Rules 4.11(1)(a)(ii), 4.11(1)(c) and 4.11(2).

<sup>54</sup> Including both an AP disclosure consent (as defined in CDR Rule 1.10A) and a direct marketing consent for an accredited data recipient of particular CDR data to disclose that CDR data to another accredited person for the purposes of direct marketing: CDR Rule 1.10A(1)(c)(ii).

<sup>55</sup> CDR Rules 4.11(1)(ba) and 4.11(2).

<sup>56</sup> CDR Rule 4.11(1)(c).

- not pre-select these options,<sup>57</sup> except where the accredited person is asking the consumer to amend an existing consent.<sup>58</sup> In this situation, the accredited person may pre-select the above options to reflect what the consumer has selected in the past.<sup>59</sup>

C.43 An accredited person must not ask a consumer to give a disclosure consent<sup>60</sup> unless the consumer has already given their consent for the relevant CDR data to be collected and used.<sup>61</sup> This means that an accredited person may:

- ask a consumer to give a collection consent and use consent, and subsequently ask for a disclosure consent, or
- ask a consumer to give a consent to collect, use and disclose at the same time.<sup>62</sup>

## Fees for disclosure

C.44 An accredited person may charge the consumer a fee for the disclosure of CDR data, or pass on to the consumer a fee charged by the data holder for the disclosure of CDR data.<sup>63</sup> This must be made clear to the consumer

C.45 To do this, the accredited person must:

- clearly distinguish between the CDR data for which a fee will, and will not, be charged or passed on<sup>64</sup>
- inform the consumer of the amount of the fee, and the consequences if the consumer does not consent to the collection or disclosure, as appropriate, of the CDR data for which a fee will be charged or passed on,<sup>65</sup> and
- allow the consumer to actively select or otherwise clearly indicate whether they consent to the collection or disclosure, as appropriate, of the CDR data for which a fee will be charged or passed on.<sup>66</sup>

---

<sup>57</sup> CDR Rule 4.11(2).

<sup>58</sup> CDR Rule 4.12C(2)(a).

<sup>59</sup> For example, where this would assist the consumer to make an informed decision as to how they would like to amend their consent.

<sup>60</sup> Including both an AP disclosure consent (as defined in CDR Rule 1.10A) and a direct marketing consent for an accredited data recipient of particular CDR data to disclose that CDR data to another accredited person for the purposes of direct marketing: CDR Rule 1.10A(1)(c)(ii).

<sup>61</sup> CDR Rule 4.11(1A).

<sup>62</sup> See the note to CDR Rule 4.11(1A) which clarifies that this Rule does not prevent the accredited person from asking for a disclosure consent in relation to CDR data that has yet to be collected.

<sup>63</sup> For example, where the consumer's request covers voluntary consumer data, the data holder may decide to charge the accredited person a fee. For information regarding 'required consumer data' and 'voluntary consumer data', see [Chapter B \(Key concepts\)](#).

<sup>64</sup> CDR Rule 4.11(1)(d).

<sup>65</sup> CDR Rule 4.11(3)(d).

<sup>66</sup> CDR Rule 4.11(1)(d).

## Name and accreditation number

- C.46 The accredited person must ensure that their name is clearly displayed in the consent request.<sup>67</sup>
- C.47 The accredited person's accreditation number must also be included in the consent request.<sup>68</sup> This number has been assigned to the accredited person by the Data Recipient Accreditor.
- C.48 For more information on the Data Recipient Accreditor and the accreditation process and conditions, see the ACCC's Accreditation Guidelines.

## Data minimisation principle

- C.49 Collection and use of CDR data is limited by the data minimisation principle,<sup>69</sup> 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 or to fulfil any other purpose consented to by the consumer.<sup>70</sup>

**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 would therefore likely be in breach of the data minimisation principle.

- C.50 Where an accredited person is seeking a collection consent or use consent,<sup>71</sup> the accredited person must explain how their collection and use is in line with the data minimisation principle.<sup>72</sup>
- C.51 For a collection consent, this explanation must include an outline of why the accredited person believes collecting the data is 'reasonably needed' to provide the relevant goods or services or to fulfil another purpose for which the accredited person is seeking consent.<sup>73</sup>

---

<sup>67</sup> CDR Rule 4.11(3)(a).

<sup>68</sup> CDR Rule 4.11(3)(b).

<sup>69</sup> CDR Rule 4.12(2).

<sup>70</sup> CDR Rule 1.8.

<sup>71</sup> Including a de-identification consent (as defined in CDR Rule 1.10A) and a direct marketing consent for an accredited data recipient of particular CDR data to use that CDR data for the purposes of direct marketing (as per CDR Rule 1.10A).

<sup>72</sup> CDR Rule 4.11(3)(c). For further information regarding the data minimisation principle, see [Chapter B \(Key concepts\)](#).

<sup>73</sup> CDR Rule 4.11(3)(c)(i).



- For example, the accredited person must explain how the data is necessary to deliver the service they are providing.<sup>74</sup>

C.52 The accredited person must also explain the reason for the data collection period. The collection period must be no longer than is ‘reasonably needed’ to provide the goods or services or to fulfil any other purpose for which the accredited person is seeking consent.<sup>75</sup>

- This means that the accredited person needs to explain why the data is collected over the collection period.
- There should be a reason why historical data is collected, and that reason must be both in line with the data minimisation principle and explained to the consumer at the point of consent.

C.53 For a use consent,<sup>76</sup> 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 or to fulfil another purpose for which the accredited person is seeking consent.<sup>77</sup>

## Outsourced service providers

C.54 Where the accredited person uses an outsourced service provider<sup>78</sup> to collect CDR data, or may disclose the consumer’s CDR data to an outsourced service provider (including one that is based overseas), the accredited person must:

- tell the consumer that the accredited person will use an outsourced service provider to collect CDR data and/or disclose the consumer’s CDR data to an outsourced service provider, and
- provide the consumer with a link to the accredited person’s CDR policy, noting that further information about outsourced service providers can be found in that policy.<sup>79</sup>

## Withdrawal of consent

C.55 The accredited person must explain to the consumer:<sup>80</sup>

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

---

<sup>74</sup> CDR Rule 4.11(3)(c).

<sup>75</sup> CDR Rule 4.11(3)(c)(i).

<sup>76</sup> Including a de-identification consent (as defined in CDR Rule 1.10A) and a direct marketing consent for an accredited data recipient of particular CDR data to use that CDR data for the purposes of direct marketing (as per CDR Rule 1.10A).

<sup>77</sup> CDR Rule 4.11(3)(c)(ii).

<sup>78</sup> For further information regarding outsourced service providers, see [Chapter B \(Key concepts\)](#).

<sup>79</sup> CDR Rule 4.11(3)(f). An accredited data recipient’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 to those outsourced service providers. For further information, see [Chapter 1 \(Privacy Safeguard 1\)](#) and the [Guide to developing a CDR policy](#).

<sup>80</sup> CDR Rule 4.11(3)(g).

## Treatment of redundant data

C.56 The accredited person must tell the consumer whether the accredited person has a general policy of:

- deleting redundant data
- de-identifying redundant data, or
- deciding, when the CDR data becomes redundant, whether to delete or de-identify the redundant data.<sup>81</sup>

C.57 Where the accredited person will<sup>82</sup> or may<sup>83</sup> de-identify redundant data, the accredited person must also:

- allow the consumer to elect for their redundant data to be deleted,<sup>84</sup> including by outlining the consumer's right to elect for this to occur and providing instructions for how the consumer can make the election.<sup>85</sup> Where the accredited person is asking the consumer to amend an existing consent, and the consumer previously made an election, the accredited person may pre-select this election.<sup>86</sup>
- 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 means<sup>87</sup>
- 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 consumer,<sup>88</sup> and
- if applicable, provide the consumer with examples of how the accredited person could use the redundant data once de-identified.<sup>89</sup>

C.58 See [Chapter 12 \(Privacy Safeguard 12\)](#) for further information on the treatment of redundant data (i.e. destruction or de-identification).

---

<sup>81</sup> CDR Rules 4.11(3)(h)(i) and 4.17(1).

<sup>82</sup> That is, because the accredited person communicated (when seeking consent) a general policy of de-identifying redundant data.

<sup>83</sup> 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.

<sup>84</sup> CDR Rules 4.11(1)(e) and 4.16. The accredited person must allow the consumer to make this election when providing consent to the accredited person in relation to their CDR data, and at any other point in time before the consent expires (CDR Rule 4.16(1)).

<sup>85</sup> CDR Rule 4.11(3)(h).

<sup>86</sup> CDR Rule 4.12C(2)(b).

<sup>87</sup> CDR Rule 4.17(2)(a), 4.17(2)(b). The prescribed process is the CDR data de-identification process outlined in CDR Rule 1.17. Further information on the CDR data de-identification process is in [Chapter 12 \(Privacy Safeguard 12\)](#).

<sup>88</sup> CDR Rule 4.17(2)(a).

<sup>89</sup> CDR Rule 4.17(2)(c).

## De-identification consents

C.59 Where an accredited person is asking the consumer for a de-identification consent as defined under CDR Rule 1.10A, the accredited person must also tell the consumer the additional information in CDR Rule 4.15:<sup>90</sup>

- what the CDR de-identification process is<sup>91</sup>
- if the accredited person would disclose (for example, by sale) the de-identified data to one or more other persons:
  - a statement of that fact
  - the classes of persons to whom the accredited person would disclose the de-identified data (for example, to market research organisations or university research centres), and
  - the purpose/s for which the accredited person would disclose the de-identified data (for example, to sell the de-identified data or to provide to a university for research)
- if the accredited person would use the de-identified data for general research:<sup>92</sup>
  - a statement of that fact
  - that the consumer can find further information in the accredited person's CDR policy of the research to be conducted and any additional benefit to be provided to the consumer for consenting to this use of their data,<sup>93</sup> and
  - a hyperlink to the relevant section/s of the accredited person's CDR policy, and
- that the consumer would not be able to elect to have the de-identified data deleted once it becomes redundant data.

C.60 When seeking a de-identification consent, the accredited person must explain how their collection and use is in line with the data minimisation principle.<sup>94</sup> See paragraphs C.50 to C.53 above.

---

<sup>90</sup> CDR Rules 4.11(3)(e) and 4.15.

<sup>91</sup> The CDR data de-identification process is outlined in CDR Rule 1.17. More information on this requirement is in [Chapter 12 \(Privacy Safeguard 12\)](#).

<sup>92</sup> 'General research' is defined in CDR Rule 1.7 to mean research undertaken by an accredited data recipient with CDR data de-identified in accordance with the CDR Rules that does not relate to the provision of goods or services to any particular CDR consumer. An example is product or business development: Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020* at [21].

<sup>93</sup> For example, a benefit may include the accredited data recipient paying a fee to the consumer for using their data or providing a discount on the services they provide to the consumer: ACCC, CDR Rules Expansion Amendments Consultation Paper, September 2020, 48.

<sup>94</sup> CDR Rule 4.11(3)(c). For further information regarding the data minimisation principle, see paragraphs C.49 to C.53 and [Chapter B \(Key concepts\)](#).

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

## Amendment of consent

C.61 Where an accredited person is inviting a consumer to amend their existing consent, in addition to the other requirements outlined in the above sections, the accredited person must give the consumer statements that outline:<sup>95</sup>

- the consequences of amending a consent, and
- the extent to which the accredited person will be able to use any CDR data that has already been disclosed to it.

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

*“If you amend your consent, we will no longer collect your account balance and details, but we will use the data we’ve already collected. Don’t worry – when you withdraw your use consent or when it expires on 1 October, we will delete it,<sup>96</sup> along with all your other data, in accordance with our CDR policy...”<sup>97</sup>*

## Restrictions on seeking consents

C.62 CDR Rule 4.12 provides that when seeking consent from a consumer, an accredited person must not ask for:<sup>98</sup>

- consent to collect, use or disclose CDR data over a period exceeding 12 months
- consent to collect or use the data in a manner that is in breach of the data minimisation principle,<sup>99</sup> or
- a consent that is not in a ‘category’ of consents (see paragraph C.17 for a list of the categories of consents)<sup>100</sup>

<sup>95</sup> CDR Rule 4.12C(3).

<sup>96</sup> See [Chapter 12 \(Privacy Safeguard 12\)](#) for information on when CDR data will become ‘redundant data’ that must be deleted or de-identified in accordance with the CDR Rules, unless an exception applies.

<sup>97</sup> Example from Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020*, 16.

<sup>98</sup> CDR Rule 4.12.

<sup>99</sup> The data minimisation principle is discussed in [Chapter B \(Key concepts\)](#), and at paragraph C.49.

<sup>100</sup> See CDR Rule 1.10A(2).

- consent to use the CDR data, including by aggregating it, for the purpose of identifying, compiling insights or building a profile in relation to any identifiable person who is not the consumer who is providing the consent.<sup>101</sup>

C.63 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:<sup>102</sup>

- the person's identity is readily apparent
- the accredited person is seeking consent to derive, from the consumer's CDR data, CDR data about the non-CDR consumer's interactions with the consumer, and
- the accredited person will use that derived CDR data only for the purpose of providing the goods or services requested by the consumer.

**Example:** ChiWi is an accredited person offering a budgeting service that tracks a person's spending. One category of spending is 'gifts'.

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

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

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

## How consents must be managed

### Consumer dashboards

- C.64 An accredited person must provide a consumer dashboard for each consumer who has provided a consent in relation to their CDR data.<sup>103</sup>
- C.65 Where an accredited person collects a consumer's CDR data on behalf of another accredited person (the 'principal') under a CDR outsourcing arrangement, only the principal needs to provide the relevant consumer with a dashboard.<sup>104</sup>
- C.66 An accredited person's consumer dashboard is an online service that can be used by each consumer to manage consumer data requests<sup>105</sup> and consents for the accredited person to collect, use and disclose CDR data.

<sup>101</sup> 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.

<sup>102</sup> CDR Rule 4.12(4).

<sup>103</sup> CDR Rule 1.14.

<sup>104</sup> See CDR Rule 1.7(5). For information regarding CDR outsourcing arrangements, see [Chapter B \(Key concepts\)](#).

<sup>105</sup> See [Chapter B \(Key concepts\)](#).

- C.67 The consumer dashboard should be provided to the consumer as soon as practicable after the accredited person receives a valid request from that consumer for the collection and use of their CDR data.<sup>106</sup> This is so that the accredited person can comply with its obligation under Privacy Safeguard 5 to notify of the collection of CDR data via the consumer's dashboard.<sup>107</sup>
- C.68 The consumer dashboard must contain the following details of each consent that has been given by the consumer:<sup>108</sup>
- the CDR data to which the consents relate
  - for a use consent,<sup>109</sup> the specific use or uses for which the consumer has given consent
  - the date on which the consumer gave the consents
  - whether the consents were for the collection of CDR data on a single occasion or over a period of time
  - if the consumer consented to collection and/or disclosure of CDR data over a period of time – what that period is and how often data has been (and is expected to be) collected and/or disclosed over that period
  - if the consents are current – when they will expire
  - if the consents are not current – when they expired
  - the information required to notify the consumer of the collection of their CDR data, being:
    - what CDR data was collected
    - when the CDR data was collected, and
    - the CDR participant of the CDR data that was collected.<sup>110</sup>
  - the information required to notify the consumer of the disclosure of their CDR data to an accredited person, being:
    - what CDR data was disclosed
    - when the CDR data was disclosed, and
    - the accredited person to whom the CDR data was disclosed, identified in accordance with any entry on the Register of Accredited Persons specified as being for that purpose,<sup>111</sup> and

---

<sup>106</sup> For further information regarding 'valid requests', see CDR Rule 4.3 and [Chapter 3 \(Privacy Safeguard 3\)](#).

<sup>107</sup> Privacy Safeguard 5 requires an accredited person to notify the consumer of the collection of their CDR data by updating the consumer's dashboard as soon as practicable to include certain matters. For further information, see CDR Rule 7.4 and [Chapter 5 \(Privacy Safeguard 5\)](#) of the CDR Privacy Safeguard Guidelines.

<sup>108</sup> CDR Rule 1.14(3).

<sup>109</sup> Including a de-identification consent (as defined in CDR Rule 1.10A) and a direct marketing consent for an accredited data recipient of particular CDR data to use that CDR data for the purposes of direct marketing (as per CDR Rule 1.10A).

<sup>110</sup> Privacy Safeguard 5 requires an accredited person to notify the consumer of the collection of their CDR data by updating the consumer's dashboard to include certain matters. For further information, see CDR Rule 7.4 and [Chapter 5 \(Privacy Safeguard 5\)](#).

<sup>111</sup> Privacy Safeguard 10 requires an accredited data recipient to notify the consumer of the disclosure of their CDR data to an accredited person by updating the consumer's dashboard to include certain matters. For further information, see CDR Rule 7.9(2) and [Chapter 10 \(Privacy Safeguard 10\)](#).

- from 1 July 2021, if applicable, details of each amendment that have been made to a consent.

C.69 The consumer dashboard must have a functionality that allows the consumer, at any time, to:<sup>112</sup>

- withdraw each consent
- elect for their CDR data be deleted once it becomes redundant, and
- withdraw an election regarding whether their CDR data should be deleted once it becomes redundant.

C.70 These functionalities must be simple and straightforward to use, and prominently displayed.<sup>113</sup>

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

C.71 From 1 July 2021, the consumer dashboard may also include a functionality that allows a consumer to amend an existing consent.<sup>114</sup>

C.72 Data holders also have an obligation under the CDR Rules to provide a consumer dashboard to a consumer when the data holder receives a consumer data request on behalf of the consumer by an accredited person. The consumer dashboard is used to manage the consumer's authorisations to disclose the consumer's CDR data to the accredited person.<sup>115</sup> For further information, see [Chapter B \(Key concepts\)](#) and the [Guide to privacy for data holders](#).

## Consumers may withdraw consent

C.73 A consumer who has given a consent to an accredited person in relation to their CDR data may withdraw the consent at any time.

C.74 Where a consumer withdraws a collection consent, the accredited person must notify:

- the data holder of the withdrawal in accordance with the data standards,<sup>116</sup> and/or
- the accredited data recipient of the CDR data, as soon as practicable.<sup>117</sup>

C.75 Where a consumer withdraws an AP disclosure consent, the accredited person must notify the accredited data recipient to whom the data is being disclosed to, as soon as practicable.<sup>118</sup>

---

<sup>112</sup> CDR Rule 1.14(1)(c).

<sup>113</sup> CDR Rule 1.14(1)(c).

<sup>114</sup> See paragraphs C.27 to C.36 for information on amending consents.

<sup>115</sup> CDR Rule 1.15.

<sup>116</sup> CDR Rule 4.13(2).

<sup>117</sup> CDR Rule 4.18B(2).

<sup>118</sup> CDR Rule 4.18B(3).

- C.76 An accredited person must allow a consumer to withdraw each consent they have provided by:<sup>119</sup>
- using the accredited person’s consumer dashboard, or
  - using a simple alternative method of communication made available by the accredited person.
- C.77 The functionality to withdraw consent on the consumer dashboard must be simple and straightforward to use, and prominently displayed.<sup>120</sup>
- C.78 The alternative method of communicating the withdrawal of consent must be simple.<sup>121</sup> In addition, it:
- should be accessible and straightforward for a consumer to understand and use, and
  - may be written or verbal. Where it is written, the communication may be sent by electronic means (such as email) or non-electronic means (such as by post).
- C.79 An accredited person may wish to ensure their alternative method of communication is consistent with existing channels already made available to its customers,<sup>122</sup> for example:
- through their telephone helpline, or
  - in the case of direct marketing consents, through embedded links in any email communications that will allow a consumer to notify the accredited person of their intention to ‘opt out’ of receiving direct marketing communications.<sup>123</sup>
- C.80 Where an accredited person 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:<sup>124</sup>
- 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).

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

<sup>119</sup> CDR Rule 4.13. A consumer must be enabled by an accredited person to independently withdraw each type of consent. For example, where a consumer provided a collection consent and use consent, the consumer can choose to withdraw only the collection consent. See the Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020* at [7].

<sup>120</sup> CDR Rule 1.14(1)(c).

<sup>121</sup> CDR Rule 4.13(1).

<sup>122</sup> Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2020*.

<sup>123</sup> For information about the use and disclosure of CDR data for direct marketing, see [Chapter 7 \(Privacy Safeguard 7\)](#).

<sup>124</sup> Consumer Experience Standards #16, Version 1.4.0.



## Effect of withdrawing consent

- C.81 The main consequence of the withdrawal of a consent is that the consent expires,<sup>125</sup> and the accredited person may no longer collect, use or disclose the CDR data (as applicable, depending on what category of consent has been withdrawn). Information about when a consent expires is contained in the following section.
- C.82 Where a collection consent for the collection of CDR data from a data holder is withdrawn, the accredited person must notify the data holder of the withdrawal in accordance with the data standards.<sup>126</sup>
- C.83 Where only a collection consent of particular CDR data is withdrawn, but other use consents<sup>127</sup> and/or disclosure consents<sup>128</sup> for that CDR data with the same accredited data recipient remain current, an accredited data recipient may continue to use<sup>129</sup> and/or disclose the relevant CDR data.
- C.84 Where a consumer withdraws each of their collection, use and disclosure consents, the CDR data is likely to become redundant data that the accredited person is required to delete or de-identify in accordance with Privacy Safeguard 12 (unless an exception applies).<sup>130</sup>
- C.85 If a consumer withdraws a consent using the accredited person's consumer dashboard, the withdrawal is immediately effective.<sup>131</sup>
- C.86 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.<sup>132</sup>
- C.87 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.

---

<sup>125</sup> CDR Rules 4.14(1)(a) and (1)(b).

<sup>126</sup> CDR Rule 4.13(2)(b). When a data holder is notified of the withdrawal of the collection consent, the authorisation given by the consumer to the data holder to disclose that CDR data expires: see CDR Rule 4.26(1)(d).

<sup>127</sup> Including a de-identification consent (as defined in CDR Rule 1.10A) and a direct marketing consent for an accredited data recipient of particular CDR data to use that CDR data for the purposes of direct marketing (as per CDR Rule 1.10A).

<sup>128</sup> Including both an AP disclosure consent (as defined in CDR Rule 1.10A) and a direct marketing consent for an accredited data recipient of particular CDR data to disclose that CDR data to another accredited person for the purposes of direct marketing: CDR Rule 1.10A(1)(c)(ii).

<sup>129</sup> An accredited person may only collect CDR data in response to a 'valid request' from a consumer: s 56EF of the Competition and Consumer Act. A request ceases to be 'valid' if the consumer withdraws their collection consent: CDR Rule 4.3(4). However, if the consumer does not also withdraw their use consent, the accredited person may continue to use the CDR data it has already collected to provide the requested goods or services: see the note under CDR Rule 4.3(4). See further CDR Rule 4.18A for ongoing notification requirements in this circumstance. For further information, see [Chapter 3 \(Privacy Safeguard 3\)](#).

<sup>130</sup> More information on 'redundant data' and the requirement to destroy or de-identify redundant data is in [Chapter 12 \(Privacy Safeguard 12\)](#).

<sup>131</sup> CDR Rule 4.14(1)(b).

<sup>132</sup> CDR Rule 4.13(2)(a).

- C.88 ‘Giving effect’ to the withdrawal includes updating the consumer dashboard to reflect that the consent has expired,<sup>133</sup> as required by CDR Rule 4.19.<sup>134</sup>
- C.89 Where a consumer has elected for their CDR data to be deleted upon becoming redundant data, withdrawal of a consent will not affect this election.<sup>135</sup>

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

## When a consent expires

- C.90 Where a consent expires, the accredited person may no longer collect, use or disclose the CDR data (as applicable, depending on what category of consent has expired).
- C.91 Where each of a consumer’s collection, use and disclosure consents expire, the CDR data is likely to become redundant data that the accredited person is required to delete or de-identify in accordance with Privacy Safeguard 12 (unless an exception applies).<sup>136</sup>
- C.92 CDR Rule 4.14 provides that a 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.<sup>137</sup> 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.<sup>138</sup>
  - **At the end of the period of consent (no longer than 12 months after consent was given):** a consent expires at the end of the specified period for which the consumer gave the consent.<sup>139</sup> This specified period cannot be longer than 12 months.<sup>140</sup>
  - **Twelve months after the consent was given or last amended:** a consent expires at the end of the period of 12 months after:
    - the consent was given, or
    - if the duration of the consent has been amended, the consent was last amended.<sup>141</sup>
  - **For a collection consent, when the accredited person is notified:**

<sup>133</sup> See CDR Rule 1.14(3)(g).

<sup>134</sup> CDR 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.

<sup>135</sup> CDR Rule 4.13(3) provides that withdrawal of a consent does not affect an election under CDR Rule 4.16 that the consumer’s collected CDR data be deleted once it becomes redundant. CDR Rule 4.16 is discussed in [Chapter 12 \(Privacy Safeguard 12\)](#).

<sup>136</sup> More information on ‘redundant data’ and the requirement to destroy or de-identify redundant data is in [Chapter 12 \(Privacy Safeguard 12\)](#).

<sup>137</sup> CDR Rule 4.14(1)(b).

<sup>138</sup> CDR Rule 4.14(1)(a).

<sup>139</sup> CDR Rule 4.14(1)(e).

<sup>140</sup> CDR Rule 4.12(1). CDR Rule 4.14(1)(d) reinforces this maximum duration by providing that consent expires after the 12 month period after the consent was given.

<sup>141</sup> CDR Rule 4.14(1)(d).

- **by the data holder of the withdrawal of authorisation:** upon such notification, the consent expires immediately.<sup>142</sup>
  - **by the accredited data recipient of the expiry of the AP disclosure consent:** upon such notification, the AP disclosure consent expires immediately.<sup>143</sup>
  - **For an AP disclosure consent, when the accredited data recipient is notified by the accredited person of the expiry of the collection consent:** upon such notification, the collection consent expires immediately.<sup>144</sup>
  - **If the accredited person's accreditation is revoked or surrendered:** consent expires when the revocation or surrender takes effect.<sup>145</sup>
  - **If an accredited person becomes a data holder, rather than an accredited data recipient, of particular CDR data:** upon becoming a data holder,<sup>146</sup> all consents in relation to the particular CDR data expire.<sup>147</sup>
  - **If another CDR Rule provides that a consent expires:**<sup>148</sup> (however, there are currently no such CDR Rules.)
- C.93 The expiry of a consumer's collection consent does not automatically result in expiry of the use consent relating to any CDR data that has already been collected.<sup>149</sup>
- C.94 In light of this, where a consumer's collection consent expires, but their use consent to provide the requested goods or services<sup>150</sup> remains current,<sup>151</sup> the accredited person must notify the consumer as soon as practicable that they may, at any time:<sup>152</sup>
- withdraw the use consent, and
  - make the election to delete redundant data in respect of that CDR data.<sup>153</sup>
- C.95 This notification must be given in writing (though not through the consumer's dashboard - although a copy of the notification may also be included in the consumer's dashboard).
- C.96 This notification is important because where the collection consent expired as a result of the consumer's withdrawal, and the consumer did not also withdraw their use consent, the

---

<sup>142</sup> CDR Rule 4.14(1A).

<sup>143</sup> CDR Rule 4.14(1B).

<sup>144</sup> CDR Rule 4.14(1B).

<sup>145</sup> A revocation or surrender takes effect when the fact that the accreditation has been revoked or surrendered is included in the Register of Accredited Persons: CDR Rule 5.22. For further information, see the ACCC's Accreditation Guidelines.

<sup>146</sup> As a result of s 56AJ(4) of the Competition and Consumer Act and related clause 7.2 of Schedule 3.

<sup>147</sup> CDR Rule 4.14(1C).

<sup>148</sup> CDR Rule 4.14(1)(f).

<sup>149</sup> See the note under CDR Rule 4.3(4). See also the Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020* at [8].

<sup>150</sup> Being the goods or services requested under CDR Rule 4.3(1) as part of the valid request.

<sup>151</sup> For example, because the consumer withdraws only their collection consent.

<sup>152</sup> CDR Rule 4.18A.

<sup>153</sup> See CDR Rule 4.16.

accredited person may continue to use the CDR data it has already collected to provide the requested goods or services.<sup>154</sup> A consumer might not be aware of this.<sup>155</sup>

## Notification requirements

### Notifications to consumers

C.97 The CDR Rules require an accredited person to provide the following notifications to a consumer about consents, collections and disclosures:<sup>156</sup>

- **Notification following consent:** There is a requirement to provide a notice in the form of a CDR receipt to the consumer after they provide, amend or withdraw a consent.<sup>157</sup> The matters that must be included in the CDR receipt are outlined in CDR Rule 4.18.<sup>158</sup>
- **Ongoing notification for collection and use consents:** There is an ongoing notification requirement regarding the currency of the consumer's collection and use consents. CDR Rule 4.20 requires an accredited person to notify the consumer that their collection consent and/or use consent is still current where 90 days have elapsed since the latest of the following events:<sup>159</sup>
  - the consumer consenting to the collection and/or use of their CDR data
  - the consumer last amending their collection and/or use consents
  - the consumer last using their consumer dashboard, or
  - the accredited person last sending the consumer a notification that their collection consent or use consent is still current.
- **Notification if collection consent expires:** Where a consumer's collection consent expires, but their use consent to provide the requested goods or services remains current, the accredited person must notify the consumer of the matters in CDR Rule 4.18A as soon as practicable.<sup>160</sup>

---

<sup>154</sup> See the note under CDR Rule 4.3(4).

<sup>155</sup> An accredited data recipient must also provide a statement in its CDR policy indicating the consequences to the consumer for withdrawing a consent to collect and use CDR data: CDR Rule 7.2(4)(a).

<sup>156</sup> For an accredited person who received consent, collected CDR data and/or disclosed CDR data on behalf of a principal in a CDR outsourcing arrangement, note the effect of CDR Rule 1.7(5) which provides that, in the CDR Rules, 'unless the contrary intention appears, a reference to an accredited person making a consumer data request, collecting CDR data, obtaining consents, providing a consumer dashboard, or using or disclosing CDR data does not include a reference to an accredited person doing those things on behalf of a principal in its capacity as the provider in an outsourced service arrangement, in accordance with the arrangement.'

For information on 'CDR outsourcing arrangements', see [Chapter B \(Key concepts\)](#), 'Outsourced service provider'.

<sup>157</sup> CDR Rule 4.18(1).

<sup>158</sup> CDR Rule 4.18(1). A CDR receipt must be given in writing other than through the consumer dashboard (although a copy of the CDR receipt may be included in the consumer's consumer dashboard). For more information, see CDR Rule 4.18.

<sup>159</sup> CDR Rules 4.20(3) and (4) state that this notification must be given in writing otherwise than through the consumer's consumer dashboard, however a copy may be included on the consumer dashboard.

<sup>160</sup> CDR Rule 4.18A. For further information on when a consent expires, see paragraphs C.90 to C.96.

- **Notification of collection:** There is a requirement to notify the consumer of the collection of their CDR data as soon as practicable after the collection of CDR data.<sup>161</sup>
- **Notification of disclosure:** There is requirement to notify the consumer of the disclosure of their CDR data to an accredited person as soon as practicable after the disclosure of the CDR data.<sup>162</sup>
- **Updating the consumer's dashboard:** There is a general obligation to update the consumer's dashboard as soon as practicable after the information required to be contained on the consumer dashboard changes.<sup>163</sup>

C.98 Data holders also have a general obligation under the CDR Rules to update the consumer's consumer dashboard as soon as practicable, where there is a change in the information required for that dashboard.<sup>164</sup> In addition, data holders must notify the consumer of the disclosure of their CDR data as soon as practicable after the disclosure of CDR data.<sup>165</sup>

## Notifications to CDR participants

C.99 An accredited person must provide the following notifications about consents to CDR participants under the CDR Rules:

- **Notification to accredited data recipient if collection consent expires:** Where a consumer's collection consent expires, and the CDR data is being collected from an accredited data recipient, the accredited person must notify that accredited data recipient of the CDR data, as soon as practicable.<sup>166</sup>
- **Notification to data holder if collection consent is withdrawn:** Where a consumer withdraws their collection consent, and the CDR data is being collected from a data holder, the accredited person must notify that data holder of the withdrawal in accordance with the data standards.<sup>167</sup>
- **Notification if collection consent is amended:** Where a consumer amends their collection consent, the accredited person must notify the relevant CDR participant/s that the consent has been amended, in accordance with CDR Rule 4.18C.<sup>168</sup>

---

<sup>161</sup> Privacy Safeguard 5 requires an accredited data recipient to notify the consumer of the collection of their CDR data by updating the consumer's dashboard to include certain matters. For further information, see CDR Rule 7.4 and [Chapter 5 \(Privacy Safeguard 5\)](#).

<sup>162</sup> Privacy Safeguard 10 requires an accredited data recipient to notify the consumer of the disclosure of their CDR data to an accredited person by updating the consumer's dashboard to include certain matters. For further information, see CDR Rule 7.9(2) and [Chapter 10 \(Privacy Safeguard 10\)](#).

<sup>163</sup> CDR Rule 4.19.

<sup>164</sup> CDR Rule 4.27.

<sup>165</sup> Privacy Safeguard 10 requires a data holder to notify the consumer of the collection of their CDR data by updating the consumer's dashboard to include certain matters. For further information, see CDR Rule 7.9 and [Chapter 10 \(Privacy Safeguard 10\)](#).

<sup>166</sup> CDR Rule 4.18B(2).

<sup>167</sup> CDR Rule 4.13(2).

<sup>168</sup> For further information on the requirements under CDR Rule 4.18C, see paragraph C.34.

- **Notification if AP disclosure consent expires:** Where a consumer's AP disclosure consent expires, the accredited person must notify the accredited data recipient to whom the data is being disclosed to, as soon as practicable.<sup>169</sup>

## Authorisation

- C.100 Before an accredited person can receive a consumer's CDR data from a data holder, the consumer must authorise the data holder to disclose the particular data to that accredited person.
- C.101 After receiving a consumer data request, the data holder must seek the consumer's authorisation for required or voluntary consumer data in accordance with Division 4.4 of the CDR Rules and the data standards,<sup>170</sup> unless an exception applies.<sup>171</sup>
- C.102 For the banking sector, for requests that relate to joint accounts, in some cases, the data holder might need to seek an authorisation (known as an 'approval') from the other joint account holder/s.<sup>172</sup>
- C.103 Once a data holder has received this authorisation it:
- must disclose the required consumer data, and
  - may disclose the relevant voluntary consumer data
- through its accredited person request service and in accordance with the data standards, unless an exception applies.<sup>173</sup>
- C.104 The flow chart below demonstrates the role of authorisation in the key information flow between a consumer, accredited person and data holder.
- C.105 For further information on a data holder's authorisation obligations, see the [Guide to privacy for data holders](#).

---

<sup>169</sup> CDR Rule 4.18B(3).

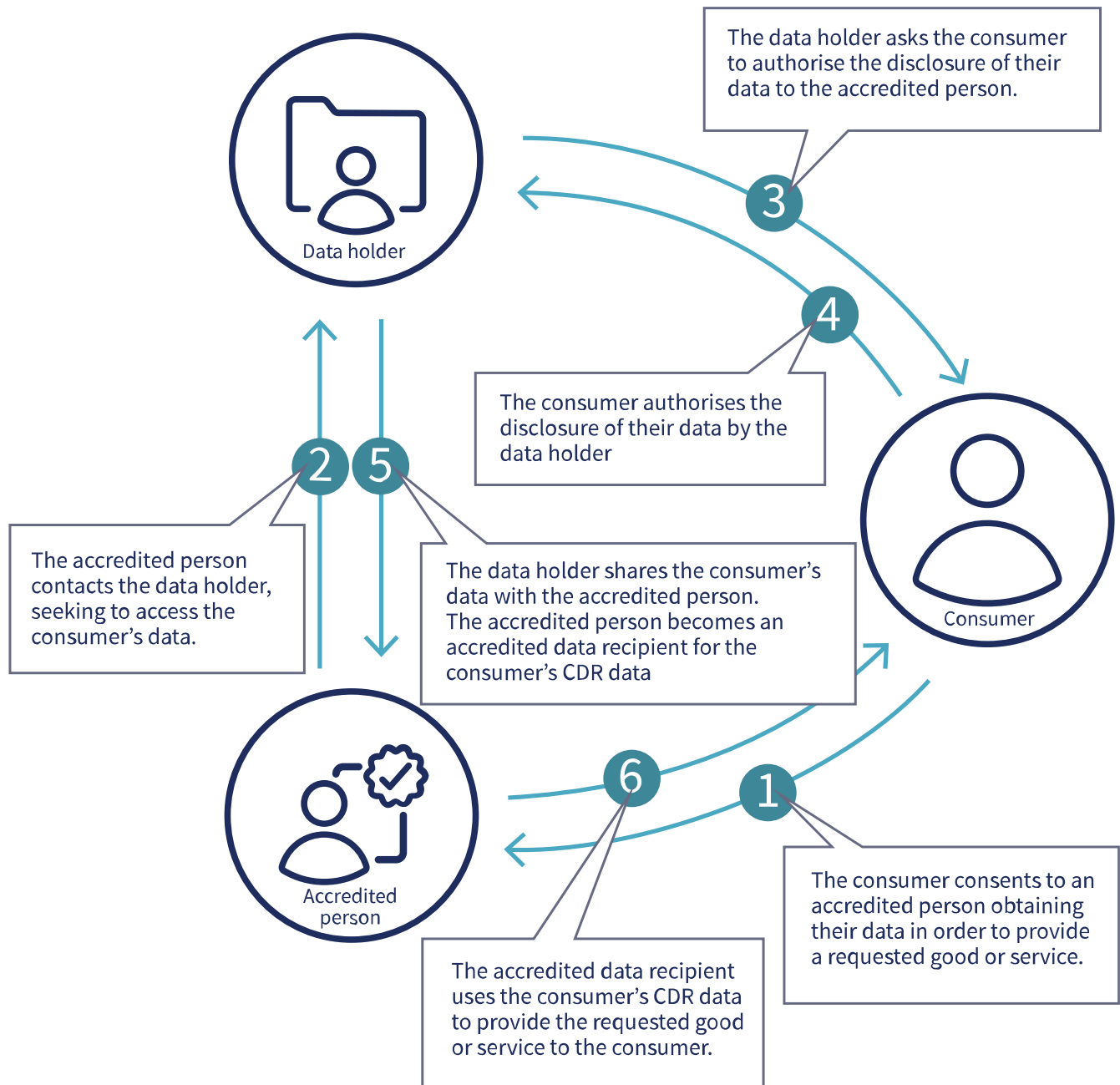
<sup>170</sup> See CDR Rule 4.5.

<sup>171</sup> See CDR Rule 4.7.

<sup>172</sup> See subdivision 4.3.2 of Schedule 3 to the CDR Rules, which set out how consumer data requests to data holders that relate to joint accounts are handled in the CDR regime.

<sup>173</sup> See CDR Rule 4.6A.

## Overview: key information flow in the CDR regime



## Chapter 1:

# Privacy Safeguard 1 —

## Open and transparent management of CDR data

Version 3.0, June 2021



# Contents

<b>Key points</b>	<b>3</b>
<b>What does Privacy Safeguard 1 say?</b>	<b>3</b>
<b>Importance of open and transparent management of CDR data and having a CDR policy</b>	<b>3</b>
<b>Who Privacy Safeguard 1 applies to</b>	<b>4</b>
<b>How Privacy Safeguard 1 interacts with the Privacy Act</b>	<b>4</b>
<b>Implementing practices, procedures and systems to ensure compliance with the CDR regime</b>	<b>5</b>
Circumstances that affect reasonable steps	6
Existing privacy governance arrangements	8
Have a CDR data management plan	9
A suggested approach to compliance with Privacy Safeguard 1	9
<b>Having a CDR policy</b>	<b>12</b>
Information that must be included in a CDR policy	13
Availability of the CDR policy	16
Consumer requests for a CDR policy	16
Interaction between an entity's privacy policy and CDR policy	16

## Key points

- Privacy Safeguard 1, together with consumer data rule (CDR Rule) 7.2, outlines the requirements for all consumer data right (CDR) entities (accredited persons who are or who may become an accredited data recipient of CDR data, data holders and designated gateways) to 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 CDR 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 CDR 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 CDR Rules and provided to the consumer upon request.

## Importance of open and transparent management of CDR data and having a CDR policy

- 1.2 The objective of Privacy Safeguard 1 is to ensure CDR entities handle CDR data in an open and transparent way. It is the bedrock principle.
- 1.3 By complying with Privacy Safeguard 1, CDR entities will be establishing accountable and auditable practices, procedures and systems that will assist with compliance with all the other privacy safeguards. This leads to a trickle-down effect where privacy is automatically considered when handling CDR data, resulting in better overall privacy management, practice and compliance through a 'privacy-by-design' approach.
- 1.4 It is also important that consumers are aware of how their CDR data is handled, and can inquire or make complaints to resolve their concerns. A CDR policy achieves this transparency by outlining how the CDR entity manages CDR data, and by providing information on how a consumer can complain and how the CDR entity will deal with a complaint.
- 1.5 CDR policies are also a key tool for ensuring open and transparent management of CDR data which can build trust and engage consumers.

## Who Privacy Safeguard 1 applies to

- 1.6 Privacy Safeguard 1 applies to data holders, designated gateways and accredited persons who are or who may become accredited data recipients of CDR data.<sup>1</sup>

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

## How Privacy Safeguard 1 interacts with the Privacy Act

- 1.7 It is important to understand how Privacy Safeguard 1 interacts with the *Privacy Act 1988* (the Privacy Act) and Australian Privacy Principle (APP) 1.<sup>2</sup>
- 1.8 APP 1 requires APP entities to manage personal information in an open and transparent way (see [Chapter 1: APP 1 — Open and transparent management of personal information of the APP Guidelines](#)).

CDR entity	Privacy protections that apply in the CDR context
<b>Accredited person who may become an accredited data recipient</b>	<p><b>Privacy Safeguard 1</b></p> <p>When an accredited person is planning to handle a CDR consumer's data, and may become an accredited data recipient of that CDR data (for example, because they are seeking to collect it), Privacy Safeguard 1 applies.</p> <p>APP 1 does not apply to the accredited person in relation to that CDR data.<sup>3</sup></p>
<b>Accredited data recipient</b>	<p><b>Privacy Safeguard 1</b></p> <p>An accredited data recipient of a consumer's CDR data must comply with Privacy Safeguard 1 in relation to the management of that CDR data.</p> <p>APP 1 does not apply to the accredited data recipient in relation to that CDR data.<sup>4</sup></p>

<sup>1</sup> An accredited person 'may become' an accredited data recipient when they are seeking to collect CDR data. This means that an accredited person must ensure that they comply with their Privacy Safeguard 1 obligations before they seek to collect CDR data.

<sup>2</sup> 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.

<sup>3</sup> See ss 56EC(4) and 56ED(1) of the Competition and Consumer Act.

**Note:** If Privacy Safeguard 1 does not apply, APP 1 may continue to apply to other open and transparent management of the individual's personal information where the accredited person is an APP entity (see s 56EC(4) and (5)(aa) of the Competition and Consumer Act). Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See s 6E(1D) of the Privacy Act.

<sup>4</sup> The APPs do not apply to an accredited data recipient of the CDR data in relation to the CDR data (s 56EC(4)(a) of the Competition and Consumer Act). However, this does not affect how the APPs apply to accredited persons in relation to the open and transparent management of the individual's other personal information outside the CDR system. It also does not affect how the APPs apply to CDR data where the accredited person does not become an accredited data recipient of the CDR data. (see s 56EC(4) and (5)(aa) of the Competition and Consumer Act). Note: Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See s 6E(1D) of the Privacy Act.

CDR entity	Privacy protections that apply in the CDR context
<b>Designated gateway</b>	<p><b>APP 1 and Privacy Safeguard 1</b></p> <p>A designated gateway must comply with:</p> <ul style="list-style-type: none"> <li>• Privacy Safeguard 1 in relation to the handling of CDR data, and</li> <li>• APP 1 in relation to the handling of personal information (if they are an APP entity).</li> </ul> <p>As the obligations in Privacy Safeguard 1 apply generally to an entity's handling of data, a designated gateway must have systems, practices and procedures to comply with both the privacy safeguards and the APPs (including having both a CDR policy and a privacy policy in place).</p>
<b>Data holder</b>	<p><b>APP 1 and Privacy Safeguard 1</b></p> <p>A data holder must comply with:</p> <ul style="list-style-type: none"> <li>• Privacy Safeguard 1 in relation to the handling of CDR data, and</li> <li>• APP 1 in relation to the handling of personal information (if they are an APP entity).</li> </ul> <p>This means that a data holder must have systems, practices and procedures to comply with both the privacy safeguards and the APPs (including having both a CDR policy and a privacy policy in place).<sup>5</sup></p>

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

- 1.9 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 CDR 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 CDR Rules.
- 1.10 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.
- 1.11 The CDR Rules contain several governance mechanisms, policies and procedures that will assist entities to take steps that are reasonable to comply with the CDR regime.<sup>6</sup> However, while compliance with the CDR 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.

<sup>5</sup> See section 56AJ of the Competition and Consumer Act for the meaning of data holder.

<sup>6</sup> For example, accredited persons/accredited data recipients are required to establish a formal governance framework for managing information security risks. See Privacy Safeguard 12, CDR Rule 5.12, CDR Rule 7.11 and Schedule 2 to the CDR Rules. For further information see [Chapter 12 \(Privacy Safeguard 12\)](#) and the ACCC's Supplementary Accreditation Guidelines on Information Security available on the ACCC's Accreditation Guidelines page.

- 1.12 To comply with Privacy Safeguard 1, CDR entities need to proactively consider, plan and address how to implement any practices, procedures and systems under the privacy safeguards and the CDR Rules (including how these interact with other obligations). This will assist CDR entities to manage CDR data in an open and transparent way, in accordance with the object of Privacy Safeguard 1.<sup>7</sup>
- 1.13 Compliance with Privacy Safeguard 1 should therefore be understood as a matter of good governance.

**Risk point:** Entities who implement the requirements of the privacy safeguards and the CDR Rules in isolation or at a late stage risk incurring unnecessary costs, and/or implementing inadequate solutions that fail to address the full compliance picture.

**Privacy tip:** Entities should take a ‘privacy-by-design’ approach in relation to handling CDR data across and within their organisation. This ensures CDR requirements are considered holistically. A tool that may assist an entity in this regard is the CDR data management plan, as outlined in paragraphs 1.29 to 1.32. The OAIC’s suggested approach to compliance with Privacy Safeguard 1 in paragraphs 1.33 to 1.42 may also be of assistance.

## Circumstances that affect reasonable steps

- 1.14 The requirement under Privacy Safeguard 1 to implement practices, procedures and systems is qualified by a ‘reasonable steps’ test.
- 1.15 This requires an objective assessment of what is considered reasonable in the specific circumstances, which could include:
- the CDR Rules and other legislative obligations that apply to the CDR entity
  - the nature of the CDR entity
  - the amount of CDR data handled by the CDR entity
  - the possible adverse consequences for a consumer in the case of a breach, and
  - the practicability, including time and cost involved.

## The CDR regime obligations that apply to the CDR entity

- 1.16 The CDR regime obligations (such as the privacy safeguards and the CDR Rules) that apply to the entity will be relevant to determining what steps will be reasonable in terms of compliance with Privacy Safeguard 1.
- 1.17 For example, the obligations that apply to accredited persons/accredited data recipients are in many cases different to those that apply to data holders and will therefore require the development and implementation of different practices, procedures and systems to achieve compliance.
- 1.18 Further, where an entity participates in the CDR regime in more than one capacity (e.g. as a data holder and an accredited person), this will also affect what constitutes reasonable

---

<sup>7</sup> Section 56ED(1) of the Competition and Consumer Act.

steps, and the entity will need to put in place mechanisms to ensure it complies with the CDR regime in all its different CDR entity capacities.

### Examples of key CDR regime privacy obligations

The CDR regime imposes a range of privacy obligations upon CDR entities. Some of these privacy obligations apply to all CDR entities, while other privacy obligations apply only to a particular entity type. Entities will need to ensure that all of the relevant obligations that apply to them are considered when deciding on the steps to be taken in relation to Privacy Safeguard 1.

For example, an accredited data recipient of CDR data must comply with the privacy safeguards in relation to the CDR data.

However, a data holder needs to comply with the APPs in relation to CDR data that is also personal information with the exception of APPs 10 and 13, which are replaced by Privacy Safeguards 11 and 13 once the data holder is required or authorised to disclose the CDR data under the CDR Rules. Data holders must also comply with both Privacy Safeguard 1 and APP 1, as well as Privacy Safeguard 10.<sup>8</sup> Information regarding compliance with each of the privacy safeguards is available in the relevant chapters of these [Guidelines](#).

In addition to obligations under the privacy safeguards, accredited persons/accredited data recipients and data holders must also consider their obligations in the CDR Rules for the purposes of compliance with Privacy Safeguard 1. These obligations will need to be reflected in the steps taken under Privacy Safeguard 1. For example:

- Accredited persons/accredited data recipients have obligations to report regularly regarding their ongoing information security obligations,<sup>9</sup> including privacy and security training to staff.<sup>10</sup>
- Data holders have obligations relating to consumer data request services.<sup>11</sup>
- Both accredited data recipients and data holders have obligations to provide consumers with access to copies of records upon request.<sup>12</sup>
- In the banking sector, both accredited persons and data holders must have internal dispute resolution processes that meet the requirements under the Australian Securities and Investments Commission's [Regulatory Guide 165](#) on internal and external dispute resolution.<sup>13</sup>

<sup>8</sup> Privacy Safeguard 10 does not have an APP equivalent.

<sup>9</sup> Part 2 of Schedule 1 to the CDR Rules. For further information, see the ACCC's Supplementary Accreditation Guidelines on Information Security available on the ACCC's Accreditation Guidelines page.

<sup>10</sup> Accredited persons/accredited data recipients must ensure all users undergo mandatory security and privacy training prior to interacting with the CDR data environment, with 'refresher courses' provided at least annually: see Privacy Safeguard 12, CDR Rule 5.12 and Part 2 of Schedule 2 to the CDR Rules. For further information, see the ACCC's Supplementary Accreditation Guidelines on Information Security available on the ACCC's Accreditation Guidelines page.

<sup>11</sup> For further information on consumer data request services, authorisation, disclosure of CDR data and a data holder's privacy obligations more generally, see the [Guide to privacy for data holders](#).

<sup>12</sup> CDR Rule 9.5. Accredited data recipients and data holders are required to keep and maintain certain records as outlined in CDR Rule 9.3. They are also required to comply with the reporting requirements in CDR Rule 9.4.

<sup>13</sup> See CDR Rule 5.12(1) (for accredited persons) and Part 6 of the CDR Rules (for data holders).

## Nature of the entity

- 1.19 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.
- 1.20 For instance, where a CDR entity uses outsourced service 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

- 1.21 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

- 1.22 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

- 1.23 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.
- 1.24 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.
- 1.25 CDR entities are also not excused from any specific processes, procedures or systems that are required by the CDR regime.

## Existing privacy governance arrangements

- 1.26 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.<sup>14</sup>
- 1.27 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.
- 1.28 Entities will need to take further action to modify practices, procedures and systems to ensure compliance with the particularities of the CDR regime, including the Privacy Safeguards and CDR Rules.

---

<sup>14</sup> CDR data protected by the privacy safeguards will also be 'personal information' under the Privacy Act. For further information, see [Chapter A \(Introductory matters\)](#) of the CDR Privacy Safeguard Guidelines.

## Have a CDR data management plan

- 1.29 A useful tool that can help CDR entities to plan and document the steps they will take to implement practices, procedures and systems under Privacy Safeguard 1 is a CDR data management plan.
- 1.30 A CDR data management plan is a document that identifies specific, measurable goals and targets, and sets out how an entity will meet its ongoing compliance obligations under Privacy Safeguard 1. As part of this, the CDR data management plan could set out the tasks an entity will undertake to ensure compliance with Privacy Safeguard 1.
- 1.31 The CDR data management plan should also set out the processes that will be used to measure and document the CDR entity's performance against their CDR data management plan.
- 1.32 Where entities have an existing privacy management plan, they may wish to update it with CDR activities so that it is integrated into the entity's privacy management processes. Alternatively, they may choose to have a separate CDR data management plan.

## A suggested approach to compliance with Privacy Safeguard 1

- 1.33 The ongoing compliance requirement in Privacy Safeguard 1 can be addressed in a range of different ways, but should be tailored to the circumstances of the particular entity.
- 1.34 The following sections outline a suggested method for how steps could be taken to implement practices, procedures and systems under Privacy Safeguard 1.
- 1.35 The suggested method consists of four overarching steps:
  - **Embed** a culture that respects and protects CDR data.
  - **Establish** robust and effective privacy practices, procedures and systems.
  - **Review** and evaluate privacy processes.
  - **Enhance** response to privacy issues.

**Privacy tip:** Where a CDR entity has a CDR data management plan, they may choose to structure that plan around the four overarching steps outlined in paragraph 1.35.

## Embed a culture that respects and protects CDR data

- 1.36 Good CDR data management stems from good data and information governance that creates a culture of privacy that respects and protects CDR data.
- 1.37 To embed a culture of privacy, entities could:
  - Appoint a member of senior management to be responsible for the strategic leadership and overall management of CDR data.
  - Appoint an officer (or officers) to be responsible for the day to day managing, advising and reporting on privacy safeguard issues.
  - Record and report on how datasets containing CDR data are treated, managed and protected.



- Implement reporting mechanisms that ensure senior management are routinely informed about privacy and data management issues.

## Establish robust and effective privacy practices, procedures and systems

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

1.39 For example, an entity should:

- Implement risk management processes that allow identification, assessment and management of privacy risks, including CDR security risks. As part of this, accredited persons/accredited data recipients should consider their obligations to implement strong minimum information security controls under Schedule 2 to the Rules.<sup>15</sup>
- Establish clear processes for reviewing and responding to CDR data complaints. For the banking sector, CDR entities should consider their obligations to have internal dispute resolution processes that meet the relevant ASIC requirements.<sup>16</sup>
- 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 of once per year. Note that accredited persons/accredited data recipients already have obligations to ensure all users undergo mandatory security and privacy training prior to interacting with the CDR data environment, with ‘refresher courses’ provided at least annually.<sup>17</sup>
- Establish processes that allow consumers to promptly and easily access and correct their CDR data, in accordance with the privacy safeguards and CDR Rules. As part of this, and in relation to access, data holders should consider their obligations to provide consumer data request services.<sup>18</sup> In relation to correction, CDR entities should consider their obligations under Privacy Safeguard 13 to respond to correction requests from consumers.<sup>19</sup>

**Privacy tip:** As a starting point for deciding what practices, procedures and systems should be established, a CDR entity should consider their privacy obligations under the privacy safeguards and CDR Rules.

See paragraphs 1.16 to 1.18 for examples of the CDR regime privacy obligations that apply to a CDR entity.

<sup>15</sup> See Privacy Safeguard 12, CDR Rule 5.12 and Schedule 2 to the CDR Rules. For further information see [Chapter 12 \(Privacy Safeguard 12\)](#) and the ACCC’s Supplementary Accreditation Guidelines on Information Security available on the ACCC’s Accreditation Guidelines page.

<sup>16</sup> The obligation is to have internal dispute resolution processes that meet the requirements under the Australian Securities and Investments Commission’s Regulatory Guide 165 on internal and external dispute resolution. See CDR Rule 5.12(1) (for accredited persons) and Part 6 of the CDR Rules (for data holders).

<sup>17</sup> See Privacy Safeguard 12, CDR Rule 5.12(1), CDR Rule 7.11 and Schedule 2 to the CDR Rules.

<sup>18</sup> See CDR Rule 1.13. For further information regarding consumer data request services, see the [Guide to privacy for data holders](#).

<sup>19</sup> See [Chapter 13 \(Privacy Safeguard 13\)](#) for further information.

## Regularly reviewing and evaluating privacy processes

- 1.40 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.
  - Create feedback channels for both staff and consumers to continue to learn lessons from complaints and breaches, as well as customer feedback more generally.
- 1.41 Notably, accredited persons are required to provide regular assurance reports (an audit report) and attestation statements concerning compliance with certain information security requirements.<sup>20</sup>

**Risk point:** Changes to a CDR entity's role in the CDR regime and/or information handling practices may mean that existing practices, procedures and systems are no longer fit for purpose.

**Privacy tip:** When reviewing and evaluating privacy processes, a CDR entity should consider a range of factors including:

- Role in the CDR regime – has the entity taken on a new role, for example by becoming an accredited person in addition to being a data holder?<sup>21</sup>
- Method of service delivery — has the entity changed the way in which it provides goods or services to CDR consumers, for example, by using outsourced service providers to perform any of its functions?<sup>22</sup>
- Online platforms – has the entity changed the online platforms used to communicate with CDR consumers, for example by creating a new mobile application?<sup>23</sup>

The answers to these questions will assist a CDR entity to make the necessary and appropriate changes to practices, procedures and systems (as recommended in the following 'Enhance response to privacy issues' section).

*cont*

<sup>20</sup> These obligations are contained in CDR Rule 5.9 and clause 2.1 of Part 2 of Schedule 1 to the CDR Rules regarding default conditions on accreditation. For further information, see the ACCC's Supplementary Accreditation Guidelines on Information Security available on the ACCC's Accreditation Guidelines page.

<sup>21</sup> Different CDR regime obligations apply depending on what capacity an entity is acting in. See paragraphs 1.16 to 1.18 for further information.

<sup>22</sup> An outsourced service provider is a person:

- who is accredited and collects CDR data from a CDR participant on behalf of an accredited person under a CDR outsourcing arrangement, and/or
- to whom an accredited person discloses CDR data under a CDR outsourcing arrangement.

Accredited persons must ensure they comply with the CDR Rules relating to outsourced service providers. For further information, see [Chapter B \(Key concepts\)](#) of the CDR Privacy Safeguard Guidelines.

<sup>23</sup> By way of example, a CDR entity would need to ensure their CDR policy was available on these new online platforms: see CDR Rule 7.2(8), which requires accredited data recipients and data holders to make their CDR policy readily available through the online service that they ordinarily use to deal with consumers, such as their website or mobile applications.

**Privacy tip:** Where a CDR entity has a CDR data management plan, they should set out the processes that will be used to measure and document the CDR entity's performance against their CDR data management plan, and measure performance against this plan as part of reviewing and evaluating privacy processes.

## Enhance response to privacy issues

- 1.42 Good privacy management requires entities to be proactive, forward thinking and to anticipate future challenges. To enhance response to privacy issues, entities should make a commitment to:
- Use the results of the evaluations to make necessary and appropriate changes to an organisation's practices, procedures and systems.
  - Consider having practices, procedures and systems externally assessed to identify areas where privacy processes may be improved.<sup>24</sup>
  - Continuously monitor and address new privacy risks.

**Privacy tip:** Where a CDR entity has a CDR data management plan, they should ensure this plan is updated to reflect any changes to the entity's practices, procedures and systems and accommodate new privacy risks.

## Having a CDR policy

- 1.43 Privacy Safeguard 1 requires all CDR entities to have and maintain a clearly expressed and up-to-date CDR policy.
- 1.44 The CDR policy must be in the form of a document that is distinct from any of the CDR entity's privacy policies.<sup>25</sup> The Information Commissioner may, but has not, approved a form for the CDR policy.<sup>26</sup>
- 1.45 Privacy Safeguard 1 and CDR Rule 7.2 set out the requirements for what information must be included in a CDR policy, how it must be made available and what form it should be in.<sup>27</sup>
- 1.46 There are different requirements depending on whether the CDR entity is an accredited person/accredited data recipient, a data holder, or a designated gateway, as set out below.
- 1.47 Where an entity occupies more than one role in the CDR regime (for example is both a data holder and an accredited person), the entity can either have a single CDR policy that outlines how CDR data is handled in both capacities, or a separate CDR policy for each capacity.

<sup>24</sup> Accredited persons have obligations to provide regular assurance reports (an audit report) and attestation statements concerning compliance with certain Privacy Safeguard 12 CDR Rules. See the ACCC's Supplementary Accreditation Guidelines on Information Security available on the ACCC's Accreditation Guidelines page.

<sup>25</sup> CDR Rule 7.2(2).

<sup>26</sup> Section 56ED(3)(b) of the Competition and Consumer Act and CDR Rule 7.2(1).

<sup>27</sup> The Information Commissioner may, but has not, approved a form for the CDR policy: section 56ED(3)(b) of the Competition and Consumer Act and CDR Rule 7.2(1).

**Privacy tip:** The OAIC has prepared a [Guide to developing a CDR policy](#) to assist CDR entities to prepare and maintain a CDR policy. It provides detailed guidance about what must be included in a CDR policy, as well as a suggested process, and a checklist to help ensure all requirements have been met.

## Information that must be included in a CDR policy

- 1.48 The following sections outline the minimum requirements for information that must be included in a CDR policy.
- 1.49 For further information and discussion about the requirements for a CDR policy, see the OAIC's [Guide to developing a CDR policy](#).

## Accredited persons/Accredited data recipients

- 1.50 Privacy Safeguard 1 requires that accredited persons who are or may become accredited data recipients must include the following in their CDR policy:
- the classes of CDR data that are (or may be) held by or on behalf of the entity as an accredited data recipient. The classes of CDR data for each sector will be set out in the relevant designation instrument. For example, for the banking sector the designation instrument sets out three classes of information: customer information,<sup>28</sup> product use information,<sup>29</sup> and information about a product<sup>30</sup>
  - how the CDR data is (or is to be) held by or on behalf of the entity as an accredited data recipient
  - purposes for which the entity may 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 to accredited persons is likely, and the countries those persons are likely to be based in, if practicable to specify this
  - circumstances in which the entity may disclose CDR data to a person who is not an accredited person<sup>31</sup>
  - events about which the entity will notify the consumers of such CDR data,<sup>32</sup> and

<sup>28</sup> Specified in section 6 of the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019.

<sup>29</sup> Specified in section 7 of the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019.

<sup>30</sup> Specified in section 8 of the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019.

<sup>31</sup> An accredited data recipient is not authorised to disclose CDR data to a non-accredited person, except directly to the consumer or to an outsourced service provider in accordance with CDR Rule 7.5(1).

<sup>32</sup> The events about which an accredited person will notify a consumer will include:

- when a consumer gives consent to the person collecting, using and/or disclosing their CDR data or withdraws such a consent (for further information, see Chapter C (Consent))
- the collection of a consumer's CDR data (see Chapter 5 (Privacy Safeguard 5))
- the disclosure of a consumer's CDR data to an accredited person (see Chapter 10 (Privacy Safeguard 10))

- when the entity must delete or de-identify CDR data in accordance with a request by a consumer.

1.51 In addition, CDR Rule 7.2(4) provides other matters that an accredited data recipient must include 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 (whether based in Australia or based overseas, and whether or not any is an accredited person).
- For each such service provider, the nature of the services it provides and the CDR data or classes of CDR data that may be disclosed to it.
- Where the entity wishes to undertake general research using de-identified CDR data, a description of the research to be conducted and any benefits to be provided to the CDR consumer for consenting to the use.<sup>33</sup>
- Where the entity is likely to disclose CDR data to an overseas, non-accredited outsourced service provider, the countries where there are likely to be based in the CDR policy, where practicable.<sup>34</sup>
- If applicable, the following information about de-identification of CDR data that is not redundant data:
  - how the accredited data recipient uses CDR data that has been de-identified in accordance with the CDR data de-identification process to provide goods or services to consumers
  - how the entity de-identifies CDR data, including a description of techniques that it uses to de-identify CDR data, and
  - if the entity ordinarily discloses (by sale or otherwise) de-identified CDR data to one or more persons: the fact of this disclosure; the classes of persons such data is ordinarily disclosed to; and the purposes for which the accredited data recipient discloses de-identified CDR data.
- The following information about deletion of redundant CDR data:
  - when it deletes redundant data
  - how a CDR consumer may elect for this to happen, and
  - how it deletes redundant data.

- 
- any ongoing notification requirements concerning a consumer's consent (see Chapter C (Consent))
  - any notification requirements concerning or in relation to the expiry of a consumer's consent (see Chapter C (Consent))
  - any response to a consumer's correction request under Privacy Safeguard 13 (see Chapter 13 (Privacy Safeguard 13)), and
  - any eligible data breach affecting a consumer under the Notifiable Data Breach scheme (see Chapter 12 (Privacy Safeguard 12) and the OAIC's [Data breach preparation and response guide](#)).

<sup>33</sup> CDR Rule 7.5(1)(aa) permits the use or disclosure of CDR data for general research, where it has been de-identified in accordance with the CDR data de-identification processes.

<sup>34</sup> See sections 56ED(5)(e)-(f) of the Competition and Consumer Act, and CDR Rule 7.2(4)(d).

- If applicable, the following information about de-identification of redundant data:
  - if the de-identified data is used by the accredited data recipient—examples of how the accredited data recipient ordinarily uses de-identified data
  - how the entity de-identifies CDR data, including a description of techniques that it uses to de-identify CDR data, and
  - if the entity ordinarily discloses (by sale or otherwise) de-identified CDR data to one or more persons: the fact of this disclosure; the classes of persons such data is ordinarily disclosed to; and the purposes for which the accredited data recipient discloses de-identified CDR data.
- The following information about the consumer's election to delete their CDR data:
  - how the election operates and its effect, and
  - how consumers can exercise the election.
- Further information regarding how a consumer can complain and how the entity will deal with the complaint, specifically:
  - where, how and when a complaint can be lodged
  - when a consumer should expect an acknowledgement of their complaint
  - what information is required from the complainant
  - the complaint handling process, including time periods associated with the various stages
  - options for redress, and
  - options for review.

## Data holder

1.52 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.

1.53 In addition, the CDR 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 are,<sup>35</sup> and
- 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

---

<sup>35</sup> Voluntary product data means CDR data for which there are no consumers that is not required product data: clause 3.1 of Schedule 3 to the CDR Rules. Voluntary consumer data means CDR data for which there are consumers that is not required consumer data: clause 3.2 of Schedule 3 to the CDR Rules.

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

## Designated gateway

1.54 Privacy Safeguard 1 requires that designated gateways must include the following in their CDR policy:

- an explanation of how the entity will act between persons to facilitate the disclosure of the CDR data, the accuracy of the CDR data, or any other matters required under the CDR Rules, and
- how a consumer may complain about a failure of the CDR entity to comply with the privacy safeguards or the CDR Rules, and how the CDR entity will deal with such a complaint.

## Availability of the CDR policy

1.55 The CDR policy must be publicly and freely available in accordance with the CDR Rules.<sup>36</sup> This furthers the objective of Privacy Safeguard 1 of ensuring that CDR data is managed in an open and transparent way.

1.56 The CDR Rules provide that the CDR policy must be readily available on each online service where the CDR entity ordinarily deals with CDR consumers.<sup>37</sup>

## 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 CDR Rule 7.2.

1.58 CDR Rule 7.2 provides 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.

## Interaction between an entity's privacy policy and CDR policy

1.59 An entity should be aware that their privacy policy and CDR policy obligations may overlap or relate to each other.

1.60 While the privacy policy and CDR policy need to be separate,<sup>38</sup> the entity's CDR policy and privacy policy may reference and link to each other where appropriate or required.

1.61 For example, Privacy Safeguard 1 requires a data holder's CDR policy to explain how a consumer may access their CDR data and seek its correction.<sup>39</sup> As a consumer who is an individual may also access their data through APP 12 or seek correction of their data under

---

<sup>36</sup> Section 56ED(7) of the Competition and Consumer Act.

<sup>37</sup> CDR Rule 7.2(8).

<sup>38</sup> CDR Rule 7.2(2).

<sup>39</sup> Section 56ED(4)(a) of the Competition and Consumer Act.

APP 13 (where the data holder has not been authorised or required to disclose that data), the CDR policy must explain these alternative processes to those under the CDR regime.



# Chapter 2:

## Privacy Safeguard 2 —

### Anonymity and pseudonymity

Version 3.0, June 2021

# Contents

<b>Key points</b>	<b>3</b>
<b>What does Privacy Safeguard 2 say?</b>	<b>3</b>
<b>Who does Privacy Safeguard 2 apply to?</b>	<b>3</b>
<b>How Privacy Safeguard 2 interacts with the Privacy Act</b>	<b>3</b>
<b>Why anonymity and pseudonymity are important</b>	<b>5</b>
<b>What is the difference between anonymity and pseudonymity?</b>	<b>5</b>
<b>Providing anonymous and pseudonymous options</b>	<b>5</b>
<b>Exceptions</b>	<b>6</b>
Requiring identification — required or authorised by law	6
Requiring identification — impracticability	7

## Key points

- An accredited person (who is or who may become an accredited data recipient of a consumer's CDR data) must provide a consumer with the option of dealing anonymously or pseudonymously with the entity in relation to that data, unless an exception applies.

## What does Privacy Safeguard 2 say?

- 2.1 Privacy Safeguard 2 provides that a consumer must have the option of not identifying themselves, or of using a pseudonym, when dealing with an accredited person (who is or who may become an accredited data recipient of the consumer's CDR data) in relation to that data.
- 2.2 'Anonymity' and 'pseudonymity' are different concepts. Privacy Safeguard 2 requires that both options be made available to consumers dealing with an accredited person unless an exception applies. The exceptions are set out in consumer data rule (CDR Rule) 7.3.
- 2.3 Consumer data rule (CDR Rule) 7.3 sets out that an accredited data recipient of a consumer's CDR data does not need to allow anonymity or pseudonymity where:<sup>1</sup>
  - 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 consumer in relation to particular CDR data.

## Who does Privacy Safeguard 2 apply to?

- 2.4 Privacy Safeguard 2 applies to accredited persons who are or who may become accredited data recipients of a consumer's CDR data.
- 2.5 It does not apply to data holders or designated gateways.
- 2.6 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 2 when dealing with individuals.

## How Privacy Safeguard 2 interacts with the Privacy Act

- 2.7 It is important to understand how Privacy Safeguard 2 interacts with the Privacy Act and the APPs.<sup>2</sup>

---

<sup>1</sup> The exceptions in CDR Rule 7.3 do not apply to an accredited person who is not yet an accredited data recipient of CDR data.

<sup>2</sup> The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies.

- 2.8 APP 2 requires entities to provide individuals with the option of not identifying themselves or of using a pseudonym.

CDR entity	Privacy protections that apply in the CDR context
<b>Accredited person who may become an accredited data recipient</b>	<p><b>Privacy Safeguard 2</b></p> <p>When an accredited person is dealing with a CDR consumer's data, and may become an accredited data recipient of that CDR data (for example, because they are seeking to collect it), Privacy Safeguard 2 applies.</p> <p>APP 2 does not apply to the accredited person in relation to dealings with the consumer regarding that CDR data.<sup>3</sup></p>
<b>Accredited data recipient<sup>4</sup></b>	<p><b>Privacy Safeguard 2</b></p> <p>An accredited data recipient of CDR data must comply with Privacy Safeguard 2 when dealing with the CDR consumer in relation to their CDR data. APP 2 does not apply to the accredited data recipient in relation to that CDR data.<sup>5</sup></p>
<b>Designated gateway</b>	<p><b>Australian Privacy Principle 2</b></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>
<b>Data holder</b>	<p><b>Australian Privacy Principle 2</b></p> <p>Privacy Safeguard 2 does not apply to a data holder.</p>

**Note:** Examples of dealings with consumers are set out in paragraph 2.14 below.

<sup>3</sup> See ss 56EC(4) and 56EE(1)(b) of the Competition and Consumer Act.

**Note:** If Privacy Safeguard 2 does not apply, APP 2 may continue to apply to other dealings with the individual's personal information where the accredited person is an APP entity (see s 56EC(4) and (5)(aa) of the Competition and Consumer Act). Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See s 6E(1D) of the Privacy Act.

<sup>4</sup> An accredited person becomes an accredited data recipient for CDR data when:

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

<sup>5</sup> The APPs do not apply to an accredited data recipient of the CDR data in relation to the CDR data (s 56EC(4) of the Competition and Consumer Act).

## Why anonymity and pseudonymity are important

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

## What is the difference between anonymity and pseudonymity?

- 2.11 Anonymity means that a consumer may deal with an accredited person (who is or who may become an accredited data recipient of the consumer's CDR data) in relation to that data without providing any personal information or identifiers. The accredited person should not be able to identify the consumer at the time of the dealing or subsequently. An example of an anonymous dealing is when a consumer has consented to the transfer of CDR data about their current service with no identifying information, to enquire generally about a service an accredited person can provide, and after receiving the consumer's CDR data, the accredited data recipient continues to deal with the consumer without any identifying information.
- 2.12 Pseudonymity means that a consumer may use a name, term or descriptor that is different to the consumer's actual name (e.g. an email address that does not contain the consumer's actual name). However, unlike anonymity, the use of a pseudonym does not necessarily mean that a consumer cannot be identified. The consumer may choose to divulge their identity, or to provide the CDR data necessary to identify them, such as an address.

## Providing anonymous and pseudonymous options

- 2.13 An accredited person (who is or who may become an accredited data recipient of the consumer's CDR data) must provide each consumer with the option of using a pseudonym, or not identifying themselves, when dealing with the accredited person in relation to that data.
- 2.14 Examples of 'dealings' include:
  - asking for the consumer's consent to collect, use and/or disclose their CDR data
  - providing a consumer with a consumer dashboard

- communicating with the consumer (for example, when providing a CDR receipt to the consumer<sup>6</sup> or notifying of collection under Privacy Safeguard 5)<sup>7</sup>
- using the consumer's CDR data to provide the requested goods or services to the consumer, and
- the consumer electing that their redundant data be deleted under CDR Rule 4.16.<sup>8</sup>

**Note:** Generally, in the banking sector, an accredited data recipient may not be able to deal with a consumer on an anonymous or pseudonymous basis. See paragraphs 2.15 to 2.22 following.

## Exceptions

### Requiring identification — required or authorised by law

- 2.15 CDR Rule 7.3(a) provides that an accredited data recipient is not required to offer a consumer the option of dealing anonymously or pseudonymously if the recipient 'is required or authorised by law or by a court/tribunal order to deal with an identified consumer in relation to particular CDR data'.<sup>9</sup>
- 2.16 The meaning of 'required or authorised by law or court/tribunal order' is discussed in [Chapter B \(Key concepts\)](#).
- 2.17 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.
- 2.18 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.<sup>10</sup>
- 2.19 The following are 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, or
  - opening a bank account for a consumer, or providing other financial services where legislation requires the consumer to be identified.

---

<sup>6</sup> See [Chapter C \(Consent\)](#).

<sup>7</sup> See [Chapter 5 \(Privacy Safeguard 5\)](#).

<sup>8</sup> See [Chapter C \(Consent\)](#).

<sup>9</sup> The exception in CDR Rule 7.3(a) does not apply to an accredited person who is not yet an accredited data recipient of CDR data.

<sup>10</sup> For further information, see [Chapter B \(Key concepts\)](#).

## Requiring identification — impracticability

- 2.20 CDR Rule 7.3(b) provides that a consumer may not have the option of dealing anonymously or pseudonymously with an accredited data recipient if it is impracticable to deal with a consumer who has not identified themselves.<sup>11</sup>
- 2.21 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.
- 2.22 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, or
  - changing internal systems or practices to include the option of anonymous or pseudonymous dealings, would be excessive in all the circumstances.

### **Anonymity and pseudonymity in the banking sector**

Generally, an accredited data recipient in the banking sector may not be able to deal with a consumer on an anonymous or pseudonymous basis.<sup>12</sup> This may be for a range of reasons, including because there may be obligations under law to verify the identity of the customer prior to providing goods or services.

Further, consumers should be aware that even where it is possible for a consumer to use a pseudonym, as CDR data in the banking sector is highly granular the consumer may remain identifiable.

<sup>11</sup> The exception in CDR Rule 7.3(b) does not apply to an accredited person who is not yet an accredited data recipient of CDR data.

<sup>12</sup> Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019, paragraph 1.322.

## Chapter 3:

# Privacy Safeguard 3 —

## Seeking to collect CDR data from CDR participants

Version 3.0, June 2021



# Contents

<b>Key points</b>	<b>3</b>
<b>What does Privacy Safeguard 3 say?</b>	<b>3</b>
<b>Why is it important?</b>	<b>4</b>
<b>Who does Privacy Safeguard 3 apply to?</b>	<b>4</b>
<b>How Privacy Safeguard 3 interacts with the Privacy Act</b>	<b>4</b>
<b>What is meant by ‘seeking to collect’ CDR data?</b>	<b>5</b>
<b>When can an accredited person seek to collect CDR data?</b>	<b>5</b>
What is a ‘valid request?’	5
Process for asking for consent	6
Consumer data request	7
Data minimisation principle	8
<b>Can an accredited person engage a third party to seek to collect CDR data on their behalf?</b>	<b>8</b>
<b>Interaction with other privacy safeguards</b>	<b>11</b>

## 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 (CDR Rules) set out what constitutes a valid request, including requirements and processes for seeking the consumer’s consent.
- The accredited person must also comply with all other requirements in the CDR Rules for collection of CDR data. This includes the ‘data minimisation principle’, which requires that an accredited person must not seek to collect data beyond what is reasonably needed to provide the good or service to which a consumer has consented, or for a longer time period than is reasonably needed.

## 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 consumer has requested the accredited person’s good or service and provided a valid request under the CDR Rules, and
  - the accredited person complies with all other requirements in the CDR Rules for the collection of CDR data from the CDR participant.<sup>1</sup>
- 3.2 Under the CDR Rules:
- the valid request must meet specific requirements, including compliance with the CDR Rules regarding consent,<sup>2</sup> and
  - accredited persons must have regard to the data minimisation principle,<sup>3</sup> which limits the scope of a consumer data request that an accredited person may make on behalf of a consumer.
- 3.3 The requirement in Privacy Safeguard 3 applies where an accredited person seeks to collect CDR data directly from a CDR participant, or via a designated gateway.<sup>4</sup> Privacy Safeguard 3 will also apply to an accredited person where they engage an accredited outsourced service provider to seek to collect CDR data on their behalf.<sup>5</sup>

---

<sup>1</sup> Section 56EF of the Competition and Consumer Act.

<sup>2</sup> CDR Rule 4.3.

<sup>3</sup> CDR Rule 4.12(2).

<sup>4</sup> Section 56EF(2) of the Competition and Consumer Act.

<sup>5</sup> The CDR Rules requirements for engaging an accredited outsourced service provider to collect data on an accredited person’s behalf are outlined in paragraphs 3.30 – 3.35.

## 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.
- 3.5 By adhering to Privacy Safeguard 3, an accredited person will ensure consumers have control over what CDR data is collected, and for what purposes and time-period. This will assist in enhancing consumer trust, as well as minimise the possibility of over-collection.

## Who does Privacy Safeguard 3 apply to?

- 3.6 Privacy Safeguard 3 applies to accredited persons.
- 3.7 Privacy Safeguard 3 does not apply to data holders and designated gateways. These entities must continue to ensure that they are adhering to their obligations under the *Privacy Act 1988* (the Privacy Act) and the Australian Privacy Principles (APPs), including APP 3 and APP 5, when collecting personal information.

## How Privacy Safeguard 3 interacts with the Privacy Act

- 3.8 It is important to understand how Privacy Safeguard 3 interacts with the Privacy Act and the APPs.<sup>6</sup>
- 3.9 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](#)).

CDR entity	Privacy protections that apply in the CDR context
<b>Accredited person</b>	<p><b>Privacy Safeguard 3</b></p> <p>When an accredited person is seeking to collect CDR data under the CDR Rules, Privacy Safeguard 3 applies.</p> <p>APP 3 does not apply to the accredited person in relation to that CDR data.<sup>7</sup></p>
<b>Designated gateway</b>	<p><b>APP 3</b></p> <p>Privacy Safeguard 3 does not apply to a designated gateway.</p>

<sup>6</sup> 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](#).

<sup>7</sup> See ss 56EC(4) and 56EF the Competition and Consumer Act.

**Note:** If Privacy Safeguard 3 does not apply, APP 3 may continue to apply to other collections of the individual's personal information where the accredited person is an APP entity (see s 56EC(4) and (5)(aa) of the Competition and Consumer Act). Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See s 6E(1D) of the Privacy Act.

CDR entity	Privacy protections that apply in the CDR context
<b>Data holder</b>	<b>APP 3</b> Privacy Safeguard 3 does not apply to a data holder.

## What is meant by ‘seeking to collect’ CDR data?

- 3.10 Privacy Safeguard 3 applies when an accredited person ‘seeks to collect CDR data’ (before the CDR data is actually collected).
- 3.11 ‘Seeking to collect’ CDR data refers to any act of soliciting CDR data, which includes explicitly requesting another entity to provide CDR data, or taking active steps to collect CDR data.
- 3.12 The main way in which an accredited person will ‘seek to collect’ CDR data under the CDR Rules is by making a ‘consumer data request’ to a CDR participant on behalf of the consumer. Consumer data requests are explained at paragraphs 3.22–3.26. The point at which an accredited person makes a consumer data request is demonstrated by the flow chart on page 10 of this Chapter.
- 3.13 The term ‘collect’ is discussed in detail in [Chapter B \(Key concepts\)](#). An accredited person ‘collects’ information if they collect the information for inclusion in a ‘record’ or a ‘generally available publication’.<sup>8</sup> ‘Record’<sup>9</sup> and ‘generally available publication’<sup>10</sup> have the same meaning as within the Privacy Act.

## 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 consumer, and the accredited person complies with all other requirements in the CDR Rules for the collection of CDR data.

## What is a ‘valid request?’

- 3.15 Under CDR Rule 4.3, a consumer gives an accredited person a ‘valid’ request to seek to collect their CDR data from a CDR participant if:

---

<sup>8</sup> Section 4(1) of the Competition and Consumer Act.

<sup>9</sup> Section 6(1) of the Privacy Act: ‘record’ includes a document or an electronic (or other) device. Some items are excluded from the definition, such as anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition, and Commonwealth records in the open access period.<sup>10</sup> Section 6(1) of the Privacy Act: ‘generally available publication’ means a ‘magazine, book, article, newspaper or other publication that is, or will be, generally available to members of the public’, regardless of the form in which it is published and whether it is available on payment of a fee.

<sup>10</sup> Section 6(1) of the Privacy Act: ‘generally available publication’ means a ‘magazine, book, article, newspaper or other publication that is, or will be, generally available to members of the public’, regardless of the form in which it is published and whether it is available on payment of a fee.

- the request is for the accredited person to provide goods or services
- the accredited person needs to collect the consumer's CDR data from a CDR participant and use it in order to provide the requested goods or services
- the accredited person asks the consumer for a collection consent and a use consent,<sup>11</sup> in accordance with Division 4.3 of the CDR Rules (see paragraphs 3.18–3.21 for further information), and
- the consumer expressly consents to this collection and use of their CDR data.

3.16 A request ceases to be 'valid' if the consumer withdraws their collection consent.<sup>12</sup>

3.17 Entities should also be mindful that the Competition and Consumer Act prohibits persons from engaging in conduct that misleads or deceives another person into believing certain matters, including that the person is making a valid request or has given their consent.<sup>13</sup>

## Process for asking for consent

3.18 Division 4.3 of the CDR Rules outlines the requirements for consent for the purposes of making a valid request for the collection and use of CDR data.

3.19 Specifically, the CDR Rules provide the following processes and requirements must be met to ensure that consent is voluntary, express, informed, specific as to purpose, time limited, and easily withdrawn:

- **Processes for asking for consent** (CDR Rule 4.10): to ensure that the consent is as easy to understand as practicable.
- **Requirements when asking for consent** (CDR Rules 4.11, 4.16 and 4.17): including to allow the consumer to actively select the types and uses of data to which they provide consent, and provide express consent for the accredited person to collect and use the selected data for those specified purposes. Additional requirements apply where the accredited person is seeking consent to de-identify CDR data (CDR Rule 4.15).
- **Restrictions on seeking consent** (CDR 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** (CDR Rule 4.13): including that a consumer may withdraw the consent at any time through their consumer dashboard or by using a simple alternative method made available by the accredited person.

---

<sup>11</sup> The consumer must provide a collection consent for the accredited person to collect their data from a CDR participant and a use consent for the accredited person to use that CDR data. See [Chapter C \(Consent\)](#) for further information.

<sup>12</sup> CDR Rule 4.3(4). If the consumer does not also withdraw their use consent, the accredited person may continue to use the CDR data it has already collected to provide the requested goods or services. See the note under CDR Rule 4.3(4). See further Rule 4.18A for ongoing notification requirements in this circumstance.

If the consumer also withdraws their use consent, the CDR data is likely to become redundant data that the accredited person is required to delete or de-identify in accordance with Privacy Safeguard 12 (unless an exception applies). More information on 'redundant data' and the requirement to destroy or de-identify redundant data is in [Chapter 12 \(Privacy Safeguard 12\)](#).

<sup>13</sup> Sections 56BN and 56BO of the Competition and Consumer Act.

- Time of **expiry of consent** (CDR 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).
- 3.20 The accredited person is also required to have regard to the Consumer Experience Guidelines<sup>14</sup> when asking a consumer to give consent.
- 3.21 These specific requirements and processes for the above CDR Rule requirements are explained in [Chapter C \(Consent\)](#).

## Consumer data request

- 3.22 If a consumer has given an accredited person a valid request (see paragraph 3.15 above), and the consumer's consent for the accredited person to collect and use their CDR data is current,<sup>15</sup> the accredited person may request the relevant CDR participant to disclose some or all of the CDR data that:
- is the subject of the relevant collection consent and use consent, and
  - it is able to collect and use in compliance with the data minimisation principle.<sup>16</sup>
- 3.23 In doing so, the accredited person makes a 'consumer data request' to a CDR participant on behalf of the consumer.<sup>17</sup> The accredited person may make consumer data requests to more than one CDR participant where the relevant CDR data required to provide the requested goods or services is held by different CDR participants. The accredited person may also need to make repeated consumer data requests over a period of time in order to provide the requested goods or services.
- 3.24 When the accredited person makes a consumer data request on behalf of a consumer, they must not seek to collect more CDR data than is reasonably needed, or for a longer time period than reasonably needed, in order to provide the requested goods or services.<sup>18</sup>
- 3.25 When an accredited person makes a consumer data request to a data holder, they must make the request:
- using the data holder's accredited person request service, and
  - in accordance with the data standards.<sup>19</sup>
- 3.26 An accredited person complies with Privacy Safeguard 3 after giving the relevant CDR participant/s a consumer data request in the manner set out above at paragraph 3.25.<sup>20</sup>

---

<sup>14</sup> CDR Rule 4.10(1)(a)(ii). The Consumer Experience Guidelines provide best practice interpretations of the CDR Rules relating to consent and are discussed [in Chapter B \(Key concepts\)](#).

<sup>15</sup> See paragraph 3.15 above.

<sup>16</sup> CDR Rules 4.4(1) and 4.7A(1).

<sup>17</sup> CDR Rules 4.4(2) and 4.7A(2).

<sup>18</sup> CDR Rules 1.8(a), 4.4(1)(d) and 4.7A(1)(d).

<sup>19</sup> CDR Rule 4.4(3).

<sup>20</sup> The effect of CDR Rules 4.4(2) and 4.7A(2) is that a request for CDR data from an accredited person on behalf of a consumer that does not comply with CDR Rule 4.4(1) or CDR Rule 4.7A(1) is not a 'consumer data request'.

## Data minimisation principle

- 3.27 Collection of CDR data is limited by the data minimisation principle,<sup>21</sup> which requires that an accredited person:
- must not collect more data than is reasonably needed in order to provide the requested goods or services or for a time period longer than what is reasonably needed, and
  - may only use the collected data consistently with the consent provided, and only as reasonably needed in order to provide the requested goods or services or to fulfill any other purpose as consented to by the consumer.
- 3.28 The data minimisation principle is relevant both when an accredited person seeks consent from the consumer to collect their CDR data, and then when the accredited person gives a CDR participant a consumer data request.
- 3.29 The data minimisation principle is discussed further in [Chapter B \(Key concepts\)](#).

### Example

MiddleMan Ltd, an accredited person, makes a consumer data request on behalf of a consumer, Athena, to seek information about Athena's eligibility to open a bank account.

MiddleMan has asked Athena for her consent to collect information about her transaction history from the data holder (in addition to other data), when this information would not be required to determine her eligibility for the service.

MiddleMan will likely be in breach of Privacy Safeguard 3 as it has sought to collect CDR data beyond what is reasonably needed to provide the requested service (as required by the data minimisation principle) and therefore has not sought to collect Athena's CDR data from a CDR participant in accordance with the CDR Rules.

## Can an accredited person engage a third party to seek to collect CDR data on their behalf?

- 3.30 An accredited person may engage another accredited person to seek to collect CDR data on their behalf, in accordance with the CDR Rules.<sup>22</sup> This is currently the only type of third party that can be engaged for this purpose under the CDR Rules.
- 3.31 CDR Rule 1.10 requires the accredited person (the 'principal') to have a CDR outsourcing arrangement with the other accredited person (the 'outsourced service provider', or

---

<sup>21</sup> CDR Rule 4.12(2). There are no equivalent requirements for how an accredited person makes a consumer data request to an accredited data recipient.

<sup>22</sup> CDR Rule 1.10(2)(a)(i).

‘provider’). A CDR outsourcing arrangement is a written contract between the principal and provider which meets the requirements set out in CDR Rule 1.10(2).<sup>23</sup>

- 3.32 Where an accredited person intends to use an accredited provider to seek to collect a consumer’s CDR data, the accredited person must:
- provide certain information to the consumer at the time of seeking the consumer’s consent to collect and use the consumer’s CDR data,<sup>24</sup> and
  - include certain information about outsourced service providers in its CDR policy.<sup>25</sup>
- 3.33 The accredited person must ensure the accredited provider complies with its requirements under the CDR outsourcing arrangement.<sup>26</sup>
- 3.34 The CDR data collected by an accredited provider in accordance with the CDR outsourcing arrangement, including any data directly or indirectly derived from such CDR data, is known as ‘service data’ in relation to that arrangement.<sup>27</sup>
- 3.35 Any use or disclosure of such service data by the accredited provider will be taken to have been by the accredited person. This occurs regardless of whether the use or disclosure is in accordance with the CDR outsourcing arrangement.<sup>28</sup>

**Risk point:** Entities that fail to take prudent and robust measures in their CDR outsourcing arrangements risk non-compliance by their third parties.

**Privacy tip:** To ensure the third party complies with the outsourcing arrangement, the accredited person should ensure that:

- the relevant CDR outsourcing arrangement requires the third party to adhere to the accredited person’s privacy safeguard obligations, and
- the contract provides an appropriate level of transparency to allow them to monitor the third party where relevant, and audit the CDR outsourcing arrangement.

---

<sup>23</sup> ‘CDR outsourcing arrangement’ is discussed in [Chapter B \(Key Concepts\)](#).

<sup>24</sup> CDR Rule 4.11(3)(f). [See Chapter 3 \(Privacy Safeguard 3\)](#).

<sup>25</sup> CDR Rule 7.2(4). [See Chapter 1 \(Privacy Safeguard 1\)](#).

<sup>26</sup> CDR Rule 1.16(1). The requirements for a CDR outsourcing arrangement are set out in CDR Rule 1.10(2).

<sup>27</sup> CDR Rule 1.10(4).

<sup>28</sup> CDR Rule 7.6(2).



## Consent and collection process for accredited persons

### Obtaining consumer consent for the collection and use of CDR data

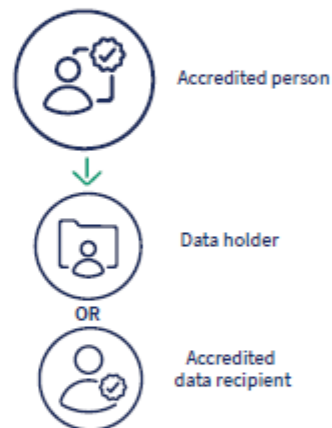
- Accredited person offers a good or service which requires CDR data
- Consumer wishes to be provided the good or service
- Accredited person asks the consumer to consent to the collection and use of their CDR data for this purpose, for up to 12 months
- Consumer provides their express consent to the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



The consumer has given the accredited person a valid request ✓

### Making a consumer data request on behalf of the consumer

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



CDR participant sends the consumer's CDR data to the accredited person after obtaining:

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



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

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

[2] Note: there are no equivalent requirements for how an accredited person must make a request to another accredited data recipient

# Interaction with other privacy safeguards

## Privacy Safeguard 4

- 3.36 The privacy safeguards distinguish between an accredited person collecting solicited CDR data ([Privacy Safeguard 3](#)) and unsolicited CDR data ([Privacy Safeguard 4](#)).
- 3.37 Privacy Safeguard 4 requires an accredited person to destroy unsolicited CDR data collected from a data holder, unless an exception applies ([see Chapter 4 \(Privacy Safeguard 4\)](#)).
- 3.38 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

- 3.39 Privacy Safeguard 5 requires an accredited data recipient who collected data in accordance with Privacy Safeguard 3 to notify the consumer of the collection in accordance with the CDR Rules ([see Chapter 5 \(Privacy Safeguard 5\)](#)).

## Chapter 4:

# Privacy Safeguard 4 —

## Dealing with unsolicited CDR data from CDR participants

Version 3.0, June 2021

# Contents

<b>Key points</b>	<b>3</b>
<b>What does Privacy Safeguard 4 say?</b>	<b>3</b>
<b>Why is it important?</b>	<b>3</b>
<b>Who does Privacy Safeguard 4 apply to?</b>	<b>3</b>
<b>How Privacy Safeguard 4 interacts with the Privacy Act</b>	<b>4</b>
<b>Unsolicited CDR data</b>	<b>4</b>
<b>In what circumstances does Privacy Safeguard 4 apply?</b>	<b>5</b>
Meaning of ‘purportedly under the CDR Rules’	5
Meaning of ‘not as the result of seeking to collect that data under the CDR Rules’	5
<b>What is the obligation to destroy unsolicited data?</b>	<b>6</b>
‘Destroy’	6
As soon as practicable	6
Not required to retain the data	7
<b>How does Privacy Safeguard 4 interact with the other privacy safeguards?</b>	<b>7</b>

## Key points

- Privacy Safeguard 4 requires an accredited person to destroy unsolicited consumer data right (CDR) data that the entity collects and 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 data holder or accredited data recipient ('CDR participant'), purportedly under the consumer data rules (CDR Rules), where the accredited person has not sought to collect that particular data and is not required to retain it by or under an Australian law or court/tribunal order.<sup>1</sup>
- 4.3 This obligation applies regardless of whether the accredited person collects the CDR data directly from a CDR participant or indirectly through a designated gateway.<sup>2</sup>

## Why is it important?

- 4.4 The objective of Privacy Safeguard 4 is to ensure that CDR data collected by an accredited person is afforded appropriate privacy protection, even where the accredited person has not solicited the CDR data.
- 4.5 Privacy Safeguard 4 requires accredited persons to destroy CDR data they have collected but not requested, unless an exception applies. This destruction requirement strengthens the protections for consumers under the CDR 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 1988* (Privacy Act) and Australian Privacy Principle (APP) 4 when dealing with unsolicited personal information.

---

<sup>1</sup> Section 56EG(1) of the Competition and Consumer Act.

<sup>2</sup> Section 56EG(2) of the Competition and Consumer Act.

# How Privacy Safeguard 4 interacts with the Privacy Act

- 4.8 It is important to understand how Privacy Safeguard 4 interacts with the Privacy Act and APPs.<sup>3</sup>
- 4.9 APP 4 applies to unsolicited personal information. APP 4 requires an APP entity to destroy or de-identify unsolicited personal information it receives if the entity determines that it could not have collected the information under APP 3.<sup>4</sup>

CDR Entity	Privacy protections that apply in the CDR context
<b>Accredited person</b>	<p><b>Privacy Safeguard 4</b></p> <p>When an accredited person collects unsolicited CDR data purportedly under the CDR Rules, Privacy Safeguard 4 applies.</p> <p>APP 4 does not apply to the accredited person in relation to that CDR data.<sup>5</sup></p>
<b>Designated gateway</b>	<p><b>APP 4</b></p> <p>Privacy Safeguard 4 does not apply to a designated gateway.</p>
<b>Data holder</b>	<p><b>APP 4</b></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 CDR Rules.
- 4.11 An example of how an accredited person might collect such ‘unsolicited’ CDR data is where:
- the accredited person makes a consumer data request on a consumer’s behalf to collect CDR data from a data holder, in accordance with Privacy Safeguard 3 and CDR Rule 4.4
  - the data holder has or receives authorisation from the consumer, and

<sup>3</sup> 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](#).

<sup>4</sup> See [Chapter 3: APP 3 – Collection of solicited personal information of the APP Guidelines](#).

<sup>5</sup> See ss 56EC(4) and 56EG the Competition and Consumer Act.

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

- 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).<sup>6</sup>

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

## In what circumstances does Privacy Safeguard 4 apply?

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

- purportedly under the CDR Rules, but
- not as the result of seeking to collect that CDR data under the CDR Rules.<sup>7</sup>

### Meaning of 'purportedly under the CDR Rules'

4.14 Privacy Safeguard 4 applies to CDR data collected 'purportedly under the CDR Rules'<sup>8</sup>

4.15 'Purportedly' in this context means that the mechanisms of the CDR rules appear to have been used but this did not validly occur because the accredited person did not, in fact, seek to collect the CDR data.

### Meaning of 'not as the result of seeking to collect that data under the CDR Rules'

4.16 Privacy Safeguard 4 applies to CDR data that is collected other than as a result of the accredited person seeking to collect it under the CDR Rules.<sup>9</sup>

4.17 In practice, Privacy Safeguard 4 will typically apply to CDR data received by the accredited person that is outside the scope of the accredited person's consumer data request to the CDR participant.

---

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

<sup>7</sup> Section 56EG(1)(a) of the Competition and Consumer Act.

<sup>8</sup> Section 56EG(1)(a)(i) of the Competition and Consumer Act.

<sup>9</sup> Section 56EG(1)(a)(ii) of the Competition and Consumer Act.

**Example**

Friedrich makes a valid request for Green Bank (an accredited person) to collect his CDR data. Green Bank then seeks to collect Friedrich's CDR data from Yellow Bank, a data holder for Friedrich's CDR data, through a consumer data request in accordance with the CDR Rules.

Yellow Bank mistakenly discloses Salome's CDR data to Green Bank, rather than Friedrich's data. A Green Bank employee realises the error and immediately arranges for the collected data to be destroyed, in compliance with Privacy Safeguard 4. The next day, Yellow Bank discloses Friedrich's CDR data pursuant to the consumer data request. Unfortunately, Yellow Bank also discloses data outside the scope of the request.

Green Bank soon realises that additional CDR data outside the scope of the request has been disclosed to it, which it is not required to retain. However, Green Bank does not take any steps to destroy the additional data. Green Bank has likely breached Privacy Safeguard 4.

## What is the obligation to destroy unsolicited data?

### 'Destroy'

- 4.18 Privacy Safeguard 4 requires unsolicited CDR data to be 'destroyed'. Destruction of CDR data should follow the CDR data deletion process discussed in detail in Chapter 12 ([Privacy Safeguard 12](#)).

### As soon as practicable

- 4.19 Privacy Safeguard 4 requires unsolicited CDR data to be destroyed 'as soon as practicable'.
- 4.20 The test of practicability is an objective test. It is the responsibility of the accredited person to be able to justify that it is not practicable to destroy unsolicited data promptly after its collection.
- 4.21 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.
- 4.22 In adopting a timetable that is 'practicable' an accredited person can take technical and resource considerations into account. However, it is the responsibility of the accredited person to justify any delay in destroying unsolicited CDR data.
- 4.23 The timeframe in which an accredited person must destroy unsolicited CDR data begins at the time the entity becomes aware that the data was not solicited. How quickly an accredited person becomes aware of unsolicited CDR data may depend on its available technical and other resources.



## Not required to retain the data

- 4.24 The obligation to destroy unsolicited data does not apply to CDR data that an accredited person is required to retain by or under an Australian law or court/tribunal order.<sup>10</sup>
- 4.25 The concept ‘required by or under another Australian law or court/tribunal order’ is discussed in Chapter B (Key concepts).

## How does Privacy Safeguard 4 interact with the other privacy safeguards?

- 4.26 Privacy Safeguard 3 prohibits an accredited person from seeking to collect CDR data from a CDR participant unless in response to a valid request from a consumer, and in compliance with the CDR Rules ([see Chapter 3 \(Privacy Safeguard 3\)](#)).
- 4.27 Privacy Safeguard 12 requires an accredited data recipient to destroy or de-identify redundant data unless the entity is required by or under an Australian law or court/tribunal 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 \(Privacy Safeguard 12\)](#)).
- 4.28 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).

---

<sup>10</sup> Section 56EG(1)(b) of the Competition and Consumer Act.

# Chapter 5:

## Privacy Safeguard 5 —

### Notifying of the collection of CDR data

Version 3.0, June 2021

# Contents

<b>Key points</b>	<b>3</b>
<b>What does Privacy Safeguard 5 say?</b>	<b>3</b>
<b>Why is this important?</b>	<b>3</b>
<b>Who does Privacy Safeguard 5 apply to?</b>	<b>3</b>
<b>How Privacy Safeguard 5 interacts with the Privacy Act</b>	<b>4</b>
<b>How must notification be given?</b>	<b>5</b>
<b>Who must be notified?</b>	<b>5</b>
<b>When must notification be given?</b>	<b>5</b>
<b>What matters must be included in the notification?</b>	<b>6</b>
What CDR data was collected	7
When the CDR data was collected	7
From whom the CDR data was collected	8
<b>Other notification requirements under the CDR Rules</b>	<b>8</b>
<b>How does Privacy Safeguard 5 interact with the other privacy safeguards?</b>	<b>9</b>

## Key points

- An accredited data recipient of a consumer's CDR data must notify that consumer when they collect the data.
- This notification must occur through the consumer's dashboard as soon as practicable after the accredited data recipient has received the consumer's CDR data.

## What does Privacy Safeguard 5 say?

- 5.1 If an accredited data recipient collected a consumer's CDR data under Privacy Safeguard 3, the accredited data recipient must notify that consumer of the collection by taking the steps identified in the consumer data rules (CDR Rules).<sup>1</sup>
- 5.2 The notification must:
  - be given to the consumer at whose request the CDR data was collected
  - cover the matters set out in the CDR Rules, and
  - be given at or before the time specified in the CDR Rules.
- 5.3 Under CDR Rule 7.4, an accredited data recipient of a consumer's CDR data must notify the consumer by updating the consumer's dashboard to include certain matters as soon as practicable after CDR data is collected from a data holder or accredited data recipient.
- 5.4 For information about the concept of 'collects' refer to [Chapter B \(Key concepts\)](#). For information about seeking to collect CDR data under Privacy Safeguard 3, see [Chapter 3 \(Privacy Safeguard 3\)](#).

## Why is this important?

- 5.5 Notification of collection of CDR data is an integral element of the CDR 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 accredited data recipients.

## Who does Privacy Safeguard 5 apply to?

- 5.7 Privacy Safeguard 5 applies to accredited data recipients of a consumer's CDR data. It does not apply to data holders or designated gateways.
- 5.8 Data holders and designated gateways must ensure that they are adhering to their obligations under the *Privacy Act 1988* (the Privacy Act) and the Australian Privacy Principles (APPs), including APP 3 and APP 5, when collecting personal information.

---

<sup>1</sup> Section 56EH of the Competition and Consumer Act.

- 5.9 Data holders must also ensure they adhere to Privacy Safeguard 10, which requires them to notify consumers of the disclosure of their CDR data.

## How Privacy Safeguard 5 interacts with the Privacy Act

- 5.10 It is important to understand how Privacy Safeguard 5 interacts with the Privacy Act and the APPs.<sup>2</sup>
- 5.11 Like Privacy Safeguard 5, APP 5 outlines when an entity must notify of collection, as well as what information must be included in the notification.
- 5.12 The Privacy Act and APP 5 provide protection where collected data is personal information, but not CDR data.

CDR entity	Privacy protections that apply in the CDR context
<b>Accredited data recipient</b>	<p><b>Privacy Safeguard 5</b></p> <p>For accredited data recipients of a consumer's CDR data, the Privacy Safeguard 5 notification requirements apply to any of that consumer's CDR data that been collected in accordance with Privacy Safeguard 3.<sup>3</sup></p> <p>APP 5 does not apply in relation to that CDR data.<sup>4</sup></p>
<b>Designated gateway</b>	<p><b>APP 5</b></p> <p>Privacy Safeguard 5 does not apply to a designated gateway.</p>
<b>Data holder</b>	<p><b>APP 5</b></p> <p>Privacy Safeguard 5 does not apply to a data holder.</p>

<sup>2</sup> The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies.

<sup>3</sup> Privacy Safeguard 5 applies from the point when the accredited person becomes an accredited data recipient of the CDR data. An accredited person becomes an accredited data recipient for CDR data when:

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

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

## How must notification be given?

- 5.13 An accredited data recipient must provide the notification by updating the consumer dashboard for a consumer to include the matters discussed in paragraphs 5.24 to 5.35 as soon as practicable after collecting CDR data relating to that consumer.<sup>5</sup>
- 5.14 The consumer dashboard is an online service that must be provided by an accredited person to each consumer who has provided consent to the collection, use and/or disclosure of their CDR data. Accredited persons are required by CDR Rule 1.14 to include within the consumer's dashboard certain details of each consent to collect, use and disclose CDR data that has been given by the consumer.<sup>6</sup>
- 5.15 Where an accredited data recipient collected CDR data on behalf of another accredited person (the 'principal') under a CDR outsourcing arrangement, only the principal needs to notify the relevant consumer/s of collection by updating the relevant dashboard/s.<sup>7</sup>
- 5.16 Further guidance about the consumer dashboard is set out in [Chapter B \(Key concepts\)](#) and [Chapter C \(Consent\)](#).

## Who must be notified?

- 5.17 The accredited data recipient must notify the consumer who gave the consent to collect the CDR data.
- 5.18 There may be more than one 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 data recipient is required by CDR Rule 7.4 to update only the consumer dashboard of the requesting joint account holder.

## When must notification be given?

- 5.19 An accredited data recipient must notify the consumer as soon as practicable after the CDR data is collected.
- 5.20 As a matter of best practice, notification should generally occur in as close to real time as possible (for example, in relation to ongoing collection, as close to the time of first collection as possible).
- 5.21 The test of practicability is an objective test. It is the responsibility of the accredited data recipient to be able to justify any delay in notification.
- 5.22 In determining what is 'as soon as practicable', the accredited data recipient may take the following factors into account:
  - time and cost involved, when combined with other factors

---

<sup>5</sup> CDR Rule 7.4.

<sup>6</sup> This includes the CDR data to which the consents relate and when the consents will expire. For further information regarding the requirements for an accredited person's consumer dashboard, see CDR Rule 1.14, [Chapter C \(Consent\)](#) and [Chapter B \(Key concepts\)](#).

<sup>7</sup> CDR Rule 1.16(2)(a). For information on 'CDR outsourcing arrangements', see [Chapter B \(Key concepts\)](#).

- technical matters, and
- any individual needs of the consumer (for example, additional steps required to make the content accessible).

5.23 An accredited data recipient is not excused from providing prompt notification by reason only that it would be inconvenient, time consuming or costly to do so.

**Risk point:** Delays in notification of collection may result in confusion for a consumer, and non-compliance for an accredited data recipient.

**Privacy tip:** Accredited data recipients should ensure that they have systems and processes in place to allow for real-time and automated notification.

## What matters must be included in the notification?

5.24 The minimum matters that must be included in the notification, and provided via the consumer's dashboard, are:

- what CDR data was collected
- when the CDR data was collected, and
- the data holder or accredited data recipient from which the CDR data was collected.<sup>8</sup>

5.25 Accredited data recipients should provide information about these matters clearly and simply, but also with enough specificity to be meaningful for the consumer. How much information is required may differ depending on the circumstances.

5.26 Guidance on each of the minimum matters is provided below.

**Risk point:** Consumers may not read or understand a notification where the details of collection are complex.

**Privacy tip:** An accredited data recipient should ensure that the notification is as simple and easy to understand as possible. To do this, an accredited data recipient should consider a range of factors when formulating a notification, such as:

- what the data is being used for
- the language used (including the level of detail), and
- the presentation of the information (e.g. layout, format and any visual aids used). For more complex notifications, the accredited data recipient could consider providing a condensed summary of key matters in the notification and linking to more comprehensive information or, where it may assist the consumer, a full log of access.

---

<sup>8</sup> CDR Rule 7.4.

## What CDR data was collected

- 5.27 The accredited data recipient must notify the consumer of what CDR data was collected.
- 5.28 In doing so, the accredited data recipient should ensure CDR data is described in a manner that allows the consumer to easily understand what CDR data was collected.
- 5.29 The accredited data recipient must use the Data Language Standards when describing what CDR data was collected.<sup>9</sup> This will aid consumer comprehension by ensuring consistency between how CDR data was described in the consent-seeking process and how CDR data is described in the consumer dashboard.

## When the CDR data was collected

- 5.30 The accredited data recipient must notify the consumer of when the CDR data was collected.

### *'One-off' collection<sup>10</sup>*

- 5.31 The accredited data recipient should include the date on which the CDR data was collected.

### *Ongoing collection<sup>11</sup>*

- 5.32 The accredited data recipient should, at a minimum, include the date range in which CDR data will be collected, with the starting date being the date on which the CDR data was first collected, and the end date being the date on which the accredited person will make its final collection. This end date might not necessarily be the same as the date the consent to collect expires.
- 5.33 Where an accredited data recipient is unsure of the end date they may put the date the consent to collect expires, but must update the end date as soon as practicable after it becomes known.<sup>12</sup>
- 5.34 The accredited data recipient should, in addition to stating the date range for collection, note:
- what activity will trigger ongoing collection (e.g. 'We'll continue to collect your transaction details from [e.g. data holder] each time you make a transaction'), and / or
  - if known, the frequency of any ongoing collection (e.g. 'We'll continue to collect your transaction details from [e.g. data holder] up to three times per day').

---

<sup>9</sup> The Data Language Standards are contained within the Consumer Experience Standards. They provide descriptions of the types of data to be used by accredited data recipients when making and responding to requests. Adherence to the Data Language Standards is mandatory and will help ensure there is a consistent interpretation and description of the consumer data that will be shared in the CDR regime. See s 56FA of the Competition and Consumer Act and CDR Rule 8.11.

<sup>10</sup> This is where the accredited person indicated the CDR data would be collected on a single occasion (CDR Rule 4.11(1)(b)(i)).

<sup>11</sup> This is where the accredited person indicated the CDR data would be collected over a specified period of time (CDR Rule 4.11(1)(b)(ii)).

<sup>12</sup> CDR 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.



## From whom the CDR data was collected

- 5.35 In its notification to the consumer, the accredited data recipient must indicate from whom the CDR data was collected. There may be multiple data holders and/or accredited data recipients from whom the CDR data was collected.

### Example

Watson and Co is an accredited person that provides a budgeting service through its Watspend application. Watspend uses transaction details to provide real-time, accurate budgeting recommendations to its users.

Zoe wants to use the Watspend application, so provides Watson and Co with a valid request to collect her transaction details from Bank Belle. Zoe provides consent for Watson and Co to collect and use her transaction details for the provision of the Watspend service from 1 July 2020 to 1 January 2021.

Watson and Co collect Zoe's transaction details from Bank Belle on 1 July 2020 and becomes an accredited data recipient for this CDR data.

Watson and Co updates Zoe's consumer dashboard on 1 July 2020 to include the following notification statement:

*We collected your transaction details from Bank Belle on 01.07.20. We'll continue to collect your transaction details from Bank Belle each time you make a transaction until 01.01.21.*

The above statement is an example of how Watson and Co could notify Zoe of the collection of her CDR data in accordance with CDR Rule 7.4.

## Other notification requirements under the CDR Rules

- 5.36 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:<sup>13</sup>
- providing CDR receipts to the consumer (CDR Rule 4.18)
  - notification requirements where certain consents expire or are amended (CDR Rules 4.18A, 4.18B and 4.18C)

---

<sup>13</sup> For an accredited data recipient who collected CDR data on behalf of a principal in a CDR outsourcing arrangement, note the effect of CDR Rule 1.7(5) which provides that, in the CDR Rules, 'unless the contrary intention appears, a reference to an accredited person making a consumer data request, collecting CDR data, obtaining consents, providing a consumer dashboard, or using or disclosing CDR data does not include a reference to an accredited person doing those things on behalf of a principal in its capacity as the provider in an outsourced service arrangement, in accordance with the arrangement'.

For information on 'CDR outsourcing arrangements', see [Chapter B \(Key concepts\)](#), 'Outsourced service provider'.

- general obligation to update the consumer dashboard (CDR Rule 4.19), and
- ongoing notification requirements for consents to collect and use (CDR Rule 4.20).

5.37 For further information regarding these notification requirements, see [Chapter C \(Consent\)](#).

## How does Privacy Safeguard 5 interact with the other privacy safeguards?

- 5.38 The requirement in Privacy Safeguard 5 to notify consumers about the collection of their CDR data relates to all CDR data collected under Privacy Safeguard 3 (see [Chapter 3 \(Privacy Safeguard 3\)](#)).
- 5.39 While Privacy Safeguard 5 relates to notification on *collection*, Privacy Safeguard 10 sets out when an accredited data recipient and data holder must notify consumers about the *disclosure* of their CDR data. See [Chapter 10 \(Privacy Safeguard 10\)](#).

## Chapter 6:

# Privacy Safeguard 6 —

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

Version 3.0, June 2021

# Contents

<b>Key points</b>	<b>3</b>
<b>What does Privacy Safeguard 6 say?</b>	<b>3</b>
Accredited data recipients	3
Designated gateways	3
<b>Who does Privacy Safeguard 6 apply to?</b>	<b>3</b>
<b>How Privacy Safeguard 6 interacts with the Privacy Act</b>	<b>4</b>
<b>Why is it important?</b>	<b>5</b>
<b>What is meant by ‘use’ and ‘disclose’?</b>	<b>5</b>
‘Use’	5
‘Disclose’	5
<b>When can an accredited data recipient use or disclose CDR data?</b>	<b>6</b>
Use or disclosure required or authorised under the CDR Rules	8
Use or disclosure under Australian law or a court/tribunal order	15
<b>Interaction with other Privacy Safeguards</b>	<b>15</b>

## Key points

- Privacy Safeguard 6, together with consumer data rules (CDR Rules) 7.5, 7.5A, 7.6 and 7.7, applies to accredited data recipients of a consumer's CDR data, placing restrictions and obligations on them in relation to the use and disclosure of that data.
- Generally, accredited data recipients of CDR data and designated gateways can use or disclose CDR data only where required or authorised under the CDR Rules. The consumer must consent to these uses and disclosures of their CDR data.
- CDR Rule 7.5(1) outlines the permitted uses and disclosures of CDR data.
- In addition, CDR Rules 7.5(2), 7.5A and 7.6(1) prohibit certain uses or disclosures of CDR data.
- Accredited data recipients of CDR data must comply with the data minimisation principle when using that data to provide the goods or services requested by the consumer, or to fulfil any other purpose consented to by the consumer.

## What does Privacy Safeguard 6 say?

### Accredited data recipients

- 6.1 An accredited data recipient of a consumer's CDR data must not use or disclose that data unless the:
- disclosure is required under the CDR Rules in response to a valid request from a consumer for the CDR data
  - use or disclosure is otherwise required or authorised under the CDR Rules, or
  - use or disclosure is required or authorised by or under another Australian law or a court/tribunal order, and the accredited data recipient makes a written note of the use or disclosure.
- 6.2 To be compliant with Privacy Safeguard 6, an accredited data recipient of CDR data must satisfy the requirements under CDR Rule 7.5.

### Designated gateways

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

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.<sup>1</sup>

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

## How Privacy Safeguard 6 interacts with the Privacy Act

6.6 It is important to understand how Privacy Safeguard 6 interacts with the Privacy Act and the APPs.<sup>2</sup>

6.7 APP 6 relates to the use or disclosure of personal information.<sup>3</sup>

CDR entity	Privacy protections that apply in the CDR context
<b>Accredited data recipient</b>	<p><b>Privacy Safeguard 6</b></p> <p>For accredited data recipients of a consumer's CDR data, Privacy Safeguard 6 applies to the use or disclosure of that data.<sup>4</sup></p> <p>APP 6 does not apply in relation to that CDR data.<sup>5</sup></p>
<b>Designated gateway</b>	<p><b>Privacy Safeguard 6</b></p> <p>For designated gateways for CDR data, Privacy Safeguard 6 applies to the use and disclosure of the CDR data.<sup>6</sup></p>

<sup>1</sup> For the purposes of APP 6.2(b), the Competition and Consumer Act is an Australian law that may require or authorise a data holder to disclose personal information.

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

<sup>3</sup> 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](#) of the APP Guidelines.

<sup>4</sup> Privacy Safeguard 6 applies from the point when the accredited person becomes an accredited data recipient of the CDR data. An accredited person becomes an accredited data recipient for CDR data when:

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

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

<sup>6</sup> Section 56EI(2) of the Competition and Consumer Act.

APP 6 does not apply in relation to that CDR data.<sup>7</sup>

---

**Data holder**

**APP 6**

Privacy Safeguard 6 does not apply to a data holder.

---

## Why is it important?

- 6.8 Consumer consent for the use and disclosure of their CDR data 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 disclosed 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.<sup>8</sup>
- 6.11 An accredited data recipient or designated gateway ‘uses’ CDR data where it handles or undertakes an activity with the CDR data within its effective control. For further discussion of use, see [Chapter B \(Key concepts\)](#). For example, ‘use’ includes:
- the entity accessing and reading the CDR data
  - the entity making a decision based on the CDR data
  - the entity de-identifying the CDR data, and
  - the entity passing the CDR data from one part of the entity to another.

### ‘Disclose’

- 6.12 The term ‘disclose’ is not defined within the Consumer and Competition Act.<sup>9</sup>
- 6.13 An accredited data recipient or designated gateway ‘discloses’ CDR data when it makes it accessible or visible to others outside the entity.<sup>10</sup> This focuses on the act done by the disclosing party, and not on the actions or knowledge of the recipient. There will be a disclosure in these circumstances even where the information is already known to the recipient. For further discussion of disclosure, see [Chapter B \(Key concepts\)](#).

---

<sup>7</sup> The APPs do not apply to designated gateways for CDR data in relation to that CDR data - s 56EC(4)(d) of the Competition and Consumer Act. However, s 56EC(4) does not affect how the APPs apply to designated gateways who are APP entities, in relation to the handling of personal information outside the CDR system. See s 56EC(5)(b) of the Competition and Consumer Act.

<sup>8</sup> The term ‘use’ is also not defined in the Privacy Act.

<sup>9</sup> The term ‘disclose’ is also not defined in the Privacy Act.

<sup>10</sup> Information will be ‘disclosed’ under the CDR regime regardless of whether an entity retains effective control over the data.

- 6.14 Examples of disclosure include where an accredited data recipient or designated gateway:
- shares the CDR data with another entity or individual, including a related party of the entity (subject to some exceptions, as outlined in paragraph 6.15 below)
  - publishes the CDR data on the internet, whether intentionally or not
  - accidentally provides CDR data to an unintended recipient
  - reveals the CDR data in the course of a conversation with a person outside the entity, and
  - displays data on a computer screen so that the CDR data can be read by another entity or individual.
- 6.15 Where an accredited data recipient engages a third party to perform services on its behalf, the provision of CDR data to that third party will in most circumstances be a disclosure. However, in limited circumstances, providing CDR data to a third party to perform services on behalf of the entity may be a use, rather than a disclosure. See paragraphs B.123 and B.172-173 of Chapter B (Key concepts) for guidance on how to determine whether providing CDR data to a third party is a use or disclosure.

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

- 6.16 This section outlines when an accredited data recipient may use or disclose CDR data.<sup>11</sup>
- 6.17 This chapter does not consider when a designated gateway may use or disclose CDR data. This is because there are no designated gateways for the banking sector.
- 6.18 The following diagram outlines at a high-level the permitted and prohibited uses or disclosures of CDR data for an accredited data recipient. These uses and disclosures are discussed further below in this section.
- 6.19 An accredited data recipient must comply with the data minimisation principle when using CDR data. For further information on the data minimisation principle, see paragraphs 6.25-6.27 below.

---

<sup>11</sup> Privacy Safeguard 6 allows for the use or disclosure of CDR data in certain circumstances. One of these circumstances is where the disclosure is required under the CDR Rules in response to a valid request from a consumer for the CDR data (s 56EI(1)(a) of the Competition and Consumer Act). The CDR Rules do not currently require an accredited data recipient to disclose CDR data in response to a valid request – they only *authorise* the accredited data recipient to do so.

As such, an accredited data recipient is currently only able to use or disclose CDR data where required or authorised under the CDR Rules or under an Australian law or a court/tribunal order. These circumstances are outlined in this chapter from paragraph [6.20] onwards.



## Permitted uses or disclosure of CDR data

- ✓ Providing goods or services requested by the consumer
- ✓ Deriving CDR data to provide goods or services requested by the consumer
- ✓ Disclosing CDR data to the consumer to provide the requested goods or services
- ✓ Disclosing CDR data to an outsourced service provider in order to provide goods or services requested by the consumer
- ✓ Disclosing CDR data that has been de-identified in accordance with the CDR rules
- ✓ De-identifying CDR data for use in general research and/or for disclosure, with the consumer's consent and in accordance with the CDR data de-identification process
- ✓ From 1 July 2021 (or a relevant data standard being made), disclosing CDR data to an accredited person, in accordance with a consumer's 'AP disclosure consent'
- ✓ Disclosing CDR data to an accredited person if the CDR consumer has provided the accredited person and accredited data recipient with the appropriate consents
- ✓ Disclosing service data to the principal under a CDR outsourcing arrangement
- ✓ Using or disclosing CDR data where required or authorised by law

## Prohibited uses or disclosure of CDR data

- ✗ Using the CDR data to identify, compile insights or build a profile about a person who isn't the consumer, unless an exception applies
- ✗ Any uses or disclosures that an accredited data recipient is not permitted to seek consent for (permitted consents are listed in Rule 1.10A)
- ✗ Prior to 1 July 2021 (or a relevant data standard being made) disclosing the CDR data to an accredited person in accordance with an 'AP disclosure consent'

## Use or disclosure required or authorised under the CDR Rules

6.20 Privacy Safeguard 6 provides that an accredited data recipient of CDR data must not use or disclose CDR data unless the use or disclosure is required or authorised under the CDR Rules.<sup>12</sup>

6.21 CDR Rule 7.5(1) authorises the following permitted uses or disclosures of CDR data:

- using CDR data to provide goods or services requested by the consumer in compliance with the data minimisation principle and in accordance with a current use consent from the consumer (other than a direct marketing consent)
- de-identifying CDR data in accordance with the CDR Rules to use for general research and/or for disclosing (including by selling) the de-identified data, in accordance with a current de-identification consent from the consumer<sup>13</sup>
- directly or indirectly deriving CDR data from the collected CDR data in accordance with the above uses
- disclosing to the consumer any of their CDR data for the purpose of providing the existing goods or services<sup>14</sup>
- disclosing the consumer's CDR data to an outsourced service provider:
  - for the purpose of doing the things referred to above, and
  - to the extent reasonably needed to do those things
- from 1 July 2021 or the making of a relevant data standard, disclosing CDR data to an accredited person in accordance with a current 'AP disclosure consent'<sup>15</sup>
- disclosing (by sale or otherwise) to any person, CDR data that has been de-identified in accordance with the CDR data de-identification process<sup>16</sup>

---

<sup>12</sup> Section 56EI(1)(b) of the Competition and Consumer Act. The use or disclosure of CDR data is not currently required under the CDR Rules. The use or disclosure of CDR data is authorised under the CDR Rules if it is a 'permitted use or disclosure' under CDR Rule 7.5 that does not relate to direct marketing (CDR Rules 7.6(1) and 7.7).

<sup>13</sup> 'General research' is defined in CDR Rule 1.7 to mean research undertaken by an accredited data recipient with CDR data de-identified in accordance with the CDR Rules that does not relate to the provision of goods or services to any particular CDR consumer. Note that while CDR Rule 7.5(1)(aa) refers to a current 'use consent', a de-identification consent is a form of 'use consent' and is the relevant category of consent that must be obtained for the purposes of CDR Rule 7.5(1)(aa).

<sup>14</sup> The phrase, 'existing goods or services' is defined in CDR Rule 7.5(1)(a) to mean the goods or services requested by the consumer.

<sup>15</sup> Disclosure of CDR data to an accredited person under an 'AP disclosure consent' is not a permitted use or disclosure until the earlier of 1 July 2021 or the day a consumer experience data standard is made for the disclosure of CDR data to accredited persons: CDR Rule 7.5A.

Note that while CDR Rule 7.5(1)(ca) refers to a current 'disclosure consent', an AP disclosure consent is a form of 'disclosure consent' and is the relevant category of consent that must be obtained for the purposes of CDR Rule 7.5(1)(ca).

<sup>16</sup> CDR Rule 7.5(1)(e). This permitted disclosure authorises the disclosure of CDR data that has been de-identified in accordance with the CDR data de-identification process, whether in accordance with a de-identification consent from the consumer or because the data was redundant data that needed to be de-identified for the purposes of Privacy Safeguard 12.

- where the accredited data recipient collected CDR data on behalf of a principal under a CDR outsourcing arrangement—disclosing service data to the principal under the arrangement, and
- disclosing CDR data to an accredited person if the CDR consumer has provided the accredited person and accredited data recipient the appropriate consents.<sup>17</sup>

6.22 CDR Rules 7.5(2) and 7.5A prohibit the following uses or disclosures of CDR data:

- any uses or disclosures that an accredited data recipient is not permitted to seek consent for<sup>18</sup>
- prior to 1 July 2021 or a relevant data standard being made, disclosing CDR data to an accredited person under an AP disclosure consent<sup>19</sup>
- using CDR data for the purpose of identifying, compiling insights in relation to, or building a profile in relation to, any identifiable person who is not a consumer who made the consumer data request (including through aggregating the CDR data), unless the accredited data recipient is, in accordance with the consumer's consent:
  - deriving, from that CDR data, CDR data about that person's interactions with the consumer, and
  - using that derived CDR data in order to provide the requested goods or services.

6.23 CDR Rule 4.12(3) prohibits an accredited data recipient from asking a consumer to give consent to the use or disclosure of their CDR data for the above prohibited uses or disclosures.<sup>20</sup>

6.24 The permitted uses and disclosures (in paragraph 6.21) are discussed further in this chapter.

## 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 CDR data to provide goods or services requested by the consumer, or to fulfil any other purpose consented to by the consumer.<sup>21</sup>

6.26 An accredited data recipient complies with the data minimisation principle if, when providing the requested goods or services or using collected CDR data for any other purpose consented to by the CDR consumer, it does not use the collected CDR data, or CDR data derived from it, beyond what is reasonably needed to provide the goods or services requested by the consumer or fulfill the other purpose as consented to by the consumer.<sup>22</sup>

---

<sup>17</sup> CDR Rule 7.5(1)(g) permits the disclosure of CDR data to an accredited person if the consumer has given the accredited person a collection and use consent to collect CDR data from the accredited data recipient. The consumer must also have given the accredited data recipient an AP disclosure consent. For further information on the types of consents, [see Chapter C \(Consent\)](#).

<sup>18</sup> An accredited data recipient may only ask a consumer to consent to the use or disclosure of their CDR data where use or disclosure falls within a category of consents. The categories of consents are outlined CDR Rule 1.10A(2). For further information on consent, [see Chapter C \(Consent\)](#).

<sup>19</sup> Disclosure of CDR data to an accredited person under an AP disclosure consent is not a permitted use or disclosure until the earlier of 1 July 2021 or the day a consumer experience data standard is made for the disclosure of CDR data to accredited persons: CDR Rule 7.5A.

<sup>20</sup> For further information regarding restrictions on seeking consent, [see Chapter C \(Consent\)](#).

<sup>21</sup> CDR Rule 7.5(1)(a).

<sup>22</sup> CDR Rule 1.8(b).

The accredited data recipient must also not seek to collect the CDR data to use for a longer time period than is reasonably needed.<sup>23</sup>

- 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 person should pay careful attention to its processes and systems to ensure it complies with the data minimisation principle for all uses of CDR data. This includes consideration of the minimum CDR data needed to provide each good or service to a consumer

**Privacy tip:** An accredited person should set up its systems and processes so that it can identify the minimum CDR data needed for a particular good or service. This will reduce the risk of over collection of CDR data and ensure that the person does not exceed the limitations imposed by the data minimisation principle.

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

- 6.28 An accredited data recipient is authorised to use CDR data in accordance with a current use consent from the consumer to provide goods or services requested by the consumer.<sup>24</sup>
- 6.29 The relevant uses are those uses to which the consumer expressly consented, when providing a valid request for the accredited person to collect their CDR data from a CDR participant under CDR Rule 4.3(1).<sup>25</sup> Valid requests are discussed further in [Chapter 3 \(Privacy Safeguard 3\)](#).
- 6.30 For information regarding use consents and how they must be managed, [see Chapter C \(Consent\)](#).

### Example

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

SpendLess runs Oliver’s transaction data through an algorithm to ascertain what other SpendLess products Oliver might be interested in.

*cont*

<sup>23</sup> CDR Rule 1.8 (a)(ii).

<sup>24</sup> CDR Rule 7.5(1)(a). The requested goods or services are the goods or services requested under CDR Rule 4.3(1) as part of the consumer’s valid request.

<sup>25</sup> Note: CDR Rule 7.5(1)(a) permits the general ‘use’ of CDR data to provide the goods and services requested by the consumer. CDR Rule 7.5(1)(a) does not authorise the specific types of uses defined under ‘de-identification consent’ or ‘direct marketing consent’ as per CDR Rule 1.10A. (These uses are instead authorised by 7.5(1)(aa) and 7.5(3), respectively.)

When providing his valid request to SpendLess,<sup>26</sup> Oliver consented to the analysis of his transaction data so that SpendLess can identify how much money he has been spending in particular categories. He did not consent to his transaction data being used to allow SpendLess to develop and communicate offers about other products.

SpendLess has used Oliver's CDR data in a way that is not in accordance with his use consent, and this use would therefore not be a permitted use under CDR Rule 7.5(1)(a).<sup>27</sup>

## Using or disclosing de-identified CDR data in accordance with a de-identification consent

- 6.31 An accredited data recipient is permitted to de-identify CDR data in accordance with a current de-identification consent<sup>28</sup> from the consumer to:
- use the de-identified data for general research, and/or
  - disclose (including by selling) the de-identified data.<sup>29</sup>
- 6.32 The CDR data must be de-identified in accordance with the CDR data de-identification process outlined in CDR Rule 1.17.<sup>30</sup>
- 6.33 'General research' means research undertaken using de-identified CDR data, and that does not relate to the provision of goods or services to any particular consumer<sup>31</sup> (for example, research for product or business development).<sup>32</sup>
- 6.34 Before de-identifying CDR data in accordance with CDR Rule 1.17, the accredited data recipient must have first:
- received a de-identification consent from the consumer,<sup>33</sup> and
  - provided the consumer with additional information relating to the de-identification of CDR data.<sup>34</sup>

<sup>26</sup> 'Valid requests' are defined in CDR Rule 4.3. A key component of a 'valid request' is the consumer's collection consent and use consent. For further information, see [Chapter 3 \(Privacy Safeguard 3\)](#).

<sup>27</sup> SpendLess has used Oliver's CDR data in a manner that may constitute direct marketing under the CDR regime. For information regarding direct marketing, see [Chapter 7 \(Privacy Safeguard 7\)](#).

<sup>28</sup> Note that while CDR Rule 7.5(1)(aa) refers to a current 'use consent', a de-identification consent is a form of 'use consent' and is the relevant category of consent that must be obtained for the purposes of CDR Rule 7.5(1)(aa).

<sup>29</sup> CDR Rule 7.5(1)(aa).

<sup>30</sup> For further information regarding the CDR data de-identification process, see Chapter 12 – Security of CDR data and destruction or deidentification of redundant data. CDR Rule 7.5(1)(aa).

<sup>31</sup> CDR Rule 1.7(1).

<sup>32</sup> Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020* at [21].

<sup>33</sup> A 'de-identification consent' is defined in CDR Rule 1.10A(1)(e). It must be sought in accordance with the requirements in Division 4.3 of the CDR Rules. For further information, see [Chapter C \(Consent\)](#).

<sup>34</sup> CDR Rule 4.15. CDR Rules 4.11(3)(e) and 4.15. For further information, see [Chapter C \(Consent\)](#).

## Deriving or indirectly deriving CDR data

- 6.35 An accredited data recipient is permitted to directly or indirectly derive CDR data from the collected CDR data in order to use the data to provide the goods or services requested by the consumer.<sup>35</sup>
- 6.36 This is a permitted use under CDR Rule 7.5(1) and does not require the consent of the consumer.
- 6.37 However, where an accredited person:
- 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.<sup>36</sup>
- 6.38 Derived CDR data is discussed in more detail in [Chapter B \(Key concepts\)](#).

## Disclosing CDR data to the consumer

- 6.39 An accredited data recipient is permitted to disclose to a consumer any of their CDR data for the purpose of providing the existing goods or services.<sup>37</sup>
- 6.40 This includes CDR data collected from a data holder or accredited data recipient in response to the consumer's valid request, as well as data that has been directly and/or indirectly derived from such CDR data.
- 6.41 This is a permitted disclosure under CDR Rule 7.5(1) and does not require the consent of the consumer.

## Disclosing CDR data to an outsourced service provider

- 6.42 An accredited data recipient is permitted to disclose the consumer's CDR data to an outsourced service provider for the purpose of:
- using the consumer's CDR data to provide goods or services requested by the consumer, including by directly or indirectly deriving CDR data from the CDR data, and
  - disclosing, to the consumer, any of their CDR data for the purpose of providing the existing goods or services,
- to the extent reasonably needed to do those things.<sup>38</sup>

---

<sup>35</sup> CDR Rule 7.5(1)(b).

<sup>36</sup> CDR Rule 4.12(4).

<sup>37</sup> CDR Rule 7.5(1)(c).

<sup>38</sup> CDR Rule 7.5(1)(d).

### 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 category, so that SpendLess can provide tailored budgeting advice to consumers.

SpendLess discloses Oliver's account and transaction data to KnowYourMoney. However, SpendLess did not first consider whether KnowYourMoney needs both transaction and account data for this purpose.

If KnowYourMoney does not need to analyse Oliver's account data in order to report on his spending trends, SpendLess may have disclosed Oliver's CDR data to an outsourced service provider beyond the extent reasonably needed to provide the service requested by Oliver. The disclosure by SpendLess may therefore not be a permitted disclosure under CDR Rule 7.5(1)(d).

- 6.43 The consumer's CDR data includes data collected from a data holder or accredited data recipient in response to the consumer's request. The consumer's CDR data also includes data that has been directly and/or indirectly derived from their CDR data.
- 6.44 Disclosure of a consumer's CDR data by an accredited data recipient to an outsourced service provider for the purpose outlined in paragraph 6.39 is a permitted disclosure under CDR Rule 7.5(1) that does not require the consent of the consumer.<sup>39</sup>
- 6.45 Where an accredited person intends to disclose the CDR data of a consumer to an outsourced service provider, the accredited person must:
- provide certain information to the consumer at the time of seeking the consumer's consent to collect and use the consumer's CDR data,<sup>40</sup> and
  - include certain information about outsourced service providers in its CDR policy.<sup>41</sup>
- 6.46 An accredited data recipient who discloses CDR data to an outsourced service provider under a CDR outsourcing arrangement must ensure that the provider complies with its requirements under the arrangement.<sup>42</sup>
- 6.47 For the purposes of this permitted disclosure, an outsourced service provider is a person to whom an accredited data recipient discloses CDR data under a CDR outsourcing arrangement.<sup>43</sup>
- 6.48 In addition, the accredited data recipient should ensure that the relevant CDR outsourcing arrangement requires the outsourced service provider to adhere to the accredited data recipient's Privacy Safeguard obligations.

<sup>39</sup> However, the accredited data recipient must ensure it has complied with the requirements set out in paragraph 6.39.

<sup>40</sup> CDR Rule 4.11(3)(f). See Chapter C (Consent).

<sup>41</sup> CDR Rule 7.2(4). [See Chapter 1 \(Privacy Safeguard 1\).](#)

<sup>42</sup> CDR Rule 1.16.

<sup>43</sup> CDR Rule 1.10. A CDR outsourcing arrangement is a written contract between the accredited data recipient and outsourced service provider which meets the requirements set out in CDR Rule 1.10(2), and under which the provider will provide goods or services to the accredited data recipient. For further information, see [Chapter B \(Key Concepts\)](#).



- 6.49 The contract should also provide the accredited data recipient with the appropriate level of transparency to allow them to monitor and audit the CDR outsourcing arrangement.
- 6.50 The CDR data disclosed by an accredited data recipient to a provider under the CDR outsourcing arrangement, including any data directly or indirectly derived from such CDR data, is known as ‘service data’ in relation to that arrangement.
- 6.51 Any use or disclosure of such service data by the outsourced service provider (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.<sup>44</sup>
- 6.52 When disclosing CDR data to an outsourced service provider located outside of Australia, an accredited data recipient must also have regard to the requirements for disclosure of CDR data to an overseas recipient under Privacy Safeguard 8.<sup>45</sup> [See Chapter 8 \(Privacy Safeguard 8\)](#) for more information.
- 6.53 For further information, [see Chapter B \(Key Concepts\)](#), ‘Outsourced service providers’.

## Disclosing CDR data to an accredited person

- 6.54 From the earlier of 1 July 2021 or the making of a relevant data standard,<sup>46</sup> an accredited data recipient is permitted to disclose a consumer’s CDR data to an accredited person in accordance with an ‘AP disclosure consent’.<sup>47</sup> Prior to this, disclosing CDR data to an accredited person under an AP disclosure consent is prohibited.<sup>48</sup>
- 6.55 An ‘AP disclosure consent’ is a consent given by the consumer for an accredited data recipient to disclose their CDR data to an accredited person in response to a consumer data request.<sup>49</sup>
- 6.56 For further information on ‘AP disclosure consents’ and consumer data requests, see [Chapter C Consent](#).

## Disclosing service data to a principal in an CDR outsourcing arrangement

- 6.57 Where an accredited data recipient has collected CDR data on behalf of a principal (i.e. as an outsourced service provider) under a CDR outsourcing arrangement, the accredited data recipient is permitted to disclose that CDR data (known as ‘service data’) to the principal.<sup>50</sup>

---

<sup>44</sup> CDR Rule 7.6(2). This is the case whether the CDR data was used or disclosed by the outsourced service provider, or indirectly used or disclosed through one or more further CDR outsourcing arrangements (CDR Rule 7.6(2)(b)(ii)). See also s 56AU of the Competition and Consumer Act, regarding the application to acts done by or in relation to agents of CDR entities.

<sup>45</sup> An accredited person must also include certain information in its CDR policy about outsourced service providers located overseas (CDR Rule 7.2(4)(d)). [See Chapter 1 \(Privacy Safeguard 1\)](#) for further information.

<sup>46</sup> That is, a consumer experience data standard for the disclosure of CDR data to accredited persons: CDR Rules 7.5A and 8.11(1)(c)(iii).

<sup>47</sup> CDR Rules 7.5(1)(ca) and 7.5(1)(g). Note that while CDR Rule 7.5(1)(ca) refers to a current ‘disclosure consent’, an AP disclosure consent is a form of ‘disclosure consent’ and is the relevant category of consent that must be obtained for the purposes of CDR Rule 7.5(1)(ca).

<sup>48</sup> CDR Rule 7.5A.

<sup>49</sup> CDR Rule 1.10A(1)(c)(i). For further information, see [Chapter C \(Consent\)](#).

<sup>50</sup> CDR Rule 7.5(1)(f).



- 6.58 'Service data' consists of any CDR data that was collected from a CDR participant in accordance with the CDR outsourcing arrangement, or has been directly or indirectly derived from such CDR data.<sup>51</sup>
- 6.59 The 'principal' refers to the accredited person that engaged the accredited data recipient as an outsourced service provider under a CDR outsourcing arrangement.
- 6.60 Disclosure of service data in relation to a CDR outsourcing arrangement by an accredited data recipient to the relevant principal is a permitted disclosure under CDR Rule 7.5(1) that does not require the consent of the consumer.

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

- 6.61 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.<sup>52</sup>
- 6.62 For the purposes of Privacy Safeguard 6, an Australian law does not include the APPs under the Privacy Act.<sup>53</sup>
- 6.63 'Australian law' and 'court/tribunal order' are discussed in [Chapter B \(Key concepts\)](#).
- 6.64 The accredited data recipient must keep a written note of any uses or disclosures made on this ground.
- 6.65 A written note should include the following details:
- the date of the use or disclosure
  - details of the CDR data that was used or disclosed
  - the relevant Australian law or court/tribunal order that required or authorised the use or disclosure
  - if the accredited data recipient used the CDR data, how the CDR data was used by the accredited data recipient, and
  - if the accredited data recipient disclosed the CDR data, to whom the CDR data was disclosed.

## Interaction with other Privacy Safeguards

- 6.66 The restrictions on using or disclosing CDR data in Privacy Safeguard 6 are additional to those in Privacy Safeguards 7 ([see Chapter 7 \(Privacy Safeguard 7\)](#)), 8 ([see Chapter 8 \(Privacy Safeguard 8\)](#)) and 9 ([see Chapter 9 \(Privacy Safeguard 9\)](#)).
- 6.67 Privacy Safeguard 7 prohibits accredited data recipients and designated gateways from using or disclosing CDR data for direct marketing unless the use or disclosure is required or authorised under the CDR Rules and in accordance with a valid consent.
- 6.68 Privacy Safeguard 8 prohibits the accredited data recipient from disclosing CDR data to an overseas recipient unless an exception applies.

---

<sup>51</sup> CDR Rule 1.10(4).

<sup>52</sup> Section 56EI(1)(c) of the Competition and Consumer Act.

<sup>53</sup> Sections 56EI(1) (Note 3) and 56EC(4)(a) of the Competition and Consumer Act.

- 6.69 Privacy Safeguard 9 prohibits an accredited data recipient of CDR data that contains a government related identifier from adopting, using or disclosing that identifier, unless an exception applies.
- 6.70 Privacy Safeguard 7 operates to the exclusion of Privacy Safeguard 6<sup>54</sup> (which means that direct marketing uses or disclosures cannot be authorised under Privacy Safeguard 6), while Privacy Safeguards 8 and 9 operate as restrictions in addition to Privacy Safeguard 6.<sup>55</sup>

---

<sup>54</sup> Section 56E(3) of the Competition and Consumer Act.

<sup>55</sup> See Note 2 of s 56EK and Note 2 of s 56EL of the Competition and Consumer Act.

## Chapter 7:

# Privacy Safeguard 7 —

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

Version 3.0, June 2021

# Contents

<b>Key points</b>	<b>3</b>
<b>What does Privacy Safeguard 7 say?</b>	<b>3</b>
<b>Who does Privacy Safeguard 7 apply to?</b>	<b>3</b>
<b>How Privacy Safeguard 7 interacts with the Privacy Act</b>	<b>4</b>
<b>What is direct marketing?</b>	<b>5</b>
Information about upgraded or alternative goods or services	7
Offer to renew existing goods or services	7
Information about the benefits of existing goods or services	8
Using the CDR data as reasonably needed, in accordance with the data minimisation principle	9
Disclosure to an outsourced service provider	10
<b>Interaction with other privacy safeguards</b>	<b>11</b>

## Key points

- Privacy Safeguard 7 prohibits accredited data recipients of CDR data and designated gateways from using or disclosing the CDR data for direct marketing, unless the consumer consents and such use or disclosure is required or authorised under the consumer data rules (CDR Rules).
- Direct marketing in the CDR context involves the use or disclosure of consumer data right (CDR) data to promote goods and services directly to a consumer.
- The CDR Rules permit accredited data recipients of CDR data to engage in certain direct marketing activities in relation to the good or service requested by the consumer, if consent has been received to do so.
- An accredited data recipient of CDR data must comply with the data minimisation principle when using the CDR data for direct marketing.

## What does Privacy Safeguard 7 say?

- 7.1 Privacy Safeguard 7 prohibits accredited data recipients of CDR data and designated gateways from using or disclosing the CDR data for direct marketing, unless the consumer consents and such use or disclosure is required or authorised under the consumer data rules (CDR Rules). CDR Rules 7.8 and 7.5(3) authorise certain direct marketing related uses or disclosures by accredited data recipients (in accordance with the consumer's consent).

## 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 Direct marketing is addressed separately to other uses and disclosures ([see under Privacy Safeguard 6](#)) because of significant community sentiments in relation to direct marketing.

## Who does Privacy Safeguard 7 apply to?

- 7.4 Privacy Safeguard 7 applies to accredited data recipients of CDR data and designated gateways for CDR data. It does not apply to data holders.
- 7.5 Data holders 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 7 in respect of direct marketing.

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

# How Privacy Safeguard 7 interacts with the Privacy Act

7.6 It is important to understand how Privacy Safeguard 7 interacts with the Privacy Act and the APPs.<sup>1</sup>

7.7 APP 7 sets out when an APP entity is prohibited from using or disclosing personal information for the purpose of direct marketing.

CDR entity	Privacy protections that apply in the CDR context
<b>Accredited data recipient</b>	<p><b>Privacy Safeguard 7</b></p> <p>For accredited data recipients of a consumer's CDR data, Privacy Safeguard 7 applies to any uses or disclosures of that CDR data for direct marketing.<sup>2</sup></p> <p>APP 7 does not apply in relation to that CDR data.<sup>3</sup></p>
<b>Designated gateway</b>	<p><b>Privacy Safeguard 7</b></p> <p>For designated gateways for CDR data, Privacy Safeguard 7 applies to the use and disclosure of the CDR data for direct marketing.<sup>4</sup></p> <p>APP 7 does not apply in relation to that CDR data.<sup>5</sup></p>
<b>Data holder</b>	<p><b>APP 7</b></p> <p>Privacy Safeguard 7 does not apply to a data holder.</p>

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

<sup>2</sup> Privacy Safeguard 7 applies from the point when the accredited person becomes an accredited data recipient of the CDR data. An accredited person becomes an accredited data recipient for CDR data when:

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

<sup>3</sup> The APPs do not apply to an accredited data recipient of CDR data, in relation to that CDR data - s 56EC(4)(a) of the Competition and Consumer Act. However, s 56EC(4) does not affect how the APPs apply to accredited persons and accredited data recipients who are APP entities, in relation to the handling of personal information outside the CDR system. (Note: Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See s 6E(1D) of the Privacy Act.) Section 56EC(4) also does not affect how the APPs apply to an accredited person who does not become an accredited data recipient of the CDR data (other than for Privacy Safeguards 1 – 4). See s 56EC(5)(aa) of the Competition and Consumer Act.

<sup>4</sup> Section 56EJ(2) of the Competition and Consumer Act.

<sup>5</sup> The APPs do not apply to designated gateways for CDR data in relation to that CDR data - s 56EC(4)(d) of the Competition and Consumer Act. However, s 56EC(4) does not affect how the APPs apply to designated gateways who are APP entities, in relation to the handling of personal information outside the CDR system. See s 56EC(5)(b) of the Competition and Consumer Act.

## What is direct marketing?

- 7.8 ‘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.<sup>6</sup>
- 7.9 For the purpose of Privacy Safeguard 7, ‘direct marketing’ takes its ordinary meaning, and involves an entity’s use or disclosure of CDR data to communicate directly with a consumer to promote goods and services.
- 7.10 An example of direct marketing by an entity includes sending an email to a consumer promoting financial products using the consumer’s CDR data.<sup>7</sup>
- 7.11 ‘Direct marketing’ is distinct from the situation where:
- a consumer has requested a good or service
  - the accredited data recipient has obtained the consumer’s consent to collect and use the consumer’s CDR data to provide this good or service, and
  - the requested good or service is to provide the consumer with offers about suitable products (for example, a service offered by a comparison site).<sup>8</sup>

This is illustrated in the following examples.

### Example one — comparison site

Kwok wishes to obtain suitable offers from multiple providers for term deposit products and provides Tang and Co Pty Ltd, an accredited person, with a valid request to collect his CDR data from the data holders of his CDR data for this purpose.

Tang and Co provides Kwok with offers for term deposit products as requested, using Kwok’s CDR data that it has collected in accordance with the CDR Rules.

### Example two — switching banking providers

Guy is considering switching banking providers for his credit card and provides McCarthy Bank, an accredited person, with a valid request to collect his CDR data from his existing bank for the purpose of providing suitable offers in relation to credit cards.

McCarthy Bank provides Guy with the offers for credit card products as requested, using Guy’s CDR data it has collected in accordance with the CDR Rules.

In both examples, the uses of the consumer’s CDR data by the accredited person (Tang and Co/McCarthy Bank) would not be ‘direct marketing’ and Privacy Safeguard 7 would not apply. The accredited person’s use of the consumer’s CDR data would be a permitted use under Privacy Safeguard 6 as the CDR data would be used for the purpose of providing the service requested by the consumer (Kwok/Guy).

*cont*

<sup>6</sup> 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).

<sup>7</sup> For information regarding ‘valid requests’, [see Chapter 3 \(Privacy Safeguard 3\)](#).

<sup>8</sup> Explanatory Statement to the CDR Rules.

However, if Tang and Co or McCarthy Bank were to use Kwok or Guy's CDR data to provide offers about other products not requested by the consumer, this would likely be 'direct marketing' and if so would be permitted only if this was authorised under the CDR Rules.<sup>9</sup>

## When is direct marketing allowed?

- 7.12 Generally, an entity is not permitted to engage in direct marketing under the CDR regime.
- 7.13 However, the CDR Rules permit an accredited data recipient of CDR data to engage in certain specific direct marketing activities in relation to the 'existing goods or services' being provided to the consumer, in accordance with a 'direct marketing consent'.<sup>10</sup>
- 7.14 The 'existing goods or services' refer to the goods or services requested by the consumer.<sup>11</sup>
- 7.15 A 'direct marketing consent' is a consent provided by a consumer under the CDR Rules for an accredited data recipient to use or disclose CDR data for the purposes of direct marketing.<sup>12</sup> An accredited person must ask for the consumer's express consent in accordance with Division 4.3 of the CDR Rules for any direct marketing they intend to undertake. <sup>13</sup>
- 7.16 CDR Rule 7.5(3) allows an accredited data recipient to use or disclose CDR data for the following permitted direct marketing activities:
- in accordance with a consumer's direct marketing consent:
    - sending the consumer information about upgraded or alternative goods or services to the existing goods or services
    - sending the consumer an offer to renew existing goods or services when they expire
    - sending the consumer information about the benefits of existing goods or services
    - sending the consumer information about other goods and services provided by another accredited person if the accredited data recipient reasonably believes the consumer might benefit from these other goods or services, and only sends such information on a reasonable number of occasions
    - disclosing the consumer's CDR data to an accredited person so that the accredited person may provide the goods or services referred to in the dot point above, but only where the consumer has provided a disclosure consent.
  - using CDR data in a way and to the extent that is reasonably needed in order to send the consumer something permitted by the paragraph above (including by analysing the CDR data to identify the appropriate information to send), and
  - disclosing the consumer's CDR data to an outsourced service provider:
    - for the purpose of doing the things referred to in the above two paragraphs, and

<sup>9</sup> This would be 'direct marketing' even where the offers were about other products related to the requested product.

<sup>10</sup> CDR Rules 7.8 and 7.5(3). Examples of existing goods or services include the services provided by Tang and Co to Kwok, and McCarthy Bank to Guy, in the examples under paragraph 7.11.

<sup>11</sup> CDR Rule 7.5(1)(a).

<sup>12</sup> CDR Rule 1.10A(d). See Chapter B (Key concepts) for further information on direct marketing consents.

<sup>13</sup> See especially CDR Rules 4.11(1)(a)(ii), 4.11(1)(c) and 4.11(2). For guidance regarding the requirements for seeking direct marketing consents, [see Chapter C \(Consent\)](#).



- to the extent reasonably needed to do those things.

## Information about upgraded or alternative goods or services

- 7.17 Sending the consumer information about upgraded<sup>14</sup> or alternative<sup>15</sup> goods or services is direct marketing.<sup>16</sup> An accredited data recipient of CDR data may only engage in this form of direct marketing if it has obtained a direct marketing consent (which is still current) from the consumer under Division 4.3 of the CDR Rules.<sup>17</sup>

### Example

Loan Tracker Pty Ltd is an accredited person that offers products and services to assist consumers to monitor and repay their loans.

Loan Tracker asks its customers for their consent to receive direct marketing information about upgraded or alternative goods or services when seeking their consent to collect and use their CDR data to provide the requested service.

Through the 'Show Me My Money' service offered by Loan Tracker, monthly emails are sent to consumers setting out their current aggregate loan balances, the amount required to be repaid over the month, and estimating the consumer's disposable income for that month after repayments and living expenses are taken into account.

Loan Tracker also wishes to include in its monthly emails links to information about other products and services offered by Loan Tracker which it considers might be useful to the consumer.

*If Loan Tracker includes these links to information about other products and services, this may constitute using consumers' CDR data to directly market its other products and services.*

*Loan tracker may only use the CDR data to engage in the direct marketing activities if it:*

- *has obtained a direct marketing consent (which is still current) for the purpose of sending information about upgraded or alternative goods or services, and*
- *is able to show that the other products and services marketed are truly 'upgraded' or 'alternative' services to the 'Show Me My Money' service.*

## Offer to renew existing goods or services

- 7.18 Sending the consumer an offer to renew the existing goods or services is direct marketing.<sup>18</sup> An accredited data recipient may only engage in this form of direct marketing if it has

<sup>14</sup> A good or service will be an 'upgraded' good or service if the good or service is an improved version of the existing good or service.

<sup>15</sup> A good or service will be an 'alternative' good or service if a consumer could choose between that good or service and the existing good or service in order to achieve a similar outcome.

<sup>16</sup> CDR Rule 7.5(3)(a)(i).

<sup>17</sup> See especially CDR Rules 4.11(1)(a)(ii), 4.11(1)(c) and 4.11(2). For guidance regarding the requirements for seeking direct marketing consents, [see Chapter C \(Consent\)](#).

<sup>18</sup> CDR Rule 7.5(3)(a)(ii).

obtained a direct marketing consent (which is still current) from the consumer under Division 4.3 of the CDR Rules.<sup>19</sup>

- 7.19 If the consumer wishes to ‘renew’ the existing goods or services, the accredited data recipient must once again seek the consumer’s consent to the collection, use and (if applicable) disclosure of their CDR data for the relevant good or service. This is because an accredited person may seek to collect CDR data only in response to a valid request from the consumer.<sup>20</sup>
- 7.20 From 1 July 2021,<sup>21</sup> an accredited data recipient may, in certain cases, invite a consumer to amend the duration of their consent (for example, by extending its duration).<sup>22</sup> Where an accredited data recipient wishes to issue such an invitation, they should first consider whether the invitation would constitute an offer to renew the existing goods or services under CDR Rule 7.5(3)(a)(ii) (in which case a direct marketing consent would be required).

## Information about the benefits of existing goods or services

- 7.21 Sending the consumer information about the benefits of the existing goods or services being used by the consumer is direct marketing.<sup>23</sup> An accredited data recipient may only engage in this form of direct marketing if it has obtained a direct marketing consent (which is still current) from the consumer under Division 4.3 of the CDR Rules.<sup>24</sup>

## Information about other goods or services provided by another accredited person

- 7.22 Sending the consumer information about other goods or services provided by another accredited person is direct marketing. An accredited data recipient may only engage in this form of direct marketing if it:
- has obtained a direct marketing consent from the consumer under Division 4.3 of the CDR Rules<sup>25</sup>
  - reasonably believes that the consumer might benefit from the goods or services offered by the other accredited person, and

---

<sup>19</sup> See especially CDR Rules 4.11(1)(a)(ii), 4.11(1)(c) and 4.11(2). For guidance regarding the requirements for seeking direct marketing consents, [see Chapter C \(Consent\)](#).

<sup>20</sup> The consumer’s consent to the collection and use of their CDR data for an accredited person to provide goods or services is required for a ‘valid request’: CDR Rule 4.3. For information regarding valid requests and the requirements for seeking consent, [see Chapter C \(Consent\)](#).

<sup>21</sup> CDR Rule 4.12B(5) provides that an accredited person must not invite a consumer to amend their consent before 1 July 2020.

<sup>22</sup> CDR Rule 4.12B. For further information about the requirements for asking a consumer to amend their consent, see CDR Rule 4.12C and [Chapter C \(Consent\)](#).

<sup>23</sup> CDR Rule 7.5(3)(a)(iii).

<sup>24</sup> See especially CDR Rules 4.11(1)(a)(ii), 4.11(1)(c) and 4.11(2). For guidance regarding the requirements for seeking direct marketing consents, [see Chapter C \(Consent\)](#).

<sup>25</sup> See especially CDR Rules 4.11(1)(a)(ii), 4.11(1)(c) and 4.11(2). For guidance regarding the requirements for seeking direct marketing consents, [see Chapter C \(Consent\)](#).

- sends such information to the consumer on no more than a reasonable number of occasions.<sup>26</sup>

## Disclosure to another accredited person to enable provision of promoted goods and services

- 7.23 An accredited data recipient of CDR data is permitted to disclose a consumer's CDR data to another accredited person for the purposes of enabling that accredited person to provide the goods or services outlined in paragraph 7.22.<sup>27</sup>
- 7.24 An accredited data recipient may only disclose CDR data to another accredited person if the consumer has provided both a direct marketing consent and a disclosure consent to the accredited data recipient in accordance with Division 4.3 of the CDR Rules.<sup>28</sup>

## Using the CDR data as reasonably needed, in accordance with the data minimisation principle

- 7.25 Using CDR data for the purpose of sending the information or renewal offer outlined above in paragraphs 7.17, 7.18, 7.21, 7.22 and 7.23 including by analysing the data to decide what, if any, information will be sent, is direct marketing.<sup>29</sup>
- 7.26 In order to use the CDR data for this purpose, the underlying direct marketing consent for the sending of information or renewal offers must be current.
- 7.27 An accredited data recipient must comply with the data minimisation principle when using the CDR data for these direct marketing purposes. This means that the CDR data, and any CDR data derived from it, must only be used as reasonably needed to fulfil the relevant direct marketing purpose
- 7.28 For further information on the data minimisation principle, see [Chapter B \(Key concepts\)](#).

**Privacy tip:** An accredited data recipient must allow a consumer to withdraw their direct marketing consent by:<sup>30</sup>

- using their dashboard, or
- through a 'simple alternative method of communication' made available for that purpose, such as an embedded link in an email communication through which they may notify the accredited data recipient of their intention to 'opt out'.

For further information regarding withdrawal of consent, see [Chapter C \(Consent\)](#).

<sup>26</sup> CDR Rule 7.5(3)(a)(iv).

<sup>27</sup> CDR Rule 7.5(3)(aa).

<sup>28</sup> For information regarding direct marketing consents and disclosure consents, see [Chapter C \(Consent\)](#).

<sup>29</sup> CDR Rule 7.5(3)(b).

<sup>30</sup> CDR Rule 4.13(1).

## Disclosure to an outsourced service provider

- 7.29 An accredited data recipient is permitted to disclose CDR data to an outsourced service provider for the purpose of sending the information or renewal offer (outlined above in paragraphs 7.17, 7.18, 7.21, 7.22 and 7.23), or to use the CDR data (as outlined above in paragraph 7.25).<sup>31</sup>
- 7.30 An accredited data recipient may only disclose CDR data to the extent reasonably needed for these purposes.<sup>32</sup>
- 7.31 Under this permitted disclosure, accredited persons may engage third parties (who fall within the meaning of ‘outsourced service provider’)<sup>33</sup> to undertake direct marketing activities on their behalf, where such activities are permitted under CDR Rule 7.5(3).
- 7.32 In order to disclose the CDR data for this purpose, the underlying direct marketing consent to send information or renewal offers must be current. In addition, the accredited person must:
- provide the information required by CDR Rule 4.11(3)(f) to the consumer at the time of seeking the consumer’s consent to collect and use the consumer’s CDR data, and
  - include certain information about outsourced service providers in its CDR policy.<sup>34</sup>
- 7.33 An accredited data recipient who discloses CDR data to an outsourced service provider must ensure that the provider complies with its requirements under the arrangement.<sup>35</sup>
- 7.34 For the purposes of this permitted disclosure, an outsourced service provider is a person to whom an accredited data recipient discloses<sup>36</sup> CDR data under a CDR outsourcing arrangement.<sup>37</sup>
- 7.35 If the disclosure is proposed to be made to an overseas outsourced service provider, Privacy Safeguard 8 will apply in addition to Privacy Safeguard 7 ([see Chapter 8 \(Privacy Safeguard 8\)](#)).
- 7.36 For further information, [see Chapter B \(Key Concepts\)](#), ‘Outsourced service providers’. For further guidance regarding an accredited data recipient’s obligations in relation to outsourced service providers, see [Chapter 6 \(Privacy Safeguard 6\)](#).

---

<sup>31</sup> CDR Rule 7.5(3)(c)(i).

<sup>32</sup> CDR Rule 7.5(3)(c)(ii).

<sup>33</sup> See CDR Rule 1.10. ‘Outsourced service provider’ is discussed in [Chapter B \(Key concepts\)](#).

<sup>34</sup> CDR Rule 7.2(4). [See Chapter 1 \(Privacy Safeguard 1\)](#).

<sup>35</sup> CDR Rule 1.16.

<sup>36</sup> Data will be ‘disclosed’ under the CDR regime where it is made accessible or visible to others outside the entity. Whether an accredited data recipient retains effective control over the data does not affect whether data is ‘disclosed’.

<sup>37</sup> CDR Rule 1.10. A CDR outsourcing arrangement is a written contract between the accredited data recipient and outsourced service provider which meets the requirements set out in CDR Rule 1.10(2), and under which the provider will provide goods or services to the accredited data recipient. For further information, see [Chapter B \(Key Concepts\)](#).

**Risk point:** As soon as the customer's direct marketing consent is no longer current (i.e. because it expires or is withdrawn), the accredited data recipient can no longer engage in the permitted uses or disclosure relating to direct marketing under the CDR Rules.

**Privacy tip:** Accredited data recipients should have processes and systems in place to promptly inform any outsourced service providers engaging in direct marketing activities of the expiry of a consumer's direct marketing consent.<sup>38</sup>

## Interaction with other privacy safeguards

- 7.37 The prohibition against direct marketing in Privacy Safeguard 7 is complemented by Privacy Safeguards 6 (see Chapter 6 (Privacy Safeguard 6)), 8 ([see Chapter 8 \(Privacy Safeguard 8\)](#)) and 9 (see [Chapter 9 \(Privacy Safeguard 9\)](#)).
- 7.38 Privacy Safeguard 6 prohibits an accredited data recipient of CDR data from using or disclosing CDR data unless required or authorised under the CDR Rules or another Australian law or court or tribunal order.
- 7.39 Privacy Safeguard 8 restricts disclosures of CDR data made to recipients located overseas.
- 7.40 Privacy Safeguard 9 prohibits an accredited data recipient of CDR data that contains a government related identifier from adopting, using or disclosing that identifier, unless an exception applies.

## Interaction with other legislation

- 7.41 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.
- 7.42 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,<sup>39</sup> and the entity uses or discloses CDR data for that purpose, the entity will be in breach of Privacy Safeguard 7 unless that use or disclosure is required or authorised under the CDR Rules.
- 7.43 Similarly, this means that if an accredited data recipient or designated gateway engages in a form of direct marketing permitted under Privacy Safeguard 7 and the CDR Rules, the entity may nevertheless be in breach of another Act if the requirements relating to marketing communications under that Act are not also satisfied.

<sup>38</sup> This will assist the accredited data recipient in directing an outsourced service provider under CDR Rule 1.10(2)(b)(iii).

<sup>39</sup> 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*, s 11(2)).

## Chapter 8:

# Privacy Safeguard 8 —

## Overseas disclosure of CDR data by accredited data recipients

Version 3.0, June 2021

# Contents

<b>Key points</b>	<b>3</b>
<b>What does Privacy Safeguard 8 say?</b>	<b>3</b>
<b>Why is this important?</b>	<b>4</b>
<b>Who does Privacy Safeguard 8 apply to?</b>	<b>4</b>
<b>How Privacy Safeguard 8 interacts with the Privacy Act</b>	<b>4</b>
<b>Meaning of disclosure</b>	<b>5</b>
<b>What is an overseas recipient?</b>	<b>5</b>
<b>When can CDR data be disclosed to an overseas recipient?</b>	<b>6</b>
Exception 1 — Disclosing CDR data to an overseas recipient who is an accredited person	8
Exception 2 — Disclosing CDR data after taking ‘reasonable steps’ to ensure an overseas recipient does not breach the privacy safeguards	8
Exception 3 — Disclosing CDR data where overseas recipient is subject to a substantially similar law	10
<b>When is an accredited data recipient accountable for the breaches by an overseas recipient?</b>	<b>12</b>
<b>How does Privacy Safeguard 8 interact with the other privacy safeguards?</b>	<b>13</b>
Privacy Safeguard 6	13
Privacy Safeguard 7	13
Privacy Safeguard 9	13

## Key points

- Privacy Safeguard 8 sets out the circumstances in which an accredited data recipient of a consumer's CDR data can disclose that data to a recipient located overseas.
- Under Privacy Safeguard 8, an accredited data recipient of a consumer's CDR data must not disclose that data to a recipient located overseas unless one of the following exceptions applies:
  - the overseas recipient is also an accredited person
  - the accredited data recipient takes reasonable steps to ensure the overseas recipient will not breach the privacy safeguards (noting that, for this exception, the accredited data recipient remains accountable for any breach 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.
- These requirements are in addition to the other disclosure restrictions set out in Privacy Safeguards 6, 7 and 9 and the consumer data rules (CDR Rules).

## What does Privacy Safeguard 8 say?

- 8.1 In addition to the disclosure restrictions set out in Privacy Safeguards 6, 7 and 9, and the CDR Rules, an accredited data recipient of a consumer's CDR data must not disclose that data to a person located overseas unless one of the following four exceptions applies:
- a. the overseas recipient is an accredited person
  - b. the accredited data recipient takes reasonable steps to ensure the overseas recipient does not breach the privacy safeguards<sup>1</sup> and the overseas recipient has a CDR policy in place in relation to the CDR data
  - c. the accredited data recipient reasonably believes the overseas recipient is bound by a law or scheme that is substantially similar to the privacy safeguards and a consumer will be able to enforce that law or scheme in relation to the CDR data, or
  - d. conditions specified in the CDR Rules for overseas disclosure are met. As there are currently no CDR Rules made specifically in relation to Privacy Safeguard 8, an accredited data recipient cannot rely on this exception.
- 8.2 Where the overseas recipient is not accredited or subject to a similar law or binding scheme to the privacy safeguards, even if an accredited data recipient takes reasonable steps to ensure the overseas recipient does not breach the privacy safeguards, but the overseas recipient nevertheless breaches a relevant privacy safeguard, the accredited data recipient remains accountable for that breach.

---

<sup>1</sup> The relevant privacy safeguards are the privacy safeguard penalty provisions as defined in s 56EU of the Competition and Consumer Act (Privacy Safeguards 3–13 inclusive, and the requirement to have a CDR policy in Privacy Safeguard 1).



- 8.3 For the purposes of a CDR outsourcing arrangement, an accredited data recipient must also comply with the CDR Rules that relate to CDR outsourcing arrangements.<sup>2</sup>

## Why is this important?

- 8.4 As an overarching objective of the CDR framework, consumers should be able to trust that an accredited data recipient will manage CDR data appropriately and in compliance with the privacy safeguards, especially when it is disclosed overseas.
- 8.5 It is also important that entities are aware of and understand the obligations on them to protect CDR data where they seek to make a disclosure of CDR data to an overseas recipient.

## Who does Privacy Safeguard 8 apply to?

- 8.6 Privacy Safeguard 8 applies to accredited data recipients of CDR data.
- 8.7 It does not apply to data holders or designated gateways.
- 8.8 Data holders and designated gateways should ensure that they adhere to their obligations under the *Privacy Act 1988* (Privacy Act) and the Australian Privacy Principles (APPs), including APP 8, when disclosing personal information to an overseas recipient.

## How Privacy Safeguard 8 interacts with the Privacy Act

- 8.9 It is important to understand how Privacy Safeguard 8 interacts with the Privacy Act and the APPs.<sup>3</sup>
- 8.10 APP 8 outlines when an APP entity may disclose personal information about an individual to an overseas recipient (see [Chapter 8 of the APP Guidelines: APP 8 — Cross-border disclosure of personal information](#)).

CDR entity	Privacy protections that apply in the CDR context
<b>Accredited data recipient</b>	<b>Privacy Safeguard 8</b> For accredited data recipients of a consumer's CDR data, Privacy Safeguard 8 applies to any overseas disclosures of that CDR data. <sup>4</sup>

<sup>2</sup> CDR Rules 1.10, 1.16(1), 7.5(1)(d) and 7.6. For more information on CDR outsourcing arrangements, please refer to [Chapter B \(Key concepts\)](#).

<sup>3</sup> The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies (APP entities).

<sup>4</sup> Privacy Safeguard 8 applies from the point when the accredited person becomes an accredited data recipient of the CDR data. An accredited person becomes an accredited data recipient for CDR data when:

- CDR data is held by (or on behalf of) the person
- the CDR data, or any other CDR data from which it was directly or indirectly derived, was disclosed to the person under the consumer data rules, and

CDR entity	Privacy protections that apply in the CDR context
	APP 8 does not apply in relation to that CDR data. <sup>5</sup>
<b>Designated gateway</b>	<b>APP 8</b> Privacy Safeguard 8 does not apply to a designated gateway.
<b>Data holder</b>	<b>APP 8</b> Privacy Safeguard 8 does not apply to a data holder.

## Meaning of disclosure

- 8.11 The term ‘disclose’ is not defined in the *Competition and Consumer Act 2010* (Competition and Consumer Act). It is discussed in [Chapter B \(Key concepts\)](#).
- 8.12 An accredited data recipient discloses CDR data when it makes it accessible or visible to others outside the entity.<sup>6</sup>
- 8.13 The release of the information may be a release in accordance with the CDR Rules, an accidental release or an unauthorised release.
- 8.14 This focuses on the act done by the disclosing party. The state of mind or intentions of the recipient does not affect the fact of disclosure. Further, there will be a disclosure even where the information is already known to the overseas recipient.
- 8.15 Where an accredited data recipient engages a third party to perform services on its behalf, the provision of CDR data to that provider will in most circumstances be a disclosure. However, in limited circumstances, providing CDR data to a third party to perform services on behalf of the entity may be a use, rather than a disclosure. See paragraphs B.123 and B.172 to B.173 of Chapter B (Key concepts) for guidance on how to determine whether providing CDR data to a third party a use or disclosure.

## What is an overseas recipient?

- 8.16 Under Privacy Safeguard 8, an overseas recipient is a person,<sup>7</sup> who receives CDR data from an accredited data recipient, who is not:
- in Australia or in an external Territory and
  - a consumer for the CDR data.

- 
- the person is neither a data holder, nor a designated gateway, for the first mentioned CDR data. See s 56EK of the Competition and Consumer Act.

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

<sup>6</sup> Whether an accredited data recipient retains effective control over the data does not affect whether data is ‘disclosed’.

<sup>7</sup> Being a body corporate, body politic or individual.

# When can CDR data be disclosed to an overseas recipient?

- 8.17 When making an overseas disclosure of CDR data, an accredited data recipient must comply with Privacy Safeguard 8 in addition to each of the other privacy safeguards and CDR Rules that relate to disclosure of CDR data (to the extent they are applicable to the relevant disclosure).<sup>8</sup>
- 8.18 Privacy Safeguard 8 provides that an accredited data recipient must not disclose CDR data to a person located overseas unless one of the following four exceptions applies:
- the overseas recipient is an accredited person
  - the accredited data recipient takes reasonable steps to ensure the overseas recipient does not breach the privacy safeguards<sup>9</sup> and that the overseas recipient has a CDR policy in place in relation to the CDR data
  - the accredited data recipient reasonably believes the overseas recipient is bound by a law or scheme that is substantially similar to the privacy safeguards which can be enforced by the consumer, or
  - conditions specified in the CDR Rules for overseas disclosure are met. As there are currently no CDR Rules made specifically in relation to Privacy Safeguard 8, an accredited data recipient cannot currently rely on this exception.
- 8.19 The flow chart following outlines at a high level when an accredited data recipient may disclose CDR data to an overseas recipient, including by demonstrating the point at which the entity must consider other relevant privacy safeguards and CDR Rules, and relevant exceptions under Privacy Safeguard 8.

---

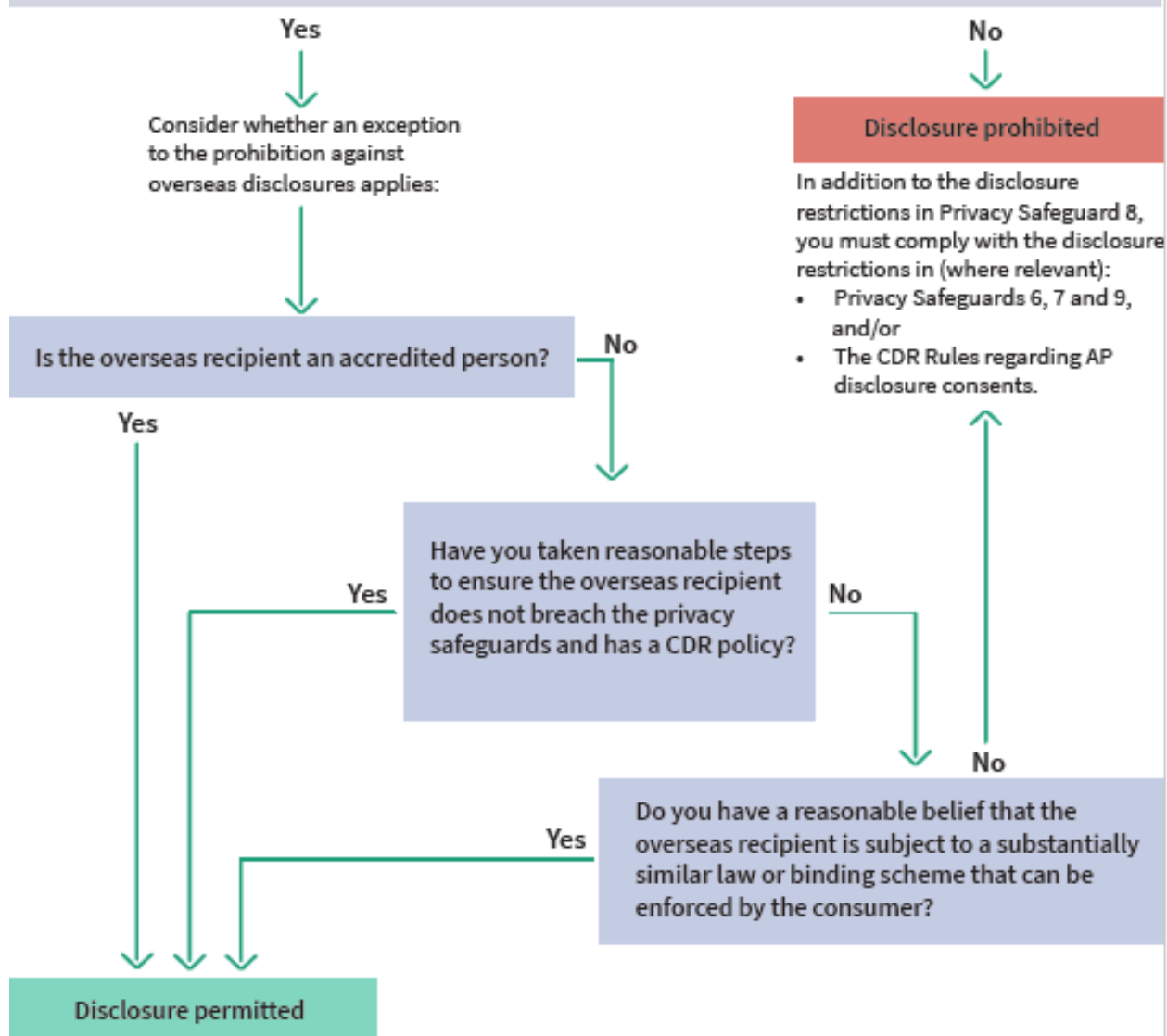
<sup>8</sup> Privacy Safeguard 6 and the CDR Rules relating to permitted disclosures (CDR Rules 7.5(1), 7.5(2), 7.5A, 7.6 and 7.7); Privacy Safeguard 7 and the CDR Rules relating to disclosure of CDR data for direct marketing (CDR Rules 7.5(3), 7.6 and 7.8); Privacy Safeguard 9 relating to disclosure of government related identifiers; CDR Rules relating to AP disclosure consents (e.g. CDR Rules 4.7B, 7.5(1)(ca), 7.5(1)(g) and 7.5A); and CDR Rules relating to outsourced service providers and CDR outsourcing arrangements (e.g. CDR Rules 7.5(1)(d) and 7.6).

<sup>9</sup> The relevant privacy safeguards are the privacy safeguard penalty provisions defined in s 56EU of the Competition and Consumer Act (Privacy Safeguards 3–13 inclusive, and the requirement to have a CDR policy in Privacy Safeguard 1).

## When can an accredited data recipient disclose CDR data to an overseas recipient?

Have you complied with the general disclosure requirements and restrictions (where relevant) in:

- Privacy Safeguard 6 (for permitted disclosures of CDR data)?
- Privacy Safeguard 7 (for direct marketing)?
- Privacy Safeguard 9 (for disclosure of government related identifiers)?
- The CDR Rules regarding AP disclosure consents (i.e. Rules 4.7B, 7.5(1)(ca), 7.5(1)(g) and 7.5A)?



## Exception 1 — Disclosing CDR data to an overseas recipient who is an accredited person

- 8.20 An accredited data recipient may disclose CDR data to an overseas recipient if the person is an accredited person.
- 8.21 This exception may be relied upon only where the accredited data recipient has obtained a disclosure consent from the consumer to disclose CDR data to the accredited overseas recipient.<sup>10</sup>
- 8.22 The term ‘accredited person’ is discussed in Chapter B (Key concepts).
- 8.23 The CDR 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.
- 8.24 The CDR Rules and the ACCC’s Accreditation Guidelines provide more information about the requirements and process for accreditation.
- 8.25 Accreditation is considered sufficient protection to ensure compliance with the privacy safeguards.<sup>11</sup>

## Exception 2 — Disclosing CDR data after taking ‘reasonable steps’ to ensure an overseas recipient does not breach the privacy safeguards

- 8.26 An accredited data recipient may disclose CDR data to an overseas recipient if they take reasonable steps to ensure that any act or omission by (or on behalf of) the overseas recipient will not breach the privacy safeguards.
- 8.27 The privacy safeguards apply to the acts or omissions as though the overseas recipient (or those who acted on behalf of the overseas recipient) was the accredited data recipient who disclosed the CDR data.<sup>12</sup>
- 8.28 Examples for persons acting on behalf of the overseas recipient could include employees, directors, officers, or subcontractors.

---

<sup>10</sup> Under the CDR Rules, an accredited data recipient may only disclose CDR data to an accredited person where they have a ‘disclosure consent’ from the consumer: see CDR Rule 1.10A. A disclosure consent is a consent given by a consumer for the accredited data recipient to disclose CDR data to an accredited person: in response to consumer data request (an ‘AP disclosure consent’), or for the purposes of direct marketing: CDR Rule 1.10A(1)(c). Note: An accredited data recipient is not permitted to disclose CDR data to an accredited person under an AP disclosure consent until the earlier of 1 July 2021 or a relevant data standard being made: see CDR Rule 7.5A.

For further information on disclosure consents, see [Chapter C \(Consent\)](#).

<sup>11</sup> Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019, section 1.348.

<sup>12</sup> Sections 56EK(2) and 56EK(3) of the Competition and Consumer Act. See also s 56AU of the Competition and Consumer Act.

## What are ‘reasonable steps’?

8.29 Reasonable steps would generally involve, at a minimum, that an accredited data recipient enters into an enforceable contractual arrangement with the overseas recipient that requires the overseas recipient to handle the CDR data in accordance with:

- the privacy safeguards, and
- the CDR Rules that relate to CDR outsourcing arrangements.<sup>13</sup>

8.30 Whether an accredited data recipient has taken reasonable steps to ensure the overseas recipient can comply with the CDR regime may include consideration of the following factors:

- the terms of the contract between the accredited data recipient and the overseas recipient
- steps taken by the accredited data recipient to monitor compliance with the contract
- the accredited data recipient’s relationship with the overseas recipient. More rigorous steps may be required when an entity discloses CDR data to an overseas recipient for the first time
- the nature of the overseas recipient, including the maturity of its processes and systems, and familiarity with CDR legislation (which may be derived from previous engagements with other CDR entities)
- the possible adverse consequences for a consumer if the CDR data is mishandled by the overseas recipient. More rigorous steps may be required as the risk of adversity increases
- the nature of the CDR data being disclosed. Where CDR data is sensitive in nature (and could, for example, cause financial or physical harm to a consumer if mishandled), it should be subject to more rigorous protections in the contractual arrangements
- existing technical and operational protections implemented by the overseas recipient to protect the CDR data (where these are not equivalent to the security requirements set out in Privacy Safeguard 12 and in Schedule 2 of the CDR Rules), and
- the practicability of taking protective steps, including time and cost involved. However, a CDR entity is not excused from ensuring that an overseas recipient is compliant with CDR legislation by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take particular steps will depend on whether the burden is excessive in all the circumstances.

---

<sup>13</sup> CDR Rules 1.10, 1.16(1), 7.5(1)(d) and 7.6. For more information on CDR outsourcing arrangements, please refer to [Chapter B \(Key concepts\)](#).

**Example**

YC Pty Ltd is an accredited person that provides banking services and products to customers. YC Pty Ltd seeks to engage a contractor located overseas, Analysed Data Services, in order to offer certain data analytics services to its customers using their payments transactions data.

YC Pty Ltd considers whether an exception under Privacy Safeguard 8 relating to overseas disclosures will apply.

Analysed Data Services is not an accredited person and is not subject to a law or scheme similar to that of the CDR regime.

Before disclosing CDR data to Analysed Data Services, YC Pty Ltd must therefore take reasonable steps to ensure Analysed Data Services complies with the privacy safeguards and has a CDR policy in place in relation to the CDR data.

YC Pty Ltd will remain accountable if Analysed Data Services mishandles the CDR data.

## Exception 3 — Disclosing CDR data where overseas recipient is subject to a substantially similar law

8.31 An accredited data recipient may disclose CDR data to an overseas recipient if:

- they reasonably believe the overseas recipient is bound by a law or binding scheme that is substantially similar to the privacy safeguards, and
- this can be enforced by the consumer.

### What is ‘reasonable belief’?

8.32 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 consumer will be able to enforce the protections provided by that law or binding scheme.

8.33 An accredited data recipient must have a reasonable basis for the belief, which is an objective test and not merely a genuinely held subjective belief. It is the responsibility of the entity to be able to justify its reasonable belief.

### What is a ‘law or binding scheme’?

8.34 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 regime, 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.

8.35 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’?

8.36 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.

8.37 Whether there is substantial similarity is a question of fact. Factors that may indicate that the overall effect is substantially similar, include:

- the law or scheme regulates the collection of consumer data in a comparable way
- the law or scheme requires the recipient to notify individuals about the collection of their consumer data
- the law or scheme requires the recipient to only use or disclose the consumer data for authorised purposes
- the law or scheme includes comparable data quality and data security standards, and
- the law or scheme includes a right to access and seek correction of consumer data

## When can a consumer enforce the protections?

8.38 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.

8.39 A range of mechanisms may satisfy those requirements, ranging from a regulatory body similar to the Office of the Australian Information Commissioner (the OAIC), to an accredited dispute resolution scheme, an independent tribunal, or a court with judicial functions and powers.

8.40 Factors that may be relevant in deciding whether the enforcement mechanism is an accessible and effective include whether the mechanism:

- is independent of the overseas recipient that is required by the law or binding scheme to comply with the consumer data protections
- is a body with authority to consider a breach of any of the consumer data protections in the law or binding scheme
- is accessible to an individual, for example, the existence of the scheme is publicly known, and can be accessed by individuals directly and without payment of any unreasonable charge
- has the power to make a finding that the overseas recipient is in breach of the law or binding scheme and to provide a remedy to the individual, and



- is required to operate according to principles of procedural fairness.

## When is an accredited data recipient accountable for the breaches by an overseas recipient?

- 8.41 Privacy Safeguard 8 provides that an accredited data recipient 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
  - the accredited data recipient 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 overseas recipient (or a person acting on behalf of the overseas recipient) breaches the privacy safeguards<sup>14</sup> and/or does not have a CDR policy.<sup>15</sup>
- 8.42 In these circumstances, for the purposes of Privacy Safeguard 8, the act or omission is taken to have been done by the accredited data recipient. The accredited data recipient is taken to have breached 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 breaches a relevant privacy safeguard, the accredited data recipient is accountable for that breach.<sup>16</sup>

**Risk point:** An accredited data recipient will be accountable under the CDR regime for the acts and omissions of an overseas recipient under Privacy Safeguard 8 in the circumstances set out above at 8.41 - 8.43.

**Privacy tip:** Accredited data recipients should maintain strong governance mechanisms, policies and procedures in relation to overseas disclosures of CDR data, including outsourcing arrangements. An accredited person should ensure that all contracts that aim to ensure compliance with the 'reasonable steps' exception in Privacy Safeguard 8 contain enforceable provisions that extend to the acts or omissions of subcontractors. Disclosing CDR data to overseas participants who are either accredited persons or a bound by a similar law to the CDR regime will reduce the risk profile for an accredited data recipient.

<sup>14</sup> The relevant privacy safeguards are those privacy safeguard penalty provisions in defined in s 56EU (privacy safeguards 3–13 inclusive, and the requirement to have a CDR policy in Privacy Safeguard 1).

<sup>15</sup> Section 56EK(2) of the Competition and Consumer Act.

<sup>16</sup> See also s 56AU of the Competition and Consumer Act. Please also note the similar liability position under CDR Rule 7.6 relating to outsourced service providers where the use or disclosure of CDR data by the outsourced service provider (or by one of its subcontractors) is taken to be the use or disclosure of the accredited data recipient whether or not in accordance with the CDR outsourcing arrangement between the parties.

- 8.44 There are also other conditions in the CDR regulatory framework that affect when an accredited data recipient is liable when making an overseas disclosure:
- Section 56AU(2) of the Competition and Consumer Act provides that acts done by or in relation to another person who is acting on behalf of a CDR entity, within the person's actual or apparent authority, are taken to have also been done in relation to the CDR entity,<sup>17</sup> and
  - CDR Rule 7.6(2) provides that an accredited data recipient will be liable for any use or disclosure of CDR data it disclosed to an outsourced service provider (or that the outsourced service provider has disclosed to its own subcontractors).

## How does Privacy Safeguard 8 interact with the other privacy safeguards?

### Privacy Safeguard 6

- 8.45 In addition to Privacy Safeguard 8, an accredited data recipient should consider Privacy Safeguard 6 when determining whether to disclose CDR data to an overseas recipient.
- 8.46 This includes whether the disclosure is a permitted disclosure for the purposes of Privacy Safeguard 6 and also whether the accredited data recipient will need to comply with CDR outsourcing arrangements relating to outsourced service providers. See [Chapter 6 \(Privacy Safeguard 6\)](#).

### Privacy Safeguard 7

- 8.47 In addition to Privacy Safeguard 8, an accredited data recipient should consider Privacy Safeguard 7 where they are seeking to disclose CDR data to engage in permitted direct marketing activities. See [Chapter 7 \(Privacy Safeguard 7\)](#).

### Privacy Safeguard 9

- 8.48 In addition to Privacy Safeguard 8, an accredited data recipient should also consider Privacy Safeguard 9 where CDR data it is seeking to disclose to an overseas recipient contains government identifiers. See [Chapter 9 \(Privacy Safeguard 9\)](#).

---

<sup>17</sup> See also s 56AU(1), which provides that the conduct of agents of a CDR entity are attributable to the CDR entity.

## Chapter 9:

# Privacy Safeguard 9 —

## Adoption or disclosure of government related identifiers by accredited data recipients

Version 3.0, June 2021

# Contents

<b>Key points</b>	<b>3</b>
<b>What does Privacy Safeguard 9 say?</b>	<b>3</b>
<b>Why is it important?</b>	<b>3</b>
<b>Who does Privacy Safeguard 9 apply to?</b>	<b>4</b>
<b>How Privacy Safeguard 9 interacts with the Privacy Act</b>	<b>4</b>
<b>Meaning of government related identifier</b>	<b>5</b>
'Identifiers'	5
'Government related identifier'	5
<b>Adopting, using or disclosing a government related identifier</b>	<b>6</b>
'Adopt'	6
'Use'	7
'Disclose'	7
Exceptions	7
<b>Interaction with other privacy safeguards</b>	<b>8</b>
Privacy Safeguards 3 and 4	8

## Key points

- Privacy Safeguard 9 sets out a prohibition on accredited data recipients of CDR data from adopting, using or disclosing government related identifiers unless required or authorised:
  - under another Australian law other than the consumer data rules (CDR Rules) or a court/tribunal order, or
  - as prescribed by regulations made under the *Privacy Act 1988* (Privacy Act).
- A government related identifier is a number, letter or symbol, or a combination of any or all of those things, that has been assigned by certain government entities and is used to identify the individual or to verify the identity of the individual.
- Privacy Safeguard 9 only concerns government related identifiers of a consumer who is an individual.
- An individual cannot consent to the adoption, use or disclosure of their government related identifier.

## What does Privacy Safeguard 9 say?

- 9.1 Where CDR data includes a government related identifier, Privacy Safeguard 9 prohibits an accredited data recipient of CDR data from:
- adopting the government related identifier as its own identifier of the consumer, or otherwise using the government related identifier, or
  - disclosing CDR data which includes the government related identifier
- unless authorised or required by or under:
- an Australian law other than the CDR Rules or in a court/tribunal order, or
  - 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 made under the Privacy Act.
- 9.2 Privacy Safeguard 9 only concerns government related identifiers of a consumer of the CDR data who is an individual.
- 9.3 In this Chapter, a government related identifier of a CDR consumer included with the 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 consumer may not agree with or expect.

## Who does Privacy Safeguard 9 apply to?

9.5 Privacy Safeguard 9 applies to accredited data recipients of CDR data. It does not apply to data holders or designated gateways. However, data holders and designated gateways must ensure that they are adhering to their obligations under the Privacy Act and APP 9 in relation to government related identifiers of individuals.

## 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 and the APPs.<sup>1</sup>

9.7 APP 9 prohibits an APP entity from adopting, using or disclosing a government related identifier unless an exception applies.

CDR entity	Privacy protections that apply in the CDR context
<b>Accredited data recipient</b>	<p><b>Privacy Principle 9</b></p> <p>For accredited data recipients of a consumer's CDR data, Privacy Safeguard 9 applies to the handling of government related identifiers contained in that CDR data.<sup>2</sup></p> <p>APP 9 does not apply in relation to that CDR data.<sup>3</sup></p>
<b>Designated gateway</b>	<p><b>APP 9</b></p> <p>Privacy Safeguard 9 does not apply to a designated gateway.</p>
<b>Data holder</b>	<p><b>APP 9</b></p> <p>Privacy Safeguard 9 does not apply to a data holder.</p>

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

<sup>2</sup> Privacy Safeguard 9 applies from the point when the accredited person becomes an accredited data recipient of the CDR data. An accredited person becomes an accredited data recipient for CDR data when:

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

<sup>3</sup> The APPs do not apply to an accredited data recipient of CDR data, in relation to that CDR data - s 56EC(4)(a) of the Competition and Consumer Act. However, s 56EC(4) does not affect how the APPs apply to accredited persons and accredited data recipients who are APP entities, in relation to the handling of personal information outside the CDR system. (Note: Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See s 6E(1D) of the Privacy Act.) Section 56EC(4) also does not affect how the APPs apply to an accredited person who does not become an accredited data recipient of the CDR data (other than for Privacy Safeguards 1 – 4). See s 56EC(5)(aa) of the Competition and Consumer Act.

## Meaning of government related identifier

- 9.8 ‘Government related identifier’ has the meaning given to it in the Privacy Act.<sup>4</sup>
- 9.9 Privacy Safeguard 9 only concerns government related identifiers of consumers of the CDR data who are individuals.
- 9.10 For example, the Australian Business Number (ABN) of a body corporate would not be subject to Privacy Safeguard 9. (Note that the ABN of an individual is not an ‘identifier’ under s 6(1) of the Privacy Act).
- 9.11 However, government related identifiers of individuals who are sole traders that manage a small business or of partners in a partnership will be captured by Privacy Safeguard 9.

### ‘Identifiers’

- 9.12 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.
- 9.13 The following are explicitly excluded from the definition of identifier:
- an individual’s name
  - an individual’s ABN, and
  - anything else prescribed by the regulations made under the Privacy Act.<sup>5</sup> 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’

- 9.14 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 agency<sup>6</sup>
  - a State or Territory authority<sup>7</sup>
  - 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,<sup>8</sup> or a State contract,<sup>9</sup> acting in its capacity as contracted service provider for that contract.

---

<sup>4</sup> Sections 56EL(1)(b) and 56EL(2)(b) of the Competition and Consumer Act.

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

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

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

<sup>8</sup> ‘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.

<sup>9</sup> ‘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 The following are examples of government related identifiers:

- Medicare numbers
- Centrelink reference numbers<sup>10</sup>
- driver licence numbers issued by State and Territory authorities, and
- Australian passport numbers.

9.16 Some government related identifiers are also regulated by other laws that restrict the way entities can collect, use or disclose the particular identifier and related personal information. Examples include tax file numbers and individual healthcare identifiers.<sup>11</sup> These other laws apply in addition to Privacy Safeguard 9, i.e. a breach of the *Privacy (Tax File Number) Rule 2015* may be both an interference with the privacy of an individual under the Privacy Act and as a breach of Privacy Safeguard 9, as well as a potential offence under the *Taxation Administration Act 1953*.

## Adopting, using or disclosing a government related identifier

9.17 An accredited data recipient must not adopt a CDR consumer government related identifier as its own identifier of the consumer, or otherwise use a government related identifier, unless an exception applies.<sup>12</sup> In addition, an accredited data recipient must not include the government related identifier when it discloses CDR data unless an exception applies.

### ‘Adopt’

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

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

---

<sup>10</sup> Note that under regulations 17 and 18 of the *Privacy Regulation 2013*, certain prescribed organisations are permitted to use or disclose certain identifiers (including Centrelink reference numbers) in specific circumstances.

<sup>11</sup> For more information about the legislative regimes, visit the OAIC’s Tax File Numbers page and Healthcare Identifiers page <https://www.oaic.gov.au>.

<sup>12</sup> Section 56EL(1) of the Competition and Consumer Act. 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.



**Example**

Stephanie, an accountant and accredited person, receives a consumer's driver licence number when it is disclosed to Stephanie in response to a consumer data request. Stephanie then uses the identifier to refer to that consumer in her own identification system.

As Stephanie has adopted a CDR consumer government related identifier, she may be in breach of Privacy Safeguard 9.

**‘Use’**

9.20 The term ‘use’ is discussed in [Chapter B \(Key concepts\)](#).

9.21 Generally, an entity uses CDR data when it handles and manages that information within its effective control. Examples include:

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

**‘Disclose’**

9.22 The term ‘disclose’ is discussed in [Chapter B \(Key concepts\)](#).

9.23 An accredited data recipient or designated gateway ‘discloses’ CDR data when it makes it accessible or visible to others outside the entity.<sup>13</sup>

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

9.24 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.<sup>14</sup>

9.25 The meaning of ‘required or authorised by or under an Australian law or a court/tribunal order’ is discussed in [Chapter B \(Key concepts\)](#).

9.26 The Australian law or court/tribunal order should specify:

- a particular government related identifier
- the entities or classes of entities permitted to adopt, use or disclose it, and
- the particular circumstances in which they may adopt, use or disclose it.

<sup>13</sup> Information will be ‘disclosed’ under the CDR regime regardless of whether an entity retains effective control over the data.

<sup>14</sup> Section 56EL(1)(c) of the Competition and Consumer Act.

## Prescribed by regulations

9.27 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.<sup>15</sup>

9.28 Regulations may be made under the Privacy Act to prescribe these matters.<sup>16</sup>

## Interaction with other privacy safeguards

### Privacy Safeguards 3 and 4

9.29 Privacy Safeguard 9 applies to the adoption, use and disclosure of government related identifiers. It does not specifically address the *collection* of government related identifiers. However, if an accredited person collects a government related identifier that is considered to be CDR data, they must comply with other privacy safeguards, including [Privacy Safeguard 3](#) and [Privacy Safeguard 4](#). These privacy safeguards are discussed in Chapters 3 and 4 respectively.

---

<sup>15</sup> Section 56EL(1)(d) of the Competition and Consumer Act and APP 9.3.

<sup>16</sup> See the Federal Register of Legislation <https://www.legislation.gov.au> for up-to-date versions of regulations made under the Privacy Act.

## Chapter 10:

# Privacy Safeguard 10 —

## Notifying of the disclosure of CDR data

Version 3.0, June 2021

# Contents

<b>Key points</b>	<b>3</b>
<b>What does Privacy Safeguard 10 say?</b>	<b>3</b>
<b>Why is it important?</b>	<b>3</b>
<b>Who does Privacy Safeguard 10 apply to?</b>	<b>3</b>
<b>How Privacy Safeguard 10 interacts with the Privacy Act</b>	<b>4</b>
<b>Who must be notified?</b>	<b>4</b>
<b>How must notification be given?</b>	<b>5</b>
<b>When must notification be given?</b>	<b>6</b>
<b>What matters must be included in the notification?</b>	<b>7</b>
What CDR data was disclosed	7
When the CDR data was disclosed	8
To whom the CDR data was disclosed	8
<b>Other notification requirements under the CDR Rules</b>	<b>9</b>
<b>Disclosure to a designated gateway</b>	<b>10</b>
<b>Interaction with other Privacy Safeguards</b>	<b>10</b>

## Key points

- Where a data holder or accredited data recipient of a consumer's CDR data discloses that data to an accredited person, they must notify the consumer by updating the consumer dashboard.
- The consumer data rules (CDR 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 CDR Rules to disclose CDR data, they must notify the consumer by taking the steps identified in the CDR Rules.<sup>1</sup>
- 10.2 Where an accredited data recipient of a consumer's CDR data discloses CDR data, they must notify that consumer by taking the steps identified in the CDR Rules.<sup>2</sup>
- 10.3 The notification must:
- be given to those consumers that the CDR Rules require to be notified
  - cover the matters set out in the CDR Rules, and
  - be given at or before the time specified in the CDR Rules.
- 10.4 Under CDR Rule 7.9, data holders and accredited data recipients of a consumer's CDR data must notify the consumer by updating each relevant consumer dashboard to include certain matters as set out in that Rule as soon as practicable after CDR data is disclosed to an accredited person.

## Why is it important?

- 10.5 Notification of disclosure of CDR data is an integral element of the CDR regime, as it provides confirmation to consumers that their CDR data has been disclosed in response to a consumer data request.
- 10.6 This ensures consumers are informed when their CDR data is disclosed and builds trust between consumers, data holders and accredited data recipients.

## Who does Privacy Safeguard 10 apply to?

- 10.7 Privacy Safeguard 10 applies to data holders and accredited data recipients of CDR data. It does not apply to designated gateways.

---

<sup>1</sup> Section 56EM(1) of the Competition and Consumer Act. For further information on 'required or authorised to use or disclose CDR data under the CDR Rules', refer to [Chapter B \(Key concepts\)](#).

<sup>2</sup> Section 56EM(2) of the Competition and Consumer Act.

# How Privacy Safeguard 10 interacts with the Privacy Act

## *For data holders*

- 10.8 Data holders must comply with Privacy Safeguard 10 when they are required or authorised to disclose CDR data under the CDR Rules.
- 10.9 There is no corresponding obligation under the *Privacy Act 1988* (the Privacy Act) or the Australian Privacy Principles (APPs) to notify an individual of the disclosure of their personal information.
- 10.10 However, APP 5 will continue to apply in relation to the notification of the collection of CDR data that is also personal information.<sup>3</sup>

## *For accredited data recipients*

- 10.11 For an accredited data recipient of a consumer's CDR data, Privacy Safeguard 10 applies whenever they disclose that consumer's data.
- 10.12 The APPs do not apply to an accredited data recipient of CDR data, in relation to that CDR data.<sup>4</sup>

# Who must be notified?

## *For data holders*

- 10.13 The data holder must notify each of the consumers for the CDR data that has been disclosed.<sup>5</sup>
- 10.14 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 each of 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.<sup>6</sup>

---

<sup>3</sup> For example, the obligations in APP 5.2 (f), (i) and (j) to notify individuals of the situations in which their personal information may be disclosed in future.

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

<sup>5</sup> Section 56EM(1)(b) of the Competition and Consumer Act and CDR Rule 7.9(1).

<sup>6</sup> CDR Rule 7.9 and clause 4.14(4) of Schedule 3 to the CDR Rules. Clause 4.14(4) of Schedule 3 provides that the data holder may decline to provide a relevant account holder with a consumer dashboard or update the consumer dashboard if the data holder considers it necessary to do either in order to prevent physical or financial harm or abuse.

- 10.15 This exception to notification is to accommodate existing procedures a data holder may have to protect consumers, for example particular arrangements relating to consumers that may be experiencing family violence.
- 10.16 Where the CDR data disclosed relates to an account with a secondary user,<sup>7</sup> and the secondary user is also a consumer for the CDR data,<sup>8</sup> the data holder must notify both the account holder and secondary user.<sup>9</sup>
- 10.17 Where the CDR data disclosed relates to a non-individual consumer or is in relation to a partnership account, the data holder must notify the relevant nominated representative.<sup>10</sup>

*For accredited data recipients*

- 10.18 The accredited data recipient must notify the consumer who provided the disclosure consent.<sup>11</sup>

## How must notification be given?

*For data holders*

- 10.19 A data holder must provide the notification by updating the consumer dashboard for a consumer (and, if applicable, the dashboard of the other joint account holder/s)<sup>12</sup> to include the matters discussed in paragraphs 10.31 to 10.42 as soon as practicable after CDR data relating to that consumer is disclosed.<sup>13</sup>

---

<sup>7</sup> A person is a secondary user for an account with a data holder if the person has ‘account privileges’ in relation to the account, and the account holder has given the data holder an instruction to treat the person as a secondary user for the purposes of the CDR Rules (CDR Rule 1.7). ‘Account privileges’ for the banking sector are defined in clause 2.2 of Schedule 3 to the CDR Rules.

<sup>8</sup> For a person to be a ‘CDR consumer’ that person must be identifiable, or ‘reasonably identifiable’, from the CDR data or other information held by the relevant entity (i.e. the data holder, accredited data recipient, or person holding data on their behalf) (s 56AI(3)(c) of the Competition and Consumer Act). See Chapter B (Key concepts) of the CDR Privacy Safeguard Guidelines for the full meaning of CDR consumer.

<sup>9</sup> Any provisions in the CDR Rules which impose obligations on data holders in relation to secondary users only apply to initial data holders in respect of NAB, CBA, ANZ, Westpac branded products on and from 1 November 2021 (and for all other data holders, on and from 1 November 2022): see cl 6.7 of Schedule 3 to the CDR Rules.

<sup>10</sup> A ‘nominated representative’ is the individual nominated by the non-individual consumer under CDR Rules 1.13(c)(i) or 1.13(d)(i) who is able to give, amend and manage authorisations to disclose CDR data on behalf of the non-individual consumer. There may be more than one nominated representative.

Note that any provisions in the CDR Rules which impose obligations on data holders in relation to consumers that are not individuals, nominated representatives or partnerships only apply to initial data holders in respect of NAB, CBA, ANZ, Westpac branded products on and from 1 November 2021 (and for all other data holders, on and from 1 November 2022): see cl 6.7 of Schedule 3 to the CDR Rules.

<sup>11</sup> A disclosure consent is a consent given by a consumer for the accredited data recipient to disclose CDR data to an accredited person: in response to consumer data request (an ‘AP disclosure consent’), or for the purposes of direct marketing: CDR Rule 1.10A(1)(c). For further information, see Chapter C (Consent).

<sup>12</sup> Where the CDR data disclosed relates to a joint account, the data holder must provide each relevant account holder with a consumer dashboard, and notify each of the joint account holders by updating their consumer dashboards to include those same matters as soon as practicable after the CDR data is disclosed. However, the data holder may decline to provide a relevant account holder with a consumer dashboard or update the consumer dashboard if the data holder considers it necessary to do either in order to prevent physical or financial harm or abuse. See clause 4.14 of Schedule 3 to the CDR Rules.

<sup>13</sup> CDR Rule 7.9.

- 10.20 The data holder's consumer dashboard is an online service that must be provided by a data holder to each consumer (and, if applicable, the other joint account holder/s)<sup>14</sup> where a consumer data request has been made on their behalf by an accredited person. Data holders must include within the dashboard certain details of each authorisation to disclose CDR data that has been given by the consumer.<sup>15</sup>
- 10.21 Further guidance about the data holder's consumer dashboard is set out in [Chapter B \(Key concepts\)](#) and the [Guide to privacy for data holders](#).

*For accredited data recipients*

- 10.22 An accredited data recipient must provide the notification by updating the consumer dashboard for the consumer who provided the disclosure consent.<sup>16</sup>
- 10.23 The accredited data recipient's consumer dashboard is an online service that must be provided by an accredited data recipient to each consumer who has provided a consent in relation to their CDR data. Accredited data recipients must include in the dashboard certain details of each consent that has been given by the consumer.<sup>17</sup>
- 10.24 Where an accredited data recipient disclosed CDR data that was collected on behalf of another accredited person (the 'principal') under a CDR outsourcing arrangement, only the principal needs to notify the relevant consumer/s by updating the relevant dashboard.<sup>18</sup>
- 10.25 Further guidance about the accredited data recipient's consumer dashboard is set out in [Chapter B \(Key concepts\)](#) and [Chapter C \(Consent\)](#).

## When must notification be given?

- 10.26 Data holders and accredited data recipients must notify the consumer/s as soon as practicable after the CDR data is disclosed.<sup>19</sup>
- 10.27 As a matter of best practice, notification should generally occur in as close to real time as possible (for example, in relation to ongoing disclosure, as close to the time of first disclosure as possible).
- 10.28 The test of practicability is an objective test. It is the responsibility of the data holder or accredited data recipient to be able to justify any delay in notification.

---

<sup>14</sup> Where the CDR data disclosed relates to a joint account, the data holder must provide each relevant account holder with a consumer dashboard, except where the data holder considers it necessary to decline to provide a relevant account holder with a dashboard in order to prevent physical or financial harm or abuse. See clause 4.14(4) of Schedule 3 to the CDR Rules.

<sup>15</sup> The requirements are outlined in CDR Rule 1.15, and include requirements to provide details of the CDR data to which the authorisation relates and when the authorisation will expire.

<sup>16</sup> A disclosure consent is a consent given by a consumer for the accredited data recipient to disclose CDR data to an accredited person: in response to consumer data request (an 'AP disclosure consent'), or for the purposes of direct marketing: CDR Rule 1.10A(1)(c). For further information, see Chapter C (Consent).

<sup>17</sup> The requirements are outlined in CDR Rule 1.14, and include requirements to provide details of the CDR data to which each consent relates and when each consent will expire.

<sup>18</sup> CDR Rule 1.16(2)(a). For information on 'CDR outsourcing arrangements', see [Chapter B \(Key concepts\)](#).

<sup>19</sup> CDR Rules 7.9(1) and 7.9(2).



10.29 In determining what is ‘as soon as practicable’, data holders and accredited data recipients may take the following factors into account:

- the time and cost involved, in combination with other factors
- technical matters, and
- the individual needs of the consumer (for example, any additional steps required to make the content accessible).

10.30 Data holders and accredited data recipients are not excused from providing prompt notification by reason only that it would be inconvenient, time consuming, or costly to do so.

## What matters must be included in the notification?

10.31 The minimum matters that must be included by data holders and accredited data recipients in the notification, and provided via the consumer’s dashboard are:

- what CDR data was disclosed
- when the CDR data was disclosed, and
- the accredited person to whom the CDR data was disclosed.<sup>20</sup>

10.32 Data holders and accredited data recipients should provide information about these matters clearly and simply, but also with enough specificity to be meaningful for the consumer. How much information is required may differ depending on the circumstances.

10.33 Guidance on each of the minimum matters follows.

**Risk point:** Consumers may not read or understand a notification if it is complex.

**Privacy tip:** Data holders and accredited data recipients should ensure that the notification is as simple and easy to understand as possible. To do this, entities should consider a range of factors when formulating a notification, such as:

- the audience
- the language used (including the level of detail), and
- the presentation of the information (e.g. layout, format and any visual aids used). For more complex notifications, entities could consider providing a condensed summary of key matters in the notification and linking to a more comprehensive summary or, where it may assist the consumer, a full log of disclosure.

## What CDR data was disclosed

10.34 Data holders and accredited data recipients must notify the consumer of what CDR data was disclosed.

---

<sup>20</sup> CDR Rules 7.9(1) and 7.9(2). The accredited person needs to be identified in accordance with any entry on the Register of Accredited Persons specified as being for that purpose.

10.35 In doing so, the entity should ensure the CDR data is described in a manner that allows the consumer to easily understand what CDR data was disclosed.

10.36 Data holders and accredited data recipients must use the Data Language Standards when describing what CDR data was disclosed.<sup>21</sup> This will aid consumer comprehension by ensuring consistency between how CDR data was described in the authorisation/consent-seeking processes and how CDR data is described in the consumer dashboard.

## When the CDR data was disclosed

10.37 Data holders and accredited data recipients must notify the consumer of when the CDR data was disclosed.

*‘One-off’ disclosure:*<sup>22</sup>

10.38 The entity should include the date on which the CDR data was disclosed.

*Ongoing disclosure:*<sup>23</sup>

10.39 The entity should, at a minimum, include the date range in which CDR data will be disclosed, with the starting date being the date on which the CDR data was first disclosed, and the end date being the date on which the entity will make its final disclosure. This end date might not necessarily be the same as the date that the authorisation (in the case of a data holder) or disclosure consent (in the case of an accredited data recipient) expires.

10.40 Where the entity is unsure of the end date they may put the date the authorisation or disclosure consent expires, but must update the end date as soon as practicable after it becomes known.<sup>24</sup>

## To whom the CDR data was disclosed

10.41 In its notification to the consumer, the entity must indicate the accredited person to whom the CDR data was disclosed.

10.42 The accredited person must be described in accordance with any entry on the Register of Accredited Persons specified as being for that purpose.<sup>25</sup>

---

<sup>21</sup> The Data Language Standards are contained within the Consumer Experience Guidelines. They provide descriptions of the types of data to be used by data holders and accredited data recipients when making and responding to requests. Adherence to the Data Language Standards is mandatory and will help ensure there is a consistent interpretation and description of the consumer data that will be shared in the CDR regime. See s 56FA of the Competition and Consumer Act and CDR Rule 8.11.

<sup>22</sup> For data holders, this is where the accredited person made a consumer data request on behalf of the consumer for a collection of CDR data on a single occasion. For accredited data recipients, this is where the consumer’s disclosure consent applies for the disclosure of CDR data on a single occasion.

<sup>23</sup> For data holders, this is where the accredited person made a consumer data request on behalf of the consumer for collection of CDR data over a specified period of time. For accredited data recipients, this is where the consumer’s disclosure consent applies for the disclosure of CDR data over a specified period of time.

<sup>24</sup> CDR Rules 4.19 and 4.27 require data holders and accredited data recipients (respectively) to update the consumer dashboard as soon as practicable after the information required to be contained on the dashboard changes.

<sup>25</sup> CDR Rule 7.9(2)(c).

**Example**

Bank Belle, a data holder, receives a consumer data request on 1 July 2020 from Watson and Co, an accredited person, to disclose Zoe's transaction details.

Bank Belle asks Zoe on 1 July 2020 to authorise the disclosure of her transaction details to Watson and Co for the sharing period specified in the consumer data request (i.e. 1 July 2020 to 1 January 2021).

Upon receiving Zoe's authorisation, Bank Belle discloses Zoe's transaction details to Watson and Co on 1 July 2020.

Bank Belle updates Zoe's consumer dashboard on 1 July 2020 to include the following notification statement:

*We shared your transaction details with Watson and Co on 01.07.20. We'll continue to share your transaction details with Watson and Co until 01.01.21.*

The above statement is an example of how Bank Belle, a data holder, could notify Zoe of the disclosure of her CDR data in accordance with CDR Rule 7.9(1).

## Other notification requirements under the CDR Rules

### *For data holders*

10.43 In addition to the Privacy Safeguard 10 notification requirements in relation to disclosure, the data holder must update a consumer's dashboard as soon as practicable after the information required to be contained on the dashboard changes.<sup>26</sup>

### *For accredited data recipients*

10.44 In addition to the Privacy Safeguard 10 notification requirements in relation to disclosure, there are other notification requirements relating to consent and collection that must be complied with by an accredited data recipient:<sup>27</sup>

- providing CDR receipts to the consumer (CDR Rule 4.18)
- notification requirements where certain consents expire or are amended (CDR Rules 4.18A, 4.18B and 4.18C)

---

<sup>26</sup> CDR Rule 4.27.

<sup>27</sup> For an accredited data recipient who collected CDR data on behalf of a principal in a CDR outsourcing arrangement, note the effect of CDR Rule 1.7(5) which provides that, in the CDR Rules, 'unless the contrary intention appears, a reference to an accredited person making a consumer data request, collecting CDR data, obtaining consents, providing a consumer dashboard, or using or disclosing CDR data does not include a reference to an accredited person doing those things on behalf of a principal in its capacity as the provider in an outsourced service arrangement, in accordance with the arrangement'.

For information on 'CDR outsourcing arrangements', see [Chapter B \(Key concepts\)](#).

- general obligation to update the consumer dashboard (CDR Rule 4.19)
- ongoing notification requirements for consents to collect and use (CDR Rule 4.20), and
- notifying the consumer of the collection of their CDR data under Privacy Safeguard 5 (CDR Rule 7.4).

10.45 For further information regarding the notification requirements for consent, see [Chapter C \(Consent\)](#). For further information regarding the notification requirement for collection, see [Chapter 5 \(Privacy Safeguard 5\)](#).

## Disclosure to a designated gateway

**Note:** *There are currently no designated gateways in the banking sector.*

10.46 Privacy Safeguard 10 applies where a data holder or accredited data recipient discloses CDR data to a designated gateway as required or authorised under the CDR Rules.<sup>28</sup>

10.47 There are currently no CDR Rules made for this circumstance.

## Interaction with other Privacy Safeguards

10.48 Data holders and accredited data recipients must comply with Privacy Safeguard 1 by taking reasonable steps to implement practices, procedures and systems that will ensure they comply with the CDR regime, including Privacy Safeguard 10. See [Chapter 1 \(Privacy Safeguard 1\)](#).

10.49 Privacy Safeguard 11 mandates the steps which data holders and accredited data recipients must take to advise a consumer where they have disclosed CDR data that was incorrect. See [Chapter 11 \(Privacy Safeguard 11\)](#).

---

<sup>28</sup> CDR Rules may be made in relation to the notification requirements for that disclosure.

# Chapter 11:

# Privacy Safeguard 11 —

# Quality of CDR data

Version 3.0, June 2021

# Contents

<b>Key points</b>	<b>3</b>
<b>What does Privacy Safeguard 11 say?</b>	<b>3</b>
<b>Why is it important?</b>	<b>4</b>
<b>Who does Privacy Safeguard 11 apply to?</b>	<b>4</b>
How Privacy Safeguard 11 interacts with the Privacy Act	4
<b>What are the quality considerations?</b>	<b>5</b>
Accurate	6
Up to date	7
Complete	7
<b>Taking reasonable steps to ensure the quality of CDR data</b>	<b>8</b>
When must an entity take reasonable steps?	8
What constitutes ‘reasonable steps’?	9
Examples of reasonable steps	9
<b>Advising a consumer when disclosed CDR data is incorrect</b>	<b>10</b>
In what circumstances must an entity disclose corrected CDR data to the original recipient?	13
<b>Record keeping requirements</b>	<b>13</b>
<b>How does Privacy Safeguard 11 interact with the other privacy safeguards?</b>	<b>14</b>
Privacy Safeguard 5	14
Privacy Safeguard 10	14
Privacy Safeguard 12	15
Privacy Safeguard 13	15

## Key points

- Privacy Safeguard 11, together with consumer data rule (CDR Rule) 7.10, sets out obligations for data holders and accredited data recipients of CDR data to:
  - ensure the quality of disclosed consumer data right (CDR) data
  - inform consumers in the event incorrect CDR data is disclosed, and
  - disclose corrected CDR data to the original recipient where requested by the affected 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 CDR Rules, and
- accredited data recipients of a consumer's CDR data who are disclosing that consumer's CDR data when required or authorised under the CDR Rules

to:

- take reasonable steps to ensure that the CDR data is, having regard to the purpose for which it is held, accurate, up to date and complete
- advise the consumer in accordance with the CDR Rules if they become aware that the CDR data disclosed was not accurate, up to date and complete when disclosed, and
- where incorrect CDR data was previously disclosed, comply with a request by the consumer to disclose corrected CDR data to the original recipient in accordance with the CDR Rules.<sup>1</sup>

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

11.3 CDR Rule 7.10 requires data holders and accredited data recipients of a consumer's CDR data who have disclosed CDR data that was incorrect at the time of disclosure to provide the consumer with a written notice by electronic means that identifies:

- the accredited person
- the CDR data that was incorrect, and
- the date of the disclosure.

11.4 The notice must also advise the consumer that they can request the entity to disclose the corrected data to the accredited person (to whom the incorrect CDR data was previously disclosed). The data holder or accredited data recipient must disclose the corrected data if the consumer requests them to do so.

---

<sup>1</sup> Both the consumer's request, and the actions taken by the CDR participant to correct the data under Privacy Safeguard 11, must be in accordance with the CDR Rules – see s 56EN(4). Further, the requirement to disclose corrected CDR data to the recipient under Privacy Safeguard 11 does not apply in circumstances specified in the CDR Rules (see section s 56EN 4A of the Competition and Consumer Act). However, no such Rules have been made.

- 11.5 This notice must be provided to the consumer as soon as practicable, but no more than five business days after becoming aware that some or all of the disclosed data was incorrect.

## Why is it important?

- 11.6 The objective of Privacy Safeguard 11 is to ensure consumers have trust in and control over the quality of their CDR data disclosed as part of the CDR regime.
- 11.7 Privacy Safeguard 11 does this by ensuring entities are disclosing CDR data that is accurate, up to date and complete, and by giving consumers control over their data by allowing them to require entities to correct any inaccuracies in their data after it is shared.
- 11.8 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?

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

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

## How Privacy Safeguard 11 interacts with the Privacy Act

- 11.10 It is important to understand how Privacy Safeguard 11 interacts with the *Privacy Act 1988* (the Privacy Act) and Australian Privacy Principles (APPs).<sup>2</sup>
- 11.11 APP 10 requires APP entities to take reasonable steps to ensure the quality of personal information in certain circumstances.
- 11.12 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.
- 11.13 Although Privacy Safeguard 11 applies only in relation to the *disclosure* of CDR data, good practices and procedures by data holders that ensure the quality of personal information collected, used and disclosed under APP 10 will also help to ensure the quality of CDR data that is *disclosed under the CDR regime*.
- 11.14 Data holders should also be aware that APP 13 (correction of personal information) obligations under the Privacy Act continue to apply in certain circumstances. For example, where the data holder becomes aware of incorrect CDR data, but the data holder has not disclosed that data to an accredited data recipient, the data holder must continue to comply with APP 13 and take steps that are reasonable to correct CDR data.<sup>3</sup>

---

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

<sup>3</sup> See [Chapter 13 \(Correction of personal information\)](#) of the OAIC's APP Guidelines for further information.



CDR entity	Privacy protections that apply in the CDR context
<b>Accredited data recipient</b>	<p><b>Privacy Safeguard 11</b></p> <p>For accredited data recipients of a consumer's CDR data, Privacy Safeguard 11 applies to the disclosure of CDR data and for corrections of that data once disclosed.<sup>4</sup></p> <p>APP 10 does not apply to in relation to that CDR data.<sup>5</sup></p>
<b>Data holder</b>	<p><b>Privacy Safeguard 11, APP 10 and APP 13</b></p> <p>Privacy Safeguard 11 applies instead of APP 10 to <i>disclosures</i> of CDR data that are required or authorised under the CDR Rules.</p> <p>APP 10 continues to apply to CDR data that is also personal information in all other circumstances, including:</p> <ul style="list-style-type: none"> <li>the collection and use of CDR data, and</li> <li>disclosures of CDR data outside the CDR regime.</li> </ul> <p><b>Note:</b> APP 13 continues to apply when the data holder becomes aware of incorrect CDR data, but the data has not been disclosed to an accredited data recipient.<sup>6</sup></p>
<b>Designated gateway</b>	<p><b>APP 10</b></p> <p>Privacy Safeguard 11 does not apply to a designated gateway.</p>

## What are the quality considerations?

11.15 The three quality considerations under Privacy Safeguard 11 are that data should be 'accurate, up to date and complete'. Whether or not CDR data is accurate, up to date and complete must be determined with regard to the purpose for which it is held. 'Held' is discussed in [Chapter B \(Key concepts\)](#).

<sup>4</sup> Privacy Safeguard 11 applies from the point when the accredited person becomes an accredited data recipient of the CDR data. An accredited person becomes an accredited data recipient for CDR data when:

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

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

<sup>6</sup> APP 13 requires that APP entities must take reasonable steps to correct personal information where the entity is satisfied, independently of any request, that personal information it holds.

- 11.16 When working out the purpose for which the CDR data is or was held, entities must disregard the purpose of holding the CDR data so that it can be disclosed as required under the CDR Rules.
- 11.17 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 \(Key concepts\)](#).

### **Example 1 – data holder**

Bright Bank is a data holder and is regularly required or authorised to disclose consumers’ CDR data under the CDR Rules.

Bright Bank receives a consumer data request from Leighton, requesting that Bright Bank share their account balance and details with Innobank.

Bright Bank holds this data for the purposes of providing a bank account service to Leighton.

When Bright Bank is required or authorised to disclose Leighton’s CDR data under the CDR Rules to Innobank, Privacy Safeguard 11 requires Bright Bank to take reasonable steps to ensure the data is accurate, up to date and complete having regard to this purpose.

### **Example 2 – accredited data recipients**

Vikingforce is an accredited data recipient who collects and uses Hamish’s CDR data to provide him with a product comparison service, and recommendations about suitable products. With Hamish’s consent, Vikingforce transfers Hamish’s CDR data to Turtledoor so he can acquire the recommended product.

Vikingforce holds Hamish’s CDR data for the purpose of providing Hamish with a product comparison service and product recommendations, and must take reasonable steps to ensure the data is accurate, up to date and complete having regard to this purpose.

Vikingforce does not hold Hamish’s CDR data for the purpose of transferring it to Turtledoor for Hamish to acquire a product, and must disregard this purpose when taking reasonable steps to ensure the data is accurate, up to date and complete under Privacy Safeguard 11.

- 11.18 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.<sup>7</sup>
- 11.19 The following analysis of each term draws on the ordinary meaning of the terms and the APP Guidelines.<sup>8</sup> As the analysis indicates, there is overlap in the meaning of the terms.

## **Accurate**

- 11.20 CDR data is inaccurate if it contains an error or defect or is misleading. An example is factual information about a consumer’s income, assets, loan repayment history or employment status which is incorrect having regard to the purpose for which it is held.

<sup>7</sup> These terms are also used in Privacy Safeguard 13 in respect of the requirement for a data holder, as an alternative to correcting the CDR data, to include a statement with CDR Data to ensure that it is accurate, up to date, complete and not misleading, after receiving a request from the consumer to correct the CDR data (see [Chapter 13 \(Privacy Safeguard 13\)](#)).

<sup>8</sup> See [Chapter 10: APP 10 — Quality of personal information of the APP Guidelines](#).

- 11.21 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.<sup>9</sup> 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 the existing information it holds on a consumer to predict their 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 basis for that estimation (i.e. it is based on the consumer’s income over previous financial years), this would not be inaccurate solely because the consumer believes their income will be higher or lower during the projected period.
- 11.22 CDR data may be inaccurate even if it is consistent with a consumer’s instructions or if the inaccuracy is attributable to the consumer. For example, if a consumer has provided an incorrect mobile number which is held by the data holder for the purpose of being able to contact the consumer, and the data holder discloses this, the CDR data may be inaccurate and the data holder may later become aware of this inaccuracy.

## Up to date

- 11.23 CDR data is not up to date if it contains information that is no longer current. An example is a statement that a consumer has an active account with a certain 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.<sup>10</sup>
- 11.24 CDR data about a past event may have been up to date at the time it was recorded but has been overtaken by a later development. Whether that data is up to date will depend on the purpose for which it is held. For example, if a consumer has had a second child but their CDR data records them as having only one child, the CDR data will still be up to date if that data is held for the purpose of recording whether the consumer is a parent.
- 11.25 In a similar manner to accuracy, CDR data may not be up to date even if it is consistent with a consumer’s instructions or if the inaccuracy is attributable to the consumer.

## Complete

- 11.26 CDR data is incomplete if it presents a partial or misleading picture of a matter of relevance, rather than a true or full picture.
- 11.27 An example is data from which it can be inferred that a consumer owes a debt, which in fact has been repaid. The CDR data will be incomplete under Privacy Safeguard 11 if the data is held, for instance, for the purpose of determining the borrowing capacity of the consumer. Where the CDR data is held for a different purpose for which the debt is irrelevant, the fact that the debt has been repaid may not of itself render the CDR data incomplete. If, however, the accredited person has requested a consumer’s CDR data for a specific period, and in that period the consumer owed a debt which is recorded in the CDR data, and that debt was repaid in a later period, the CDR data will still be ‘complete’ in respect of that specific period.

---

<sup>9</sup> Data derived from CDR data continues to be ‘CDR data’: see s 56AI of the Competition and Consumer Act.

<sup>10</sup> Such an assessment will likely be ‘materially enhanced information’ under section 10 of the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019 and therefore not ‘required consumer data’ under the CDR Rules.

# Taking reasonable steps to ensure the quality of CDR data

## When must an entity take reasonable steps?

11.28 Privacy Safeguard 11 requires an entity to take reasonable steps to ensure the quality of CDR data at the following points in time:

- **for data holders:** at the time the entity is required or authorised, or throughout the period in which the entity is required or authorised, to disclose CDR data under the CDR Rules. This includes when a data holder discloses CDR data:
  - to accredited data recipients under CDR Rule 4.6, and
  - to consumers under CDR Rule 3.4
- **for accredited data recipients:** at the time the entity discloses CDR data when required or authorised under the CDR Rules. This includes (but is not limited to) when an accredited data recipient discloses CDR data to:
  - an accredited data recipient under CDR Rules 7.5(1)(g)<sup>11</sup>
  - the consumer under CDR Rule 7.5(1)(c), and
  - an outsourced service provider under CDR Rule 7.5(1)(d).

11.29 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.

11.30 Entities should also be aware that Privacy Safeguard 11 only requires accredited data recipients to take reasonable steps when disclosing CDR data *under the CDR Rules*. It does not apply in relation to other disclosures of CDR data, for example where an accredited data recipient is required or authorised under another Australian law or court/tribunal order to disclose CDR data. The concept, ‘required or authorised to use or disclose CDR data under the CDR Rules’ is discussed in [Chapter B \(Key concepts\)](#).

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

**Privacy tip:** While the obligation to ensure the quality of CDR data under Privacy Safeguard 11 applies only at the time a data holder is required or authorised to disclose the data, data holders should have processes and procedures in place to periodically update and confirm the accuracy of the CDR data that they hold, during periods in which they are not required or authorised to disclose the data. As CDR data that falls under the privacy safeguards is also personal information, data holders should already have in place such processes and procedures to ensure the accuracy of personal information they collect and use for the purposes of APP 10.

<sup>11</sup> Disclosure of CDR data to an accredited person is not a permitted use or disclosure until the earlier of 1 July 2021 or the day a consumer experience data standard is made for the disclosure of CDR data to accredited persons. See CDR Rule 7.5A.

## What constitutes ‘reasonable steps’?

11.31 The requirement to ensure the quality of CDR data is qualified by a ‘reasonable steps’ test.

11.32 This test requires an objective assessment of what is considered reasonable, having regard to the purpose for which the information is held, which could include:

- **The nature of the entity.** The size of the entity, its resources, the complexity of its operations and its business model are all relevant to determining what steps would be reasonable for the entity to take to ensure the quality of the CDR data it is authorised or required to disclose.
- **The sensitivity of the CDR data held and adverse consequences for the consumer if the quality of CDR data is not ensured.** An entity should consider the sensitivity of the data and possible adverse consequences for the consumer concerned if the CDR data is not correct for the purpose it is held. A data holder should take more extensive steps to ensure the quality of highly sensitive data that it might be required or authorised to disclose. More rigorous steps may be required as the risk of adversity increases.
- **Whether the CDR data has been inferred.** Entities may be required to take more rigorous steps to ensure the quality of CDR data that has been created, generated or inferred through analytics processes.
- **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.

11.33 In some circumstances, it will be reasonable for an accredited data recipient to take no steps to ensure the quality of CDR data. For example, where an accredited data recipient collects CDR data from a data holder known to be reliable, and the accredited data recipient has not created, generated, or inferred any further CDR data, it may be reasonable to take no steps to ensure the quality of that data. It is the responsibility of the entity to be able to justify that this is reasonable.

## Examples of reasonable steps

11.34 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.

- Ensuring updated or new CDR data is promptly added to the relevant existing records as appropriate.<sup>12</sup>
- For a data holder, implementing protocols to ensure that the CDR data is accurate, up to date and complete both before and once it has been converted to the format required by the Data Standards.
- For an accredited data recipient, ensuring that any analytic processes used are operating appropriately and are fit for purpose, and not creating inaccurate or unjustified results. This is because data derived from CDR data collected by an accredited data recipient continues to be ‘CDR data’.<sup>13</sup>

## Advising a consumer when disclosed CDR data is incorrect

11.35 Under Privacy Safeguard 11, if a data holder or accredited data recipient becomes aware that disclosed CDR data was not accurate, up to date and complete, they must advise the consumer in accordance with the CDR Rules.<sup>14</sup>

11.36 CDR Rule 7.10 sets out the requirements for notifying the consumer where a data holder or accredited data recipient becomes aware that disclosed CDR data was not accurate, up to date and complete. These requirements are summarised below.

### In what circumstances must a consumer be advised that disclosed CDR data was incorrect?

11.37 Data holders and accredited data recipients must advise a consumer that some or all of the CDR data was incorrect if the entity:<sup>15</sup>

- has disclosed CDR data after being required or authorised to do so under the CDR Rules, and
- then later 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.

11.38 Data holders and accredited data recipients may ‘become aware’ of inaccuracies in CDR data that was previously disclosed if it discovers an inconsistency during normal business practices. Examples include but are not limited to circumstances where:

- information provided by the consumer is inconsistent with CDR data previously disclosed,
- the entity is notified by the consumer or another entity that the CDR data is incorrect, or a practice, procedure or system that the entity has implemented to ensure compliance with the safeguards (such as a periodic audit or monitoring program) indicates that the CDR data previously disclosed was incorrect.

---

<sup>12</sup> Compliance with Privacy Safeguard 13 (correction of CDR data) and where relevant, APP 13 (correction of personal information) for data holders, can also support this example for taking reasonable steps to ensure quality of CDR data.

<sup>13</sup> See section 56AI of the Competition and Consumer Act.

<sup>14</sup> See section 56EN(3) of the Competition and Consumer Act.

<sup>15</sup> Section 56EN(3) of the Competition and Consumer Act.

11.39 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. It is sufficient that the CDR data was not accurate, up to date and complete when disclosed.

## What information must be provided to the consumer when incorrect CDR data has been disclosed?

11.40 CDR Rule 7.10 requires a data holder or accredited data recipient 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.

11.41 Where the data holder or accredited data recipient disclosed the incorrect CDR data to an accredited person who was collecting that CDR data on behalf of another accredited person (the ‘principal’) under a CDR outsourcing arrangement, the data holder or accredited data recipient only needs to identify the principal accredited person in the notice.<sup>16</sup>

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

## How must a notice be provided?

11.43 CDR Rule 7.10 requires a data holder to notify the consumer in writing by electronic means after disclosing incorrect data.

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

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

## How quickly must the consumer be notified?

11.46 Data holders and accredited data recipients must provide notices to the consumer as soon as practicable, but no more than five business days after the entity becomes aware that some or all of the disclosed data was incorrect.

11.47 The test of practicability is an objective test. The entity should be able to justify that it is not practicable to give notification promptly after becoming aware of the disclosure of incorrect CDR data.<sup>17</sup>

11.48 In adopting a timetable that is ‘practicable’, an entity can take technical and resource considerations into account. However, it is the responsibility of the entity to justify any delay in providing the notice.

---

<sup>16</sup> CDR Rule 1.16(2)(b). For information on ‘CDR outsourcing arrangements’, see [Chapter B \(Key concepts\)](#).

<sup>17</sup> Options for providing early notification should, so far as practicable, be built into the entity’s processes and systems. For example, processes and systems should be in place to promptly notify a consumer that incorrect CDR data has been disclosed if the entity corrects CDR data (such as in response to a consumer’s correction request) that it had disclosed prior to it being corrected.



- 11.49 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 consumers.
- 11.50 The five business day period commences on the day after the entity becomes aware that some or all of the disclosed data was incorrect.<sup>18</sup> For example, if the entity becomes aware on 2 August, the five business day period begins on 3 August.
- 11.51 A ‘business day’ is a day that is not Saturday, Sunday or a public holiday in the place concerned.

### Example

Free Bank Ltd is a data holder for a large number of consumers. Hazel authorises Free Bank 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 Hazel’s repayments is correct.

Free Bank then becomes aware that some of the 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 able to provide a notice to Hazel over her consumer dashboard which states that:

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

*Free bank has provided Hazel with the notice required under CDR Rule 7.10 and Privacy Safeguard 11, as soon as practicable. (Free bank also ensures that it updates its own data holdings promptly, upon becoming aware of the inaccuracy. Ensuring that known errors are corrected promptly, regardless of how they are identified, is a reasonable step required by s 56EN(1).)*

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

Free Bank hires 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 Hazel.

*Free Bank would need to be able to demonstrate that it has sent the affected consumers the required notices as soon as practicable, to ensure compliance with CDR Rule 7.10 and Privacy Safeguard 11.*

<sup>18</sup> See section 36 of the *Acts Interpretation Act 1901*.



## In what circumstances must an entity disclose corrected CDR data to the original recipient?

11.52 Privacy Safeguard 11 requires data holders and accredited data recipients to disclose corrected CDR data, in accordance with the CDR Rules, to the original recipient<sup>19</sup> of the disclosure if:<sup>20</sup>

- the entity has advised the consumer that some or all of the CDR data was incorrect when the entity disclosed it, and
- the consumer requests in accordance with the CDR rules for the entity to disclose the corrected CDR data.

11.53 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.

11.54 The term ‘corrected CDR data’ is not defined in the Competition and Consumer Act. For the purposes of the obligation to disclose corrected CDR data under Privacy Safeguard 11, ‘corrected CDR data’ includes:

- CDR data which has been corrected in accordance with s 56EP(3)(a)(i), and
- CDR data for which a qualifying statement has been included in accordance with s 56EP(3)(a)(ii).

## Record keeping requirements

11.55 If an entity discloses corrected CDR data in accordance with Privacy Safeguard 11,<sup>21</sup> the entity (and, if the data is disclosed to an accredited person, the recipient) must comply with the record keeping requirements under CDR Rule 9.3.

11.56 For data holders, CDR 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.<sup>22</sup> If corrected data is disclosed, the data holder must 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. There is no requirement, however, to record the disclosure as either ‘correct’ or ‘incorrect’.

11.57 For accredited data recipients, CDR Rule 9.3(2) requires the recipient to keep and maintain various records relating to CDR data, including records of collections of CDR data under the CDR Rules.<sup>23</sup> This means that, similarly to data holders, accredited data recipients must keep

---

<sup>19</sup> The original recipient may be the consumer where the data holder disclosed the CDR data to the consumer in response to a valid consumer request in accordance with CDR Rule 3.4(2) or (3).

<sup>20</sup> Section 56EN(4) of the Competition and Consumer Act. Note that although this subsection is also expressed to apply to accredited data recipients, as there are no CDR Rules for such entities to advise consumers of disclosures of incorrect data under section 56EN(3) of the Competition and Consumer Act, the obligation in section 56EN(4) does not currently apply to those entities.

<sup>21</sup> Section 56EN(4) of the Competition and Consumer Act.

<sup>22</sup> CDR Rule 9.3(1)(d). For further information on record keeping requirements for data holders, see the [Guide to privacy for data holders](#).

<sup>23</sup> CDR Rule 9.3(2)(e).

and maintain a record of both the initial collection of the incorrect CDR data and the subsequent collection of the corrected CDR data, in circumstances where corrected CDR data is disclosed under s 56EN(4).

## How does Privacy Safeguard 11 interact with the other privacy safeguards?

### Privacy Safeguard 5

- 11.58 Privacy Safeguard 5 requires an accredited data recipient to notify a consumer of the collection of their CDR data by updating the consumer's dashboard.
- 11.59 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

- 11.60 Privacy Safeguard 10 requires data holders to notify a consumer of the disclosure of their CDR data by updating the consumer's dashboard.
- 11.61 Where a data holder has disclosed CDR data, and then discloses corrected data as the result of the consumer's request 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

McCarthy Bank Ltd, a data holder, discloses Satoko's CDR data to accredited person, Watson and Co, in response to a consumer data request made on Satoko's behalf.

McCarthy Bank updates Satoko's consumer dashboard under Privacy Safeguard 10 and CDR Rule 7.9, and Watson and Co updates Satoko's consumer dashboard under Privacy Safeguard 5 and CDR Rule 7.4.

However, Satoko realises that the CDR data disclosed by McCarthy Bank is not accurate, and asks McCarthy Bank to disclose the correct data to Watson and Co.

McCarthy Bank corrects the CDR data in accordance with Privacy Safeguard 13 and CDR Rule 7.15. McCarthy Bank also takes reasonable steps to correct their own data holdings per Privacy Safeguard 11, as they are made aware of inaccuracies through Satoko's disclosure request.

McCarthy Bank then complies with Satoko's request to disclose corrected CDR data. Both Watson and Co and McCarthy Bank update Satoko's consumer dashboards accordingly.

## Privacy Safeguard 12

11.62 Where an accredited data recipient amends CDR data to comply with Privacy Safeguard 11, it should consider whether it needs to take action under Privacy Safeguard 12 to destroy or de-identify the original data.

## Privacy Safeguard 13

11.63 As set out in [Chapter 13 \(Correction of CDR data\)](#), a correction request made under Privacy Safeguard 13 may trigger the obligations under Privacy Safeguard 11.

11.64 Privacy Safeguard 13 requires data holders and accredited data recipients to respond to a consumer request for correction of their CDR data, where that data has previously been disclosed under the CDR Rules. In response to a consumer request under Privacy Safeguard 13, CDR entities must either correct the CDR data, include a qualifying statement with the CDR data to ensure it is accurate, up to date, complete and not misleading (having regard to the purpose for which it is held), or state why a correction is unnecessary or inappropriate.<sup>24</sup>

11.65 Where a data holder corrects CDR data or includes a qualifying statement with the data in accordance with Privacy Safeguard 13, they should also consider whether the consumer must be advised of any previous disclosures of the CDR data where the data may have been incorrect when it was disclosed, in accordance with Privacy Safeguard 11. In such circumstances, the data holder will be on notice that the CDR data was likely incorrect when disclosed.

---

<sup>24</sup> Section 56EP(3)(a) of the Competition and Consumer Act.

## Chapter 12:

# Privacy Safeguard 12 —

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

Version 3.0, June 2021

# Contents

<b>Key points</b>	<b>3</b>
<b>What does Privacy Safeguard 12 say?</b>	<b>3</b>
<b>Why is it important?</b>	<b>3</b>
<b>Who does Privacy Safeguard 12 apply to?</b>	<b>4</b>
<b>Accreditation guidelines on information security</b>	<b>4</b>
<b>How Privacy Safeguard 12 interacts with the Privacy Act</b>	<b>5</b>
<b>PART A: Security of CDR data</b>	<b>6</b>
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
<b>PART B: Treatment of redundant data (destruction and de-identification)</b>	<b>17</b>
Overview of the process for treating redundant data	17
What is 'redundant data'?	19
Deciding how to deal with redundant data	20
Steps to destroy redundant data	23
Steps to de-identify redundant data	25
<b>Other relevant security obligations</b>	<b>26</b>
Privacy safeguards	26
<b>Other CDR de-identification processes</b>	<b>27</b>

## 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 of CDR data and designated gateways to ensure CDR data is protected from misuse, interference and loss, as well as from unauthorised access, modification or disclosure. The specific steps that these entities must take to protect CDR data are in the consumer data rules (CDR Rules).
- In addition, if an accredited data recipient of CDR data or a designated gateway no longer needs the CDR data for purposes permitted by privacy safeguards or the CDR Rules, then the data is considered 'redundant data' and will need to be destroyed (or deleted) or de-identified unless an exception applies.
- An applicant for accreditation must demonstrate compliance with the information security requirements in Privacy Safeguard 12 in order to gain and maintain accreditation under the CDR regime.

## What does Privacy Safeguard 12 say?

- 12.1 Accredited data recipients of CDR data and designated gateways must take the steps in the CDR Rules to protect CDR data from misuse, interference and loss, as well as unauthorised access, modification and disclosure.
- 12.2 Accredited data recipients of CDR data and designated gateways must also take the steps set out in the CDR Rules to destroy or de-identify any CDR data that is no longer needed for:
- the purposes permitted under the CDR Rules, or
  - any purpose for which the information may be used or disclosed under the privacy safeguards.
- 12.3 Consumers can request that their CDR data be deleted once it is no longer needed. Accredited data recipients of CDR data and designated gateways must delete CDR data that is subject to a deletion request unless an exception applies.
- 12.4 These requirements apply except where:
- the accredited data recipient or designated gateway is required by law or a court/tribunal order to keep the CDR data, or
  - the CDR data relates to current or anticipated legal or dispute resolution proceedings to which the accredited data recipient, designated gateway or consumer is a party.

## 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 [Australian community attitudes to privacy survey](#), privacy protection contributes to an individual's trust in an entity. If an entity is perceived to be handling data contrary to community expectations, individuals may seek out alternative products and services.
- 12.7 In addition, accredited data recipients are entrusted with CDR data under the CDR regime to allow them to provide products and services to consumers. Privacy Safeguard 12 ensures that accredited data recipients are taking steps to ensure a consistent, high standard of security under the CDR Rules to ensure this data is protected. This helps to build public trust and confidence in the security practices of accredited data recipients.
- 12.8 Deleting or de-identifying redundant data also minimises the risk profile of an accredited data recipient as they are not holding unnecessary CDR data.

## Who does Privacy Safeguard 12 apply to?

- 12.9 Privacy Safeguard 12 applies to accredited data recipients of CDR data and designated gateways for CDR data. It does not apply to data holders. However, data holders must ensure that they are adhering to their obligations under the *Privacy Act 1988* (the Privacy Act) and the Australian Privacy Principles (APPs), including APP 11, in relation to the security of personal information.

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

## Accreditation guidelines on information security

- 12.10 This chapter provides guidance on the steps for securing CDR data and managing redundant data in compliance with Privacy Safeguard 12.
- 12.11 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.
- 12.12 Accredited persons should refer to the 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 that 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

12.13 It is important to understand how Privacy Safeguard 12 interacts with the Privacy Act and the APPs.<sup>1</sup>

12.14 APP 11 requires APP entities to take measures to ensure the security of personal information they hold and to consider whether they are permitted to retain this personal information (see [Chapter 11: APP 11 – Security of personal information of the APP Guidelines](#)).

CDR entity	Privacy protections that apply in the CDR context
<b>Accredited data recipient</b>	<p><b>Privacy Safeguard 12</b></p> <p>For accredited data recipients of a consumer's CDR data, Privacy Safeguard 12 applies to the security of that CDR data.<sup>2</sup></p> <p>APP 11 does not apply in relation to that CDR data.<sup>3</sup></p> <p><b>Note:</b> Accredited persons must also demonstrate compliance with the information security requirements in Privacy Safeguard 12 to maintain accreditation.<sup>4</sup></p>
<b>Designated gateways</b>	<p><b>Privacy Safeguard 12</b></p> <p>For designated gateways for CDR data, Privacy Safeguard 12 applies to the security of the CDR data.<sup>5</sup></p> <p>APP 11 does not apply in relation to that CDR data.<sup>6</sup></p>

<sup>1</sup> 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](#).

<sup>2</sup> Privacy Safeguard 12 applies from the point when the accredited person becomes an accredited data recipient of the CDR data. An accredited person becomes an accredited data recipient for CDR data when:

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

<sup>3</sup> The APPs do not apply to an accredited data recipient of CDR data, in relation to that CDR data - s 56EC(4)(a) of the Competition and Consumer Act. However, s 56EC(4) does not affect how the APPs apply to accredited persons and accredited data recipients who are APP entities, in relation to the handling of personal information outside the CDR system. (Note: Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See s 6E(1D) of the Privacy Act.) Section 56EC(4) also does not affect how the APPs apply to an accredited person who does not become an accredited data recipient of the CDR data (other than for Privacy Safeguards 1 – 4). See s 56EC(5)(aa) of the Competition and Consumer Act.

<sup>4</sup> See the ACCC's Supplementary Accreditation Guidelines on Information Security for more information.

<sup>5</sup> Section 56EO(1) of the Competition and Consumer Act.

<sup>6</sup> The APPs do not apply to designated gateways for CDR data in relation to that CDR data - s 56EC(4)(d) of the Competition and Consumer Act. However, s 56EC(4) does not affect how the APPs apply to designated gateways who are APP entities, in relation to the handling of personal information outside the CDR system. See s 56EC(5)(b) of the Competition and Consumer Act.



**Data holders****APP 11**

Privacy Safeguard 12 does not apply to data holders.

## PART A: Security of CDR data

### What do security measures need to protect against?

12.15 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.

12.16 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.

12.17 The terms ‘misuse’, ‘interference’, ‘loss’ and ‘unauthorised access’ are not defined in the Competition and Consumer Act. The following discussion represents the OAIC’s interpretation of these terms based on their ordinary meaning. However, given that information security is an evolving concept, the discussion below is not intended 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.<sup>7</sup>
- **Interference:** occurs when there is an attack on CDR data that interferes with the CDR data but does not necessarily modify its content. For example, interference would occur if there is a ransomware attack that leads to the data being locked down and ransomed.
- **Loss:** refers to the accidental or inadvertent loss of CDR data where the data is no longer accessible and usable for its purpose, or in circumstances where it is likely to result in authorised access or disclosure. Examples of loss include physical loss by leaving data in a public place, failing to keep adequate backups in the event of systems failure or as a result of natural disasters.<sup>8</sup>
- **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.

<sup>7</sup> Privacy Safeguard 6 sets out when an accredited data recipient of CDR data or a designated gateway for CDR data is permitted to use that CDR data (see [Chapter 6 \(Privacy Safeguard 6\)](#)). Privacy Safeguards 7 and 9 also contain requirements relating to an entity’s use of CDR data for the purpose of direct marketing and use of government related identifiers respectively (see [Chapters 7 \(Privacy Safeguard 7\)](#) and [9 \(Privacy Safeguard 9\)](#)).

<sup>8</sup> Loss does not apply to intentional destruction or de-identification of CDR data undertaken in accordance with the CDR Rules.

- **Unauthorised modification:** occurs where CDR data is altered by someone who is not permitted to do so, or where the data is altered in a way that is not permitted. For example, unauthorised modification would occur if an employee of an accredited data recipient or designated gateway altered a consumer's savings account information to offer a more favourable deal.
- **Unauthorised disclosure:** occurs where an accredited data recipient or designated gateway, whether intentionally or unintentionally, makes CDR data accessible or visible to others outside the entity. For example, unauthorised disclosure includes 'human error', such as an email sent to the wrong person. It can also include disclosure of CDR data to a scammer as a result of inadequate identity verification procedures.

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

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

12.19 Privacy Safeguard 12 requires accredited data recipients and designated gateways to take the steps in the CDR Rules to protect the CDR data from misuse, interference and loss, as well as unauthorised access, modification and disclosure. These steps are detailed in Schedule 2 of the CDR Rules.

12.20 The CDR Rules provide obligations for accredited data recipients to have governance requirements in place, understand their data environment and risk posture, and implement minimum security controls.<sup>9</sup>

12.21 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 to the CDR Rules).
- **Step 4:** implement a formal controls assessment program.
- **Step 5:** manage and report security incidents.

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

12.23 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.

---

<sup>9</sup> The CDR Rules currently do not detail steps for how designated gateways must comply with Privacy Safeguard 12.

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

### Information security governance framework

- 12.24 The CDR Rules require an accredited data recipient to establish and maintain a formal governance framework<sup>10</sup> for managing information security risks relating to CDR data.
- 12.25 An accredited data recipient may leverage their existing information security governance structure and extend it to their CDR data environment.<sup>11</sup> An accredited data recipient may also utilise existing frameworks, requirements and models in developing their information security governance framework and defining security areas.<sup>12</sup>
- 12.26 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.
- 12.27 When deciding whether to adopt, apply or modify a standard information security governance framework or model, an accredited data recipient should ensure that the framework or model:
- is appropriate for CDR data and the CDR sector(s) in which the accredited data recipient is operating
  - is current and up to date
  - takes into account what internal or external auditing is undertaken, and
  - is underpinned by a risk profile comparable to the risk profile of the accredited data recipient's CDR data environment.
- 12.28 Accredited persons are subject to ongoing reporting and audit requirements set out in the CDR Rules (Schedule 1, Part 2). Further information regarding the reporting requirements is contained within the ACCC's Supplementary Accreditation Guidelines 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 (which may be part of a broader risk assessment to identify other risks including data mismanagement and quality) before establishing and maintaining a formal governance framework. This ensures the accredited data recipient is aware of their security risk profile and vulnerabilities so that the formal governance framework matches the privacy risks and is fit for purpose.

<sup>10</sup> A formal governance framework refers to policies, processes, roles and responsibilities required to facilitate the oversight and management of information security.

<sup>11</sup> For further information, see the ACCC's Supplementary Accreditation Guidelines on Information Security.

<sup>12</sup> The ACCC's 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.

## Documenting practices and procedures relating to information security and management of CDR data

- 12.29 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.<sup>13</sup>
- 12.30 Accredited data recipients may choose to document these practices and procedures as part of the information security policy required by the CDR Rules, (see paragraphs 12.34–12.38) or as a separate document.
- 12.31 Senior management will have ultimate responsibility for the management of information security.<sup>14</sup> Senior management should implement the necessary practices, procedures, resources and training to allow the accredited data recipient to effectively discharge its responsibilities under the CDR Rules.<sup>15</sup>
- 12.32 An accredited data recipient should establish formal information security governance structures, such as committees and forums, to oversee the security of CDR data.<sup>16</sup> These committees or forums should include membership from across key business areas, particularly where the entity's CDR data environment is large or complex,<sup>17</sup> so information security is an integrated component of the accredited data recipient's entire business and not left to the compliance or the information and communications technology area alone.
- 12.33 An accredited data recipient's formal information security governance structures should have clear procedures for oversight and accountability, and clear lines of authority for decisions regarding the security of CDR data.

**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

<sup>13</sup> Clause 1.3(2) of Schedule 2 to the CDR Rules.

<sup>14</sup> Senior management, of an accredited data recipient that is a body corporate, means: (a) the accredited data recipient's directors; and (b) any person who makes or participates in making decisions that affect the management of CDR data by the accredited data recipient: clause 1.2 of Schedule 2 to the CDR Rules.

<sup>15</sup> The ACCC's Supplementary Accreditation Guidelines on Information Security.

<sup>16</sup> The ACCC's Supplementary Accreditation Guidelines on Information Security.

<sup>17</sup> The ACCC's Supplementary Accreditation Guidelines on Information Security.

- it is clear to staff who holds key security roles, including who is responsible for the overall operational oversight and strategic direction of secure CDR data handling, and
- if there are several areas or teams responsible for information security and privacy, or if the organisation's CDR data environment is large or complex, there should be governance arrangements in place to ensure that key business areas work together (for example, committees and forums).

### Information security policy

12.34 An accredited data recipient must have and maintain an information security policy that governs information security across their organisation.<sup>18</sup>

12.35 The information security policy must include information about:<sup>19</sup>

- its information security risk posture (that is, the exposure and potential harm to the entity's information assets, including CDR data, from security threats)
- how the entity plans to address those risks
- the exposure and potential harm from security threats, and
- how its information security practices and procedures and its information security controls, are designed, implemented and operated to mitigate those risks.

12.36 The information security policy should be internally and externally enforceable. Compliance with the policy should also be monitored.<sup>20</sup>

12.37 An accredited data recipient may choose to address CDR data security in a single policy or across multiple policies (for example, to account for different business areas). While a specific information security policy for CDR data is preferred, it is not required.

12.38 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.

<sup>18</sup> Clause 1.3(3) of Schedule 2 to the CDR Rules.

<sup>19</sup> Clause 1.3(3) of Schedule 2 to the CDR Rules.

<sup>20</sup> The term 'enforceable' is defined in the ACCC's 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 contractual requirements and ongoing third party monitoring processes.

## Review of appropriateness

12.39 The accredited data recipient must review and update the formal governance framework for appropriateness:

- in response to material changes to both the extent and nature of threats to its CDR data environment and its operating environment, or
- where no such material changes occur — at least annually.<sup>21</sup>

### What is a material change?

A material change is one that significantly changes the CDR data environment, such as the introduction of a new system, the migration of data onto new infrastructure, introduction of a new outsourced service provider, or a change to the terms and conditions of the services provided by an existing outsourced service provider.<sup>22</sup>

## Step 2: Define the boundaries of the CDR data environment

12.40 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.<sup>23</sup>

12.41 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 collected by or disclosed to outsourced service providers. The documented analysis should generally include information about:

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

**Technology:** Such as information systems, storage systems (including whether data is stored overseas, with a cloud service provider, or other third-party), data security systems, authentication systems.

**Processes:** The entity's CDR information handling practices, such as how it collects, uses and stores personal information, including whether CDR data handling practices are outsourced to third parties.

<sup>21</sup> Clause 1.3(4) of Schedule 2 to the CDR Rules.

<sup>22</sup> See the ACCC's Supplementary Accreditation Guidelines on Information Security.

<sup>23</sup> See the ACCC's Supplementary Accreditation Guidelines on Information Security.

**Other factors to consider:** What other data exists in the data environment, and how does it overlap or connect with the CDR data? This is important to know in order to identify which datasets are high-risk. It is important to identify where non-CDR datasets could be linked with CDR data, increasing the risk of unauthorised disclosure or access.

12.42 This can either be documented through a data flow diagram or a written statement.<sup>24</sup>

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

- as soon as practicable when they become aware of material changes to the extent and nature of threats to their CDR data environment, or
- where no such material changes occur, at least annually.

### Step 3: Have and maintain an information security capability

12.44 The CDR Rules require an accredited data recipient to have and maintain an information security capability that:

- complies with minimum controls set out in Part 2 to Schedule 2 of the CDR Rules, and
- is appropriate and adapted to respond to risks to information security, having regard to:
  - the extent and nature of threats to CDR data that the accredited data recipient holds
  - the extent and nature of CDR data that it holds, and
  - the potential loss or damage to one or more consumers if all, or part, of the consumer's data were to be misused, interfered with, or accessed, modified or disclosed without authorisation.

12.45 The accredited data recipient must review and adjust its information security capability as required by the CDR Rules (see paragraphs 12.55 – 12.56 following).

#### Information security controls

12.46 The CDR Rules contain information security controls to be designed, implemented and operated by an accredited data recipient as part of its information security capability. These are detailed in Part 2 to Schedule 2 to the CDR Rules.

12.47 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

---

<sup>24</sup> For further information see the ACCC's Supplementary Accreditation Guidelines on Information Security.

- 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.

12.48 Compliance with Privacy Safeguard 12 requires the implementation of these controls across the CDR environment.

12.49 The information security controls in Part 2, Schedule 2 of the CDR Rules are the *minimum controls* required for an applicant to become accredited and for an accredited data recipient to ensure ongoing compliance with Privacy Safeguard 12. An accredited data recipient may choose to implement stronger protections.

12.50 Further information regarding the minimum information security controls is contained in the ACCC's Supplementary Accreditation Guidelines on Information Security.

#### **Additional security controls required to respond to risks to information security**

12.51 In addition to the information security controls set out in Part 2 Schedule 2 of the CDR Rules, an accredited data recipient must also have and maintain an information security capability that is appropriate and adapted to respond to risks to information security, having regard to:

- the extent and nature of threats to CDR data that it holds, and
- the extent and nature of CDR data that it holds, and the potential loss or damage to one or more consumers if all or part of the consumer's data were to be misused, interfered with, or accessed, modified or disclosed without authorisation.

12.52 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**

12.53 Where an accredited data recipient uses an outsourced service provider to:

- collect CDR data on the accredited data recipient's behalf, and/or
- provide the accredited data recipient with goods or services, using CDR data provided by the accredited data recipient,

the accredited data recipient must ensure their contract with the outsourced service provider requires them to take the steps outlined in Schedule 2 as if the outsourced service provider were an accredited data recipient.<sup>25</sup>

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

---

<sup>25</sup> CDR Rule 1.10(2)(b)(i).



- 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 CDR Rules and the security controls set out in Part 2 of the CDR 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, and
- including contractual provisions regarding security capability reflecting the definition of a CDR outsourcing arrangement in the CDR Rules.<sup>26</sup>

### Reviewing security capability

12.55 Under the CDR Rules, an accredited data recipient must review and adjust its information security capability:

- in response to material changes to both the nature and extent of threats and its CDR data environment, or
- where no such material changes occur, at least annually.<sup>27</sup>

12.56 Where changes in the operations of the accredited data recipient could lead to changes in its risk posture (for example, development of new applications, migration to new infrastructure), the accredited data recipient should review its information security capability to ensure it remains fit for purpose in managing information security risks.

## Step 4: implement a formal controls assessment program

### Assessing the effectiveness of controls

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

12.58 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
- 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.<sup>28</sup>

12.59 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

---

<sup>26</sup> CDR Rule 1.10(2).

<sup>27</sup> Clause 1.5(2) of Schedule 2 to the CDR Rules.

<sup>28</sup> Clause 1.6(1)(a) of Schedule 2 to the CDR Rules.

- the likelihood of failure of controls having regard to the results of previous testing.<sup>29</sup>

12.60 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.<sup>30</sup> More information can be found in the ACCC's Supplementary Accreditation Guidelines on Information Security.

12.61 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 to the CDR Rules.<sup>31</sup>

12.62 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.<sup>32</sup>

12.63 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.<sup>33</sup>

12.64 The accredited data recipient must review the sufficiency of its testing program:

- 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
- where no such material changes occur, at least annually.<sup>34</sup>

## Step 5: Manage and report security incidents

12.65 An accredited data recipient must have procedures and practices in place to detect, record, and respond to information security incidents as soon as practicable.<sup>35</sup> More detail about maintaining these practices can be found in ACCC's Supplementary Accreditation Guidelines on Information Security.

12.66 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.<sup>36</sup>

12.67 The accredited data recipient's CDR data security response plans must include procedures for:

- managing all relevant stages of an incident, from detection to post-incident review

---

<sup>29</sup> Clause 1.6(1)(b) of Schedule 2 to the CDR Rules.

<sup>30</sup> Clause 2.1(2) of Schedule 1 to the CDR Rules.

<sup>31</sup> Clause 1.6(2) of Schedule 2 to the CDR Rules.

<sup>32</sup> Clause 1.6(3) of Schedule 2 to the CDR Rules.

<sup>33</sup> Clause 1.6(4) of Schedule 2 to the CDR Rules.

<sup>34</sup> Clause 1.6(4) of Schedule 2 to the CDR Rules.

<sup>35</sup> Clause 1.7(1) of Schedule 2 to the CDR Rules.

<sup>36</sup> Clause 1.7(2) of Schedule 2 to the CDR Rules.

- b. notifying CDR data security breaches to the Information Commissioner and to consumers as required under Part IIIC of the Privacy Act,<sup>37</sup> 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.<sup>38</sup>
- 12.68 The accredited data recipient must review and test its CDR data security response plans to ensure they remain resilient, effective and consistent with its obligations in relation to CDR data security breaches.
- Where there is a material change to the nature and extent of threats to the accredited data recipient's CDR data environment or to the boundaries of the accredited data recipient's CDR data environment, this review and test must be undertaken as soon as practicable.
  - Where no such material changes occur, this review and test must be undertaken at least annually.<sup>39</sup>

## Notifiable Data Breach (NDB) scheme

- 12.69 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'.<sup>40</sup>
- 12.70 Under the NDB scheme, accredited data recipients are required to notify affected consumers and the Information Commissioner in the event of an 'eligible data breach' under the NDB scheme.<sup>41</sup>
- 12.71 A data breach is eligible if it is likely to result in serious harm to any of the consumers to whom the information relates. Entities must conduct a prompt and reasonable assessment if they suspect that they may have experienced an eligible data breach.
- 12.72 For more information, see the OAIC's [Notifiable Data Breaches scheme webpage](#).

The OAIC has developed the [Data breach preparation and response guide — A guide to managing data breaches in accordance with the Privacy Act](#) to support the development and implementation of an effective data breach response, including developing a data breach response plan. The principles and concepts from this guide are useful and applicable to CDR data security breaches.<sup>42</sup>

<sup>37</sup> See the 'Notifiable Data Breach (NDB) scheme' section further below in this Chapter.

<sup>38</sup> Clause 1.7(3) of Schedule 2 to the CDR Rules.

<sup>39</sup> Clause 1.7(4) of Schedule 2 to the CDR Rules.

<sup>40</sup> Section 56ES of the Competition and Consumer Act.

<sup>41</sup> See Part IIIC, Division 3 of the Privacy Act. See generally the OAIC's [Notifiable Data Breaches scheme webpage](#) for further information.

<sup>42</sup> The notifiable data breaches provisions of the Privacy Act apply in the CDR regime as if personal information was 'CDR data' (see section 56ES of the Competition and Consumer Act).

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

### Overview of the process for treating redundant data

- 12.73 An accredited data recipient must destroy or de-identify CDR data that has become ‘redundant’ unless an exception applies.<sup>43</sup> Information regarding when CDR data becomes ‘redundant’, as well as the exceptions to the requirement to destroy or de-identify redundant data, are discussed below at ‘What is ‘redundant data’?’ and outlined in the flow chart beneath paragraph 12.76.
- 12.74 Once CDR data is redundant, the steps an entity must take to determine whether to destroy or de-identify the CDR data are set out in the CDR Rules and explained under the heading ‘Deciding how to deal with redundant data’ below. What an accredited data recipient told the consumer during the consent phase (about how they treat redundant data) and whether the consumer has made an election to delete will be relevant to this decision, as demonstrated by the flow chart below at paragraph 12.83.
- 12.75 Once the accredited data recipient has determined whether to destroy or de-identify (and provided a consumer has not made an election to delete), it must follow the specific destruction and de-identification processes set out in the CDR Rules and outlined under the headings ‘Steps to destroy redundant data’ and ‘Steps to de-identify redundant data’ below.
- 12.76 Where the de-identification process does not apply or cannot result in de-identified information in accordance with the CDR Rules, the destruction process must be followed as outlined under the heading ‘Steps to destroy redundant data’ below.

---

<sup>43</sup> See Section 56EO(2)(a) of the Competition and Consumer Act.

## Redundant data in the CDR regime

### Whether CDR data is redundant

Do you need the CDR data for:

- a purpose permitted under the CDR Rules
- or
- a purpose for which you can use or disclose under the privacy safeguards?

No



Does an exception apply that allows you to keep the redundant data?

- Are you required to retain the redundant data by or under a law or court or tribunal order
- or
- Does the redundant data relate to any current or anticipated legal or dispute resolution proceedings to which you or the consumer are a party?

Yes



**You are permitted to retain the redundant data, and must continue to handle the redundant data in accordance with the privacy safeguards (including by continuing to take the steps specified in the CDR Rules to protect the redundant data).**

Yes



**The CDR data is not redundant data. Continue to handle the CDR data in accordance with the privacy safeguards.**

No



**You must delete or de-identify the redundant data in accordance with the CDR Rules.**



See the flowchart on deleting or de-identifying redundant data.

## What is ‘redundant data’?

- 12.77 ‘Redundant data’ is CDR data that an accredited data recipient or designated gateway no longer needs for a purpose permitted under the CDR Rules, or for any purpose for which it is allowed to be used or disclosed under the privacy safeguards.<sup>44</sup>
- 12.78 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.<sup>45</sup>
- 12.79 The terms ‘purpose’ (in the context of redundant data) and ‘required by or under an Australian law or court/tribunal order’ are discussed in more detail in Chapter B (Key concepts).
- 12.80 Privacy Safeguard 12 requires an accredited data recipient or designated gateway to take the steps in the CDR Rules to destroy or de-identify redundant data unless:<sup>46</sup>
- the entity is not required to retain the data by or under an Australian law or a court/tribunal order, or
  - the data does not relate to any current or anticipated legal proceedings or dispute resolution proceedings to which the entity or the consumer is a party.<sup>47</sup>
- 12.81 An accredited data recipient may request that the consumer state whether a legal or dispute resolution proceeding to which the consumer is a party is current or anticipated, and may rely on such a statement made by the consumer.<sup>48</sup>
- 12.82 A legal or dispute resolution proceeding is ‘anticipated’ if there is a real prospect of proceedings being commenced, as distinct from a mere possibility. A dispute resolution proceeding includes those undertaken through external dispute resolution schemes.
- 12.83 Within a dataset, some of the data may become redundant while other data does not. For instance, where a consumer has a number of banking accounts with a data holder, and data associated with one of those accounts is no longer needed by the accredited data recipient to provide the consumer with the requested services, that account data will become redundant data.

**Risk point:** Where an exception applies, entities risk keeping redundant data longer than they need to.

**Privacy tip:** Where, for example, laws prevent de-identification or destruction of redundant data, the entity should adopt other measures to limit privacy risks such as archiving and limiting access to those CDR data holdings. Entities should also clearly specify the law that authorises or requires the retention, how long the authorisation lasts, and the degree of information needed.

<sup>44</sup> See section 56EO(2)(a) of the Competition and Consumer Act.

<sup>45</sup> CDR Rule 5.23(4).

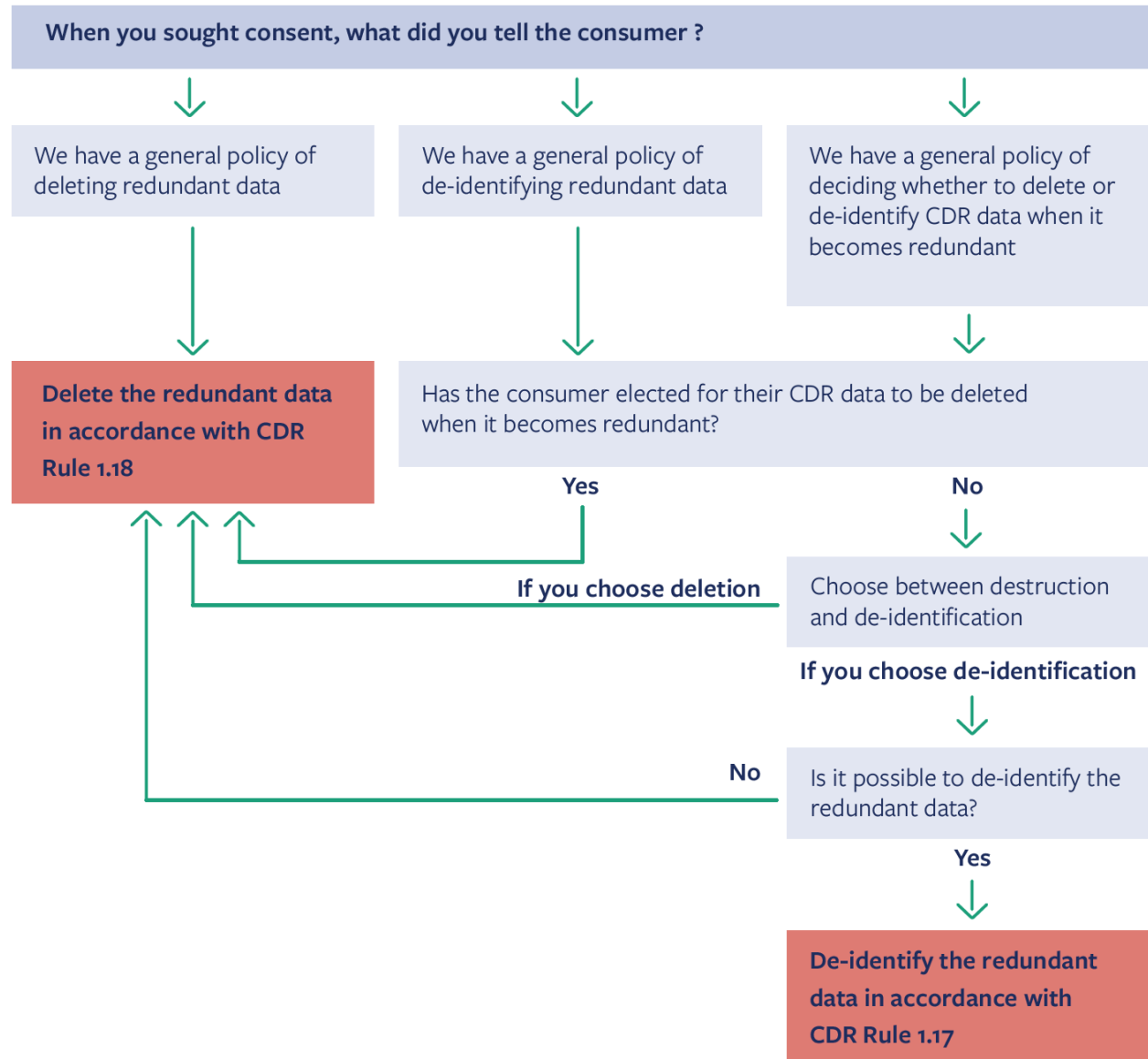
<sup>46</sup> See section 56EO(2) of the Competition and Consumer Act.

<sup>47</sup> See section 56BAA of the Competition and Consumer Act and CDR Rule 1.17A.

<sup>48</sup> CDR Rules 1.17(A)(2) – (3).

# Deciding how to deal with redundant data

## Deleting or de-identifying redundant data



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

### General policy for dealing with redundant data

12.84 When seeking consent from a consumer in relation to the handling of their CDR data,<sup>49</sup> 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.<sup>50</sup>

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

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

12.86 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).<sup>51</sup>

12.87 See Chapter B (Key Concepts) for further guidance about the meaning of 'derived data'.

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

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

12.89 An accredited data recipient must consider whether an exception to the requirement to destroy redundant data set out above at 'What is 'redundant data'?' applies to the redundant data. If an exception applies, the accredited data recipient must retain the CDR data while the exception applies.<sup>52</sup>

12.90 The CDR Rules require redundant data to be destroyed where:

- the consumer has elected for their redundant data to be deleted,
- if no election has been made, the accredited data recipient advised the consumer at the time of seeking consent that it had a general policy of deleting redundant data. Where an accredited data recipient advised the consumer of a general policy of destruction, the accredited data recipient **must destroy the redundant data**, even if their general policy has since changed, or
- it is not possible to de-identify the CDR data to the required extent (see Step 5).

---

<sup>49</sup> CDR Rule 4.11(3)(h)(i).

<sup>50</sup> CDR Rule 4.17(1).

<sup>51</sup> CDR Rule 4.16. See also 'reasonably identifiable' in [Chapter B \(Key concepts\)](#).

<sup>52</sup> CDR Rule 1.17A(2).



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

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

## Step 4: Destroying redundant data

12.92 If the accredited data recipient chooses under Step 3 to destroy the redundant data, then they must proceed to destroy the data in accordance with the 'CDR data deletion process' set out in the CDR Rules.<sup>53</sup> 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

12.93 Once an accredited data recipient has determined the de-identification process could apply, and the accredited data recipient is interested in pursuing this option, it must consider whether the CDR de-identification process will ensure that the data is de-identified in accordance with the CDR Rules.

12.94 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.<sup>54</sup>

12.95 Based on the above considerations, the accredited data recipient must determine whether it would be possible to de-identify the relevant data so that no person would any longer be identifiable, or reasonably identifiable, from:

- the relevant data after the proposed de-identification, and
- other information that would be held, following the proposed de-identification, by any person (the 'required extent').

12.96 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

---

<sup>53</sup> CDR Rule 1.18

<sup>54</sup> CDR Rule 1.17(1).

released into an open environment, or what controls and safeguards apply to the data access environment).<sup>55</sup>

12.97 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.

12.98 De-identification will be possible only where CDR data has been through an extremely robust de-identification process that ensures, with a very high degree of confidence, that no consumers are reasonably identifiable.

12.99 Accredited data recipients should be aware that there is significant complexity and risk involved with attempting to de-identify unit record data derived from CDR data to the 'required extent' as defined in the CDR Rules.

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

12.100 If, having taken the steps outlined in this section, the accredited data recipient determines that it is possible to de-identify the redundant data to the required extent<sup>56</sup>, they can then proceed to de-identify the data in accordance with the 'CDR data de-identification process' set out in the CDR Rules.<sup>57</sup> This process is explained further below under 'Steps to de-identify redundant data'.

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

12.101 If, having taken the steps outlined above, the accredited data recipient determines it is not possible to de-identify the data to the required extent, the accredited data recipient must delete the CDR data and any derived data in accordance with the CDR data deletion process set out in the CDR Rules, and explained below under 'Steps to destroy redundant data'.<sup>58</sup>

### **Steps to destroy redundant data**

12.102 The CDR Rules provide that the CDR data deletion process is to be applied for the purposes of destroying redundant data under Privacy Safeguard 12.<sup>59</sup> The CDR data deletion process is set out in CDR Rule 1.18.

12.103 CDR Rule 1.18 provides that CDR data is to be deleted using the following steps:

- delete, to the extent reasonably practicable, CDR data and any copies of that data
- make a record to evidence the deletion, and

---

<sup>55</sup> CDR Rule 1.17(2)(f).

<sup>56</sup> See paragraphs 12.91 to 12.99.

<sup>57</sup> CDR Rule 1.17.

<sup>58</sup> CDR Rule 1.17(4).

<sup>59</sup> CDR Rule 7.13.

- where another person holds the CDR data on behalf of an accredited data recipient and will perform the steps above, that accredited data recipient must direct that person to notify it when the steps are complete.<sup>60</sup>

12.104 This process applies:

- to the deletion of CDR data in response to a consumer's election,
- where the entity otherwise chooses to delete the redundant data in order to comply with their Privacy Safeguard 12 obligations, and
- where it is not possible to de-identify the CDR data to the required extent (see Step 5 above).

## Deleting the CDR data 'to the extent reasonably practicable'

12.105 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.<sup>61</sup>

12.106 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, and
- the **practicability, including time and cost involved** — however an accredited data recipient is not excused from deleting CDR data by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take a particular step will depend on whether the burden is excessive in all the circumstances.

## What if CDR data cannot practically be deleted?

12.107 The CDR Rules recognise that irretrievable destruction of CDR data such as from a back-up system or a database more generally is not always straightforward, and it may not be possible to achieve this immediately (for example, archived data that could be re-installed).

---

<sup>60</sup> Currently, an accredited data recipient is authorised to disclose CDR data to an outsourced service provider, another accredited person or the consumer to which the CDR data relates (CDR Rule 7.5(1)).

<sup>61</sup> CDR Rule 1.18(a).

12.108 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, and<sup>62</sup>
- commits to take reasonable steps to irretrievably destroy the data if, or when, this becomes possible.

12.109 It is important to note that the accredited data recipient must continue to take reasonable steps to work towards a solution to eventually delete the CDR data.

**Privacy tip:** If a consumer requests deletion of their redundant data but the accredited data recipient determines that it is required to retain the data under a relevant law, court/tribunal order, or because of legal or dispute resolution proceedings, the entity should notify the consumer in writing of the reasons that their request was not complied with.

## Steps to de-identify redundant data

12.110 If the accredited data recipient determines that it is possible to de-identify the data to the required extent, it must determine and apply the appropriate de-identification technique (or techniques).<sup>63</sup>

12.111 Specifically, the accredited data recipient must:

- determine the technique/s appropriate in the circumstances
- apply that technique/s to de-identify the relevant data to the required extent, and
- delete, in accordance with the CDR data deletion process, any CDR data that must be deleted to ensure that no person is any longer identifiable or reasonably identifiable.<sup>64</sup>

12.112 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.

---

<sup>62</sup> This should go beyond the minimum access controls specified in the CDR Rules.

<sup>63</sup> CDR Rule 1.17(3). This determination is a point in time assessment, i.e. with the technology available at that time rather than technology that may become available (such as quantum computing, for instance) in the future.

<sup>64</sup> CDR Rule 1.17(3).

12.113 If the accredited data recipient determines that it is not possible to de-identify CDR data using the appropriate technique, it must delete the relevant data and any CDR data directly or indirectly derived from it.

## De-identifying data that has been provided to an outsourced service provider

12.114 Where an accredited data recipient has provided an outsourced service provider with CDR data that then becomes redundant, the accredited data recipient cannot rely on that outsourced service provider to undertake the de-identification process on their behalf.

12.115 In this situation, an accredited data recipient must direct the outsourced service provider to either:

- return the redundant data, as well as any data directly or indirectly derived from it.<sup>65</sup> The accredited data recipient can then determine whether it is possible to de-identify the redundant data to the required extent, and if so, de-identify the data in accordance with the CDR data de-identification process (as it would with any other redundant data),<sup>66</sup> or
- delete the redundant data, as well as any data directly or indirectly derived from it.<sup>67</sup>

12.116 The accredited data recipient is responsible for ensuring these directions are made to any other person who has received the data.<sup>68</sup> If the outsourced service provider has also disclosed the data to another person, the accredited data recipient must ensure that that person receives a direction to return or delete the data. If that person has also disclosed the data, the accredited data recipient must ensure that person receives such a direction.<sup>69</sup> For information about the meaning of outsourced service provider, see Chapter B (Key concepts).

## Other relevant security obligations

### Privacy safeguards

12.117 Compliance with the privacy safeguards as a whole will promote security and reduce the risk of CDR data being accidentally or deliberately compromised. This is because the privacy 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.

12.118 Privacy Safeguard 1 requires entities to take reasonable steps to establish and maintain practices, procedures, and systems to ensure compliance with the privacy safeguards, including Privacy Safeguard 12. [Privacy Safeguard 1 also requires that certain information](#)

---

<sup>65</sup> CDR Rule 7.12(2)(b).

<sup>66</sup> CDR Rule 1.17.

<sup>67</sup> CDR Rule 7.12(2)(b).

<sup>68</sup> The outsourced service provider is required to comply with this direction. See CDR Rule 1.10.

<sup>69</sup> CDR Rule 7.12(2)(b)(ii).

about the deletion and de-identification of redundant data must be provided in an accredited data recipient's CDR Policy (see Chapter 1 (Privacy Safeguard 1)).

12.119 Privacy Safeguard 3 limits the collection of CDR data, which is an effective risk management practice reducing the scope of data that may be accessed in the case of a cyber-attack (see Chapter 3 (Privacy Safeguard 3)).

12.120 Privacy Safeguard 4 contains requirements to destroy information if it is unsolicited and not required to be retained by the entity (see Chapter 4 (Privacy Safeguard 4)). This minimises the amount of data held by an entity and the amount of time the entity holds that information, reducing overall risk of data breach.

## Other CDR de-identification processes

12.121 There are separate requirements under the CDR Rules to follow when de-identifying CDR data that is not 'redundant data'.<sup>70</sup>

12.122 For example, an accredited person must seek a consent from the consumer to:

- use the de-identified data for general research,<sup>71</sup> and/or
- disclose (including by selling) the de-identified data.

12.123 For further information on seeking consent to use de-identified CDR data that is not redundant data, see Chapter C – Consent.

---

<sup>70</sup> CDR Rule 7.5(1)(aa).

<sup>71</sup> 'General research' is defined in CDR Rule 1.7 to mean research undertaken by an accredited data recipient with CDR data de-identified in accordance with the CDR Rules that does not relate to the provision of goods or services to any particular CDR consumer.

# Chapter 13:

# Privacy Safeguard 13 —

## Correction of CDR data

Version 3.0, June 2021

# Contents

<b>Key points</b>	<b>3</b>
<b>What does Privacy Safeguard 13 say?</b>	<b>3</b>
<b>Why is it important?</b>	<b>3</b>
<b>Who does Privacy Safeguard 13 apply to?</b>	<b>4</b>
<b>How Privacy Safeguard 13 interacts with the Privacy Act</b>	<b>4</b>
<b>When must an entity correct CDR data?</b>	<b>5</b>
<b>Actioning and responding to correction requests</b>	<b>5</b>
Acknowledging receipt of correction requests	5
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?	9
<b>What are the correction considerations?</b>	<b>9</b>
Accurate	10
Up to date	10
Complete	11
Not misleading	11
<b>Charges to correct CDR data</b>	<b>12</b>
<b>Interaction with other privacy safeguards</b>	<b>12</b>
Privacy Safeguard 5	12
Privacy Safeguard 10	12
Privacy Safeguard 11	12
Privacy Safeguard 12	12



## Key points

- Privacy Safeguard 13, together with consumer data rules (CDR Rules) 7.14 and 7.15, sets out obligations for data holders and accredited data recipients of CDR data to:
  - respond to correction requests made by consumers in respect of the consumer data right (CDR) data, and to take certain steps to correct or include a qualifying statement in respect of the data, and
  - give the 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 of a consumer's CDR data who:

- receive a request from the consumer to correct their CDR data, and
- in the case of data holders, were earlier required or authorised under the CDR Rules to disclose the CDR data

to respond to the request by taking the relevant steps set out in the CDR Rules.

13.2 CDR Rule 7.15 requires an entity to acknowledge receipt of the request as soon as practicable and sets out how the entity must, within 10 business days after receipt of the request, and to the extent it considers appropriate:

- correct the CDR data, or
- qualify the data by including a statement with it.

13.3 The entity must also give the consumer a notice setting out how they responded to the request, as well as the complaint mechanisms available to the consumer.

13.4 CDR Rule 7.14 prohibits charging a fee for responding to or actioning a correction request.

## Why is it important?

13.5 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.

13.6 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.

13.7 Privacy Safeguard 13 does this by ensuring entities are required to correct CDR data in certain circumstances when requested to do so by the consumer.

13.8 This allows consumers to enjoy the benefits of the CDR regime, such as receiving competitive offers from other service providers, as the accuracy of the data made available to sector participants can be relied upon.

## Who does Privacy Safeguard 13 apply to?

13.9 Privacy Safeguard 13 applies to data holders and accredited data recipients of CDR data. It does not apply to designated gateways.

13.10 Importantly, in relation to data holders, Privacy Safeguard 13 only applies where a consumer has requested that a data holder correct their CDR data and the data holder was earlier required or authorised to disclose it under the CDR Rules.<sup>1</sup> APP 13 will continue to apply to CDR data that is personal information in all other circumstances. For example, where the consumer makes a correction request, but the data has not previously been disclosed under the CDR Rules.

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

## How Privacy Safeguard 13 interacts with the Privacy Act

13.11 It is important to understand how Privacy Safeguard 13 interacts with the *Privacy Act 1988* (the Privacy Act) and the Australian Privacy Principles (APPs).<sup>2</sup>

13.12 APP 13 requires an APP entity to correct personal information held by the entity in certain circumstances.

CDR entity	Privacy protections that apply in the CDR context
<b>Accredited data recipient</b>	<p><b>Privacy Safeguard 13</b></p> <p>For an accredited data recipient of CDR data, Privacy Safeguard 13 applies to the correction of that CDR data.<sup>3</sup></p> <p>APP 13 does not apply in relation to that CDR data.<sup>4</sup></p>

<sup>1</sup> Section 56EP(1)(c) of the Competition and Consumer Act.

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

<sup>3</sup> Privacy Safeguard 13 applies from the point when the accredited person becomes an accredited data recipient of the CDR data. An accredited person becomes an accredited data recipient for CDR data when:

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

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

CDR entity	Privacy protections that apply in the CDR context
<b>Data holder</b>	<p><b>Privacy Safeguard 13 or APP 13</b></p> <p>Privacy Safeguard 13 applies instead of APP 13 where a consumer has requested that a data holder correct their CDR data, and the data holder was earlier required or authorised to disclose it under the CDR Rules.</p> <p>APP 13 will continue to apply to CDR data that is personal information in all other circumstances. This includes where:</p> <ul style="list-style-type: none"> <li>the consumer makes a correction request, but the data has not previously been disclosed under the CDR Rules, or</li> <li>the consumer has not made a correction request, but the APP entity is satisfied that the data it holds is incorrect.<sup>5</sup></li> </ul>
<b>Designated gateway</b>	<p><b>APP 13</b></p> <p>Privacy Safeguard 13 does not apply to designated gateways.</p>

## When must an entity correct CDR data?

13.13 Privacy Safeguard 13 and CDR 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.<sup>6</sup>

## Actioning and responding to correction requests

### Acknowledging receipt of correction requests

13.14 When a consumer makes a request to correct their CDR data, CDR Rule 7.15(a) requires the entity to acknowledge receipt of a correction request as soon as practicable.

13.15 An entity must 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.

13.16 However, it is not a requirement that this acknowledgement be in writing or through the dashboard. For example, acknowledgement provided by other electronic means or over the phone is sufficient. Where an entity acknowledges receipt over the phone, it could also make a record of this as evidence that it has complied with CDR Rule 7.15(a).

<sup>5</sup> Specifically, a data holder who is also an APP entity must continue to take reasonable steps to correct CDR data that is personal information where it is inaccurate, out-of-date, incomplete, irrelevant or misleading for the purpose for which it is held under APP 13.

<sup>6</sup> For data holders, this obligation only arises if the entity was required or authorised under the CDR Rules to disclose the CDR data.

13.17 In adopting a timetable that is ‘practicable’, an entity can take technical and resource considerations into account. However, it is the responsibility of the entity to justify any delay in acknowledging receipt of a request.

## Taking action to correct, or qualify, the CDR data

13.18 CDR Rule 7.15 requires an entity that receives a correction request to either:

- correct the CDR data, or
- both:
  - include a qualifying statement with the data to ensure that, having regard to the purpose for which it is held, the data is accurate, up to date, complete and not misleading, and
  - where practicable, attach an electronic link to a digital record of the data in such a way that the statement will be apparent to any users of the data.

The entity must take one of these steps within 10 business days after receipt of the request, and to the extent that the entity considers appropriate.

13.19 The 10 business day time period commences on the day after the entity receives the request.<sup>7</sup> For example, if the entity receives the request on 2 August, the 10 business day period begins on 3 August.

13.20 A ‘business day’ is a day that is not Saturday, Sunday or a public holiday in the place concerned.

13.21 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).

13.22 The requirement to, where practicable, attach an electronic link to a digital record of the data helps to ensure that any qualifying statement included with the data is clear to those who access the data. An entity’s systems should be set up so that the data cannot be accessed without the correction statement or a link to that statement being immediately apparent.

13.23 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.

13.24 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

---

<sup>7</sup> See s 36 of the *Acts Interpretation Act 1901*.

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

- 13.25 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, for the purpose it is held.
- 13.26 In such circumstances, the entity must give the CDR consumer a notice in accordance with CDR 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.<sup>8</sup>
- 13.27 Reasons for not correcting CDR data or including a qualifying statement with the data may include:
- while there are inaccuracies in the data, it is nevertheless correct for the purpose for which it is held
  - the CDR consumer is mistaken and has made the correction request in error
  - the CDR consumer is attempting to prevent an accredited person from collecting accurate CDR data that is unfavourable to the consumer
  - the entity is an accredited data recipient of the data, but 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),<sup>9</sup> with the effect that the consumer should make the request to the data holder, or
  - the CDR data has already been corrected, or a qualifying statement already included with the data, on a previous occasion.

### Example

Jessica defaults on her credit card repayments with data holder, BankaLot Ltd. Jessica authorises BankaLot to disclose her CDR data to accredited person, CreditCardFinder Pty Ltd, which sends BankaLot a consumer data request on Jessica's behalf. Shortly after Jessica is notified that the data has been collected, Jessica requests CreditCardFinder to correct 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 Jessica a notice through her consumer dashboard that states

*cont*

<sup>8</sup> Section 56EP(3)(b) of the Competition and Consumer Act.

<sup>9</sup> Note that data derived from CDR data collected by an accredited data recipient continues to be 'CDR data': see s 56AI of the Competition and Consumer Act.

this finding, and that if Jessica wants the data to be corrected, she should request that BankaLot make the relevant correction.

The notice also sets out the complaint mechanisms available to Jessica, which are in line with the corresponding section in CreditCardFinder's CDR policy.

## How to respond to a correction request

Entity receives a correction request from consumer



Entity acknowledges receipt of request as soon as practicable



Within 10 business days after receiving the request, and to the extent the entity considers appropriate:



Entity corrects the CDR data



Entity includes a statement with the CDR data



Where practicable, entity attaches an electronic link to the digital record of the CDR data



Entity takes no action



Entity provides consumer with a written notice, by electronic means, setting out:

- What the entity did
- If the entity did not consider it appropriate to take any action, why a correction or statement is unnecessary or inappropriate
- Complaint mechanisms available to the consumer

## How must a correction notice be provided to consumers?

13.28 CDR 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. The written notice must contain the matters set out in paragraph 13.32 below.

13.29 The requirement for written notices to be given by electronic means will be satisfied if the notice is given, for example, over email or over the consumer's dashboard.

13.30 The written notice may be in the body of an email or in an electronic file attached to an email.

13.31 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 CDR Rule 7.15(c) would likely make the SMS very long.

## What must be included in a correction notice to consumers?

13.32 The correction notice to the consumer must set out:

- what the entity did in response to the request
- if the entity did not consider it appropriate to take any action, why a correction or statement is unnecessary or inappropriate, and
- the complaint mechanisms available to the consumer.

13.33 The complaint mechanisms available to the consumer that must be included in the notice are:

- the entity's internal dispute resolution processes relevant to the consumer, including any information from the entity's CDR policy about the making of a complaint relevant to the entity's obligations to respond to correction requests, and
- external complaint mechanisms the consumer is entitled to access, including the consumer's right to complain to the Australian Information Commissioner under Part V of the Privacy Act,<sup>10</sup> and any external dispute resolution schemes recognised by the Australian Competition and Consumer Commission under s 56DA(1) of the Competition and Consumer Act.

13.34 An entity may, but is not required to, advise the consumer that if they have suffered loss or damage by the entity's acts or omissions in contravention of the privacy safeguards or CDR Rules, they have a right to bring an action for damages in a court of competent jurisdiction under s 56EY of the Competition and Consumer Act.

## What are the correction considerations?

13.35 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'.<sup>11</sup> 'Held' is discussed in [Chapter B \(Key concepts\)](#).

13.36 Whether or not CDR data is accurate, up to date, complete and not misleading must be determined with regard to the purpose for which it is held.

13.37 When working out the purpose for which the CDR data is or was held, entities must disregard the purpose of holding the CDR data so that it can be disclosed as required under the CDR

---

<sup>10</sup> Section 56ET(4) of the Competition and Consumer Act.

<sup>11</sup> Section 56EP(3)(a)(ii) of the Competition and Consumer Act.

Rules.<sup>12</sup> 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 \(Key concepts\)](#).

13.38 These four terms are not defined in the Competition and Consumer Act or the Privacy Act.<sup>13</sup>

13.39 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*.<sup>14</sup> As the analysis indicates, there is overlap in the meaning of the terms.

## Accurate

13.40 CDR data is inaccurate if it contains an error or defect or is misleading. An example is factual information about a consumer’s income, assets, loan repayment history or employment status which is incorrect for the purpose it is held.

13.41 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.<sup>15</sup> 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 the existing information it holds on a consumer to predict their 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 (that is, it is based on the consumer’s income over the previous certain number of financial years), this would not be inaccurate solely because, for instance, the consumer believes their income will be higher or lower during the projected period.

13.42 CDR data may be inaccurate even if it is consistent with a consumer’s instructions or if the inaccuracy is attributable to the consumer.

## Up to date

13.43 CDR data is not up to date if it contains information that is no longer current. An example is a statement that a consumer has an active account with a certain 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.<sup>16</sup>

13.44 CDR data about a past event may have been up to date at the time it was recorded but has been overtaken by a later development. Whether that data is up to date will depend on the purpose for which it is held. If, for instance, a consumer has had their second child but their

---

<sup>12</sup> Section 56EP(4) of the Competition and Consumer Act.

<sup>13</sup> 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 \(Privacy Safeguard 11\)](#) for further information and for examples of an entity determining the purpose for which it holds CDR data.

<sup>14</sup> See [Chapter 10: APP 10 — Quality of personal information of the APP Guidelines](#).

<sup>15</sup> Data derived from CDR data continues to be ‘CDR data’: see s 56AI of the Competition and Consumer Act.

<sup>16</sup> Such an assessment will likely be ‘materially enhanced information’ under section 10 of the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019 and therefore not ‘required consumer data’ under the CDR Rules.



CDR data records them as only having one child, the CDR data will still be up to date if the data that records the consumer as having one child is held simply for the purpose of recording whether the consumer is a parent.

- 13.45 In a similar manner to accuracy, CDR data may not be up to date even if it is consistent with a consumer's instructions or if the inaccuracy is attributable to the consumer.

## Complete

- 13.46 CDR data is incomplete if it presents a partial or misleading picture of a matter of relevance, rather than a true or full picture.
- 13.47 An example is data from which it can be inferred that a consumer owes a debt, which in fact has been repaid. The CDR data will be incomplete under Privacy Safeguard 13 if the data is held, for instance, for the purpose of determining the borrowing capacity of the consumer. Where the CDR data is held for a different purpose for which the debt is irrelevant, the fact that the debt has been repaid may not of itself render the CDR data incomplete. If, however, the accredited person has requested a consumer's CDR data for a specific period, and in that period the consumer owed a debt which is recorded in the CDR data, and that debt was repaid in a later period, the CDR data will still be 'complete' in respect of that specific period.

## Not misleading

- 13.48 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.
- 13.49 Data may also be misleading if other relevant information is not included.

### Example

Angelica consents to XYZ Solutions Pty Ltd (XYZ) (an accredited person) collecting her CDR data from Good Faith Banking and Insurance Ltd (GFBI) (a data holder), and using that data for the purpose of providing Angelica with recommendations for various insurance products.

Angelica has previously spoken with GFBI employee, Bert, about insurance products offered by GFBI and been mistakenly advised that she has mortgage protection when she does not. Bert had recorded, as part of Angelica's CDR data, that Angelica has mortgage protection insurance.

If Angelica requests that XYZ or GFBI correct her CDR data, the entity may include a statement with the data that Angelica does not have the insurance product. Alternatively, the entity may delete or alter the relevant part of the data to make clear that Angelica does not have the insurance product. If any one of these actions was taken, the data would no longer be inaccurate or misleading.

## Charges to correct CDR data

13.50 CDR 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

13.51 Privacy Safeguard 5 requires an accredited data recipient of CDR data to notify a consumer of the collection of their CDR data by updating the consumer's dashboard.

13.52 Where an accredited person has collected CDR data, and then collects corrected data after the data holder or accredited data recipient complies with the consumer's requests to correct and disclose corrected data under Privacy Safeguards 11 and 13, the accredited person must notify that consumer under Privacy Safeguard 5 in respect of both collections.

### Privacy Safeguard 10

13.53 Privacy Safeguard 10 requires a data holder and accredited data recipient to notify a CDR consumer of the disclosure of their CDR data by updating the consumer's dashboard.

13.54 Where a data holder or accredited data recipient 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 entity must notify that consumer under Privacy Safeguard 10 in respect of both disclosures.

### Privacy Safeguard 11

13.55 A correction request made under Privacy Safeguard 13 may trigger a CDR entity's obligations under Privacy Safeguard 11 (Quality of CDR data).

13.56 Under Privacy Safeguard 11, data holders and accredited data recipients have an obligation to advise consumers if they disclose CDR data at a point in time, but then later become aware that some or all of the data disclosed was inaccurate, out of date or incomplete, having regard to the purpose for which the data was held at the time of disclosure.

13.57 A CDR entity may become aware of inaccuracies in CDR data in a range of ways – including pursuant to a correction request under Privacy Safeguard 13.

13.58 Therefore, an entity that corrects CDR data, or includes a qualifying statement with such data in accordance with Privacy Safeguard 13, must also consider whether the consumer must be advised of any previous disclosures of incorrect CDR data, in accordance with Privacy Safeguard 11.<sup>17</sup>

### Privacy Safeguard 12

13.59 Where an accredited data recipient corrects CDR data to comply with Privacy Safeguard 13, it should consider whether it needs to take action under Privacy Safeguard 12 to destroy or de-identify the original data.

---

<sup>17</sup> Section 56EN(3) of the Competition and Consumer Act.