Australian Government
Office of the Australian Information Commissioner

Consumer Data Right

Privacy Safeguard Guidelines

Version 2.0 July 2020

OAIC

Contents

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

Chapter A:

Introductory matters

Version 2.0, July 2020

OAIC

Contents

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.[1]

A.2 The Privacy Safeguard guidelines are made in order to guide entities on avoiding acts or practices that may breach the privacy safeguards, which are set out in Division 5 of Part IVD of the Competition and Consumer Act.

A.3 Part IVD of the Competition and Consumer Act is the legislative base for the consumer data right (CDR) regime.

A.4 The Privacy Safeguard guidelines outline:

- the mandatory requirements in the privacy safeguards and related consumer data rules (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.

[1] 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 will all be able to exercise the CDR in relation to data that is covered by the CDR regime.

A.9 The CDR will be rolled out in stages starting with the banking sector (known as 'Open Banking'). Next, CDR will be implemented in the energy and telecommunication sectors. It will then be introduced sector by sector across the broader economy.

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

A.12 The privacy safeguards only apply to CDR data for which there are one or more consumers.[2] This means that if there is no person that is identifiable or reasonably identifiable from the

[2] Section 56EB(1) of the Competition and Consumer Act.

CDR data,[3] because, for instance, it is product data for which there is no consumer, the privacy safeguards do not apply.

A.13 The privacy safeguards are structured to reflect the CDR data lifecycle. They are grouped into five subdivisions within Division 5 of Part IVD of the Competition and Consumer Act:

- Subdivision B — Consideration of CDR data privacy (Privacy Safeguards 1 and 2)
- Subdivision C — Collecting CDR data (Privacy Safeguards 3, 4 and 5)
- Subdivision D — Dealing with CDR data (Privacy Safeguards 6, 7, 8, 9 and 10)
- Subdivision E — Integrity of CDR data (Privacy Safeguards 11 and 12)
- Subdivision F — Correction of CDR data (Privacy Safeguard 13)

A.14 The requirements in each of these privacy safeguards interact with and complement each other.

How to use these guidelines

A.15 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.16 The number of the chapter corresponds to the number of the privacy safeguard.

A.17 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.18 Chapter C contains guidance on consent, which is the primary basis for collecting and using CDR data under the CDR regime.

A.19 These guidelines should be read together with the full text of Division 5 of Part IVD of the Competition and Consumer Act and the CDR Rules.

Who must comply with the privacy safeguards?

A.20 The privacy safeguards apply to entities who are authorised or required under the CDR regime to collect, use or disclose CDR data for which there is at least one consumer. This includes:

- **accredited persons:** persons who have been granted accreditation by the Australian Competition and Consumer Commission to receive data through the CDR regime[4]
- **accredited data recipients:** accredited persons who have collected the CDR data from a data holder or another accredited data recipient[5]
- **data holders:** the holders of the original data that the transfer of data applies to, [6] and

[3] Section 56AI(3)(c) of the Competition and Consumer Act.

[4] For specific requirements, see section 56CA of the Competition and Consumer Act.

[5] For specific requirements, see s 56AK of the Competition and Consumer Act.

[6] For specific requirements, see s 56AJ of the Competition and Consumer Act.

- **designated gateways:** entities designated by the Minister as responsible for facilitating the transfer of information between data holders and accredited persons.[7]

A.21 Each of these types of entities are defined in the Competition and Consumer Act and discussed further in Chapter B (Key concepts).

A.22 Each privacy safeguard chapter specifies the type of entity to which it applies.

A.23 The privacy safeguards extend to acts, omissions, matters and things outside Australia.[8]

A.24 In respect of CDR data held within Australia, the privacy safeguards apply to all persons, including foreign persons.[9]

A.25 In respect of an act or omission relating to CDR data held outside Australia, the privacy safeguards only apply if the act or omission:[10]

- is done by or on behalf of an Australian person
- occurs wholly or partly in Australia, or wholly or partly on board an Australian aircraft or an Australian ship, or
- occurs wholly outside Australia, and an Australian person suffers, or is likely to suffer, financial or other disadvantage as a result of the act or omission.

Which privacy protections apply in the CDR context?

CDR entity	Privacy safeguards that apply to CDR data[11]	APPs that apply to CDR data
Accredited person	Privacy safeguards 1,[12] 3 and 4	APPs 1, 2, 3 and 4[13]
Accredited data recipient	Privacy safeguards 1, 2 and 5–13	None, however APP 1 will continue to apply generally as the entity will be an accredited person
Data holder	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
Designated gateway	Privacy safeguards 1, 6, 7 and 12	APPs 1–5, 8–10 and 12–13

[7] For specific requirements, see s 56AL(2) of the Competition and Consumer Act.

[8] Section 56AO(1) of the Competition and Consumer Act.

[9] Section 56AO(2) of the Competition and Consumer Act.

[10] Section 56AO(3) of the Competition and Consumer Act.

[11] Note the Privacy Safeguards and/or APPs apply only to CDR data that is also personal information (i.e. not CDR data that is about businesses or corporations).

[12] Privacy Safeguard 1 applies to an accredited person who is an accredited data recipient of any CDR data.

[13] The remaining APPs will not apply to an accredited person in respect of CDR data that is personal information because the accredited person will become an accredited data recipient of the CDR data when it is collected under the CDR Rules.

Note: *The privacy safeguards and/or APPs apply only to CDR data that is also personal information (i.e. not CDR data that is about businesses or corporations).*

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

A.26 Section 56EC(4) of the Competition and Consumer Act sets out when a privacy safeguard applies instead of an APP. However, as set out in the above table, some APPs and privacy safeguards apply concurrently, to ensure there are no gaps in the protection of the data.[14]

A.27 The privacy safeguards apply only to CDR data for which there is one or more CDR consumers.[15] A CDR consumer is an identifiable or reasonably identifiable person to whom the CDR data relates, because of the supply of a good or service to the person (or an associate of the person).[16] As such, 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.28 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.29 In each chapter in these guidelines, the interaction between the privacy safeguard and corresponding APP is discussed.

A.30 See also the flow chart below which demonstrates the privacy protections that apply at various stages of the information flow.

Accredited persons and accredited data recipients

A.31 All accredited persons are subject to the Privacy Act and the APPs.[17]

A.32 For example, an accredited person must also comply with Privacy Safeguard 1 if they have received any CDR data through the CDR regime. Privacy Safeguard 1 will apply concurrently with APP 1. Together, APP 1 and Privacy Safeguard 1 require entities to put ongoing governance measures in place and have a compliant privacy policy and CDR policy in place to ensure the open and transparent management of personal information and CDR data (respectively). The obligations in APP 1 will not be satisfied if only Privacy Safeguard 1 is complied with, as Privacy Safeguard 1 applies only to the management of CDR data (not other personal information). In addition, these principles require entities to ensure compliance with the particularities of all other APPs and the Privacy Safeguards respectively.

[14] See, for example, Note 1 to section 56EC(5) of the Competition and Consumer Act. APP 1 and Privacy Safeguard 1, for example, apply in parallel given that they are general data obligations which may need to apply to regulated entities at all times.

[15] Section 56EB(1) of the Competition and Consumer Act.

[16] A CDR consumer can be an individual, a company, or a business enterprise. See Chapter B (Key concepts) of the CDR Privacy Safeguard Guidelines for further information.

[17] Section 6E(1D) of the Privacy Act.

A.33 When an accredited person receives CDR data through the CDR regime they become an accredited data recipient for that data, and then the applicable privacy safeguards will apply to that CDR data instead of the APPs.

A.34 This means that Privacy Safeguards 2, 5, 6, 7, 8, 9, 11, 12 and 13 generally apply to that data instead of the corresponding APP (2, 5, 6, 7, 8, 9, 10, 11 and 13).

Data holders

A.35 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), which 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 in addition to all other privacy protections.

A.36 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.

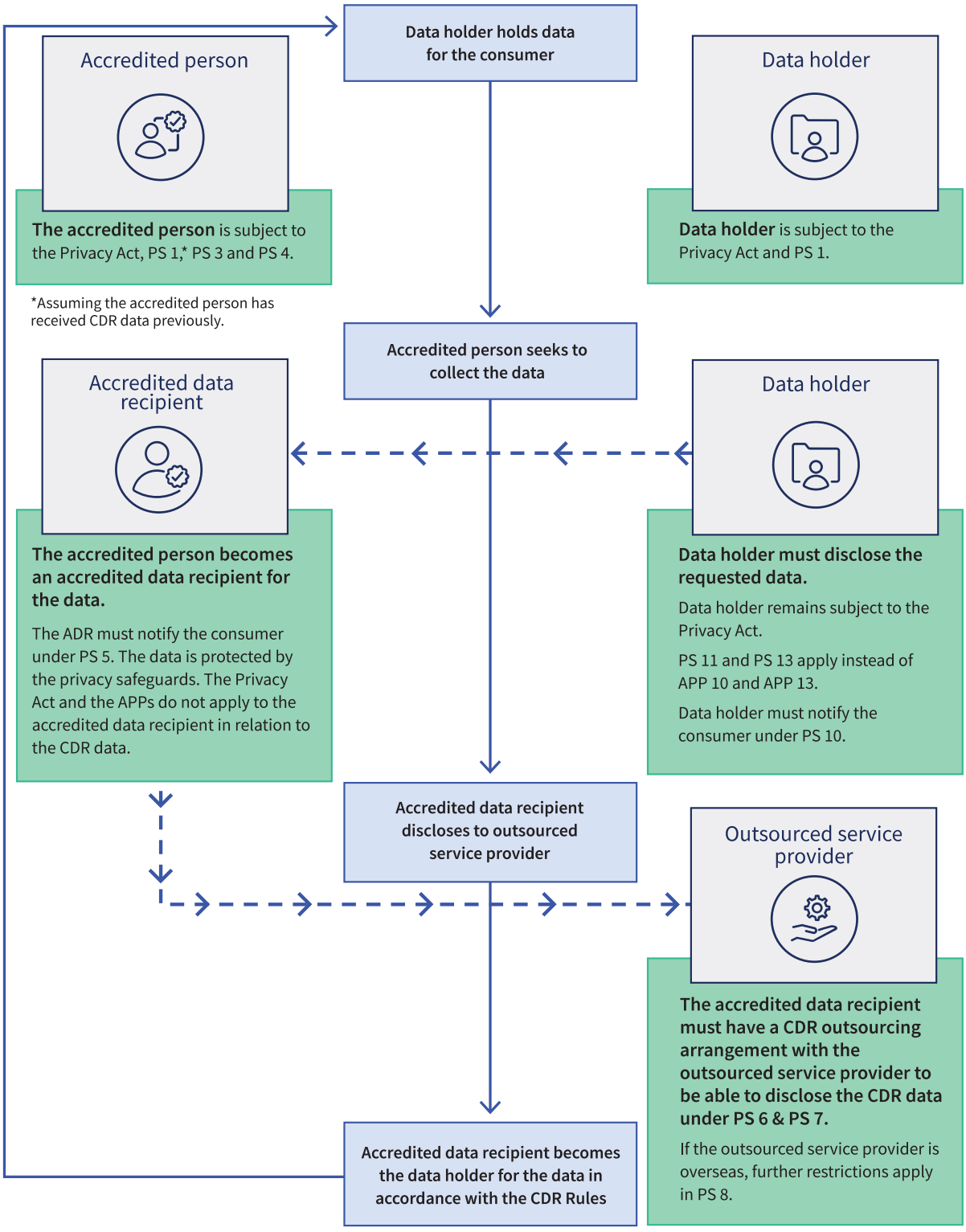
Designated gateways

A.37 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.38 Further, designated gateways must comply with Privacy Safeguard 1 (open and transparent management of CDR data) in addition to APP 1. As explained above, these obligations apply concurrently and the obligations in Privacy Safeguard 1 do not displace the APP 1 obligations.

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

Privacy protections at various stages of the information flow



What happens if an entity breaches the privacy safeguards?

A.39 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.40 Where a consumer makes a complaint, the Information Commissioner will generally attempt to conciliate the complaint.

A.41 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,[18] for example the power to make a determination,[19] 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.[20]

A.42 The Australian Competition and Consumer Commission (ACCC) will also have a strategic enforcement role where there are repeated or serious breaches.

Where do I get more information?

A.43 The Office of the Australian Information Commissioner (OAIC) has further information about the CDR and its role on the OAIC website, see www.oaic.gov.au/consumer-data-right.

[18] 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.

[19] Section 52 of the Privacy Act.

[20] 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 2.0, July 2020

OAIC

Contents

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)[1] 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 for the purposes of comparing credit card rates. Account numbers, balances, and features fall into a class of information set out in the designation instrument for the banking sector,[2] and are therefore **CDR data**.

Data holders

Sunny Bank is a **data holder**. This is because Sunny Bank holds Carly's CDR data, is not a designated gateway for the data, began to hold CDR data after 1 January 2017[3] and is an authorised deposit-taking institution (one of the categories specified in s 56AJ(1)(d) of the Competition and Consumer Act).[4]

---

[1] See paragraph B.11.

[2] Section 56AI(1) of the Competition and Consumer Act. The designation instrument for the banking sector sets out the classes of information that are subject to the CDR regime, the persons who hold this information and will be required or authorised to transfer the information under the regime, and the earliest date that the information must have begun to be held to be subject to the CDR regime.

[3] 1 January 2017 is the 'earliest holding day' specified in the designation instrument for the banking sector: s 5(3) of the designation instrument. See paragraphs B.94 to B.95 for further information.

[4] Sunny Bank is an authorised-deposit taking institution, which has been specified as a relevant class of persons in the designation instrument for the banking sector.

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),[5] and
- Carly is identifiable or reasonably identifiable from the CDR data.[6]

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.[7]

Consumer dashboards

Given that Meadow Bank has made a consumer data request on Carly's behalf, Meadow Bank provides Carly with a **consumer dashboard**.[8] 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.[9]

---

[5] See paragraph B.37 for further information.

[6] Section 56AI(3) of the Competition and Consumer Act.

[7] Section 56AK of the Competition and Consumer Act.

[8] CDR Rule 1.14(1)(a).

[9] CDR Rule 1.15(1)(a).

Accredited data recipient

B.4 A person is an 'accredited data recipient' if the person:

- is an accredited person (see paragraphs B.9-B.12 below)
- was disclosed CDR data from a data holder under the CDR Rules
- holds that CDR data (or has another person hold that CDR data on their behalf), and
- does not hold that CDR data as a data holder or designated gateway.[10]

B.5 A person will only be an 'accredited data recipient' in relation to the CDR data that it has been disclosed under the CDR Rules.[11]

B.6 Where an accredited person seeks consent from a consumer to collect and use CDR data, and subsequently seeks to collect CDR data, they do so as an accredited person because they are yet to collect the CDR data.

B.7 Once an accredited person has been disclosed CDR data under the CDR Rules, they will be both an accredited data recipient and an accredited person. For an illustration of how and when an accredited person becomes an accredited data recipient for CDR data, see the example under paragraph B.3.

B.8 A data holder may be accredited, and therefore be both a data holder and an accredited data recipient.

Accredited person

B.9 An 'accredited person' is a person who has been granted accreditation by the Data Recipient Accreditor.[12]

B.10 In the banking sector for example, an accredited person could be a bank or a fintech that wishes to provide a good or service using CDR data. This is demonstrated by the example under paragraph B.3.

B.11 The Data Recipient Accreditor is the Australian Competition and Consumer Commission (ACCC).[13]

B.12 To be granted an accreditation, the person must satisfy the accreditation criteria in Part 5 of the CDR Rules.

---

[10] Section 56AK of the Competition and Consumer Act. Rather, the person must hold that CDR data as a result of seeking to collect the CDR data from a data holder under the CDR Rules.

[11] If an accredited person is disclosed CDR data otherwise than in accordance with the CDR Rules (for instance, in breach of Privacy Safeguard 3), 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 not a 'small business operator' under the *Privacy Act 1988* (see section 6E(1D) of the Privacy Act).

[12] Section 56CA(1) of the Competition and Consumer Act.

[13] The ACCC has been appointed as the Data Recipient Accreditor by the Treasurer under s 56CG of the Competition and Consumer Act.

Authorise, Authorisation

B.13 An authorisation must meet the requirements set out in the CDR Rules, and be sought in accordance with the data standards.[14]

B.14 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.15 For the banking sector, for requests that relate to joint accounts, in some cases, the data holder might need to seek an authorisation from the other joint account holder.[15]

B.16 For further information, see the Guide to privacy for data holders. See also the example under paragraph B.3 to understand at which point a data holder must seek authorisation from the consumer to disclose CDR data.

CDR data

B.17 'CDR data' is information that is:

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

Derived CDR data

B.18 'Derived CDR data' is data that has been wholly or partly derived from CDR data, or data derived from previously derived data.[18] This means data derived from 'derived CDR data' is also 'derived CDR data'.

B.19 '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.20 A 'CDR participant' is a data holder, or an accredited data recipient, of CDR data.[19]

---

[14] CDR Rule 4.5(2). See Division 4.4 of the CDR Rules.

[15] See clause 4.5 of Schedule 3 to the CDR Rules.

[16] Section 56AI(1) of the Competition and Consumer Act. The designation instrument for the banking sector sets out the classes of information that are subject to the CDR regime, the persons who hold this information and will be required or authorised to transfer the information under the regime, and the earliest date that the information must have begun to be held to be subject to the CDR regime. The designation instrument for the banking sector is available here.

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

[18] Section 56AI(2) of the Competition and Consumer Act.

[19] Section 56AL(1) of the Competition and Consumer Act.

CDR policy

B.21 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.22 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 the Guide to developing a CDR policy.

CDR receipt

B.23 A 'CDR receipt' is a notice given by an accredited person to a CDR consumer who has consented to the accredited person collecting and using their CDR data, or given to a consumer who has withdrawn such a consent.[20]

B.24 CDR receipts must be given in accordance with CDR Rule 4.18.

CDR regime

B.25 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.26 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.27 'Collect' is not defined in the Competition and Consumer Act or the Privacy Act.

B.28 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.29 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).[21]

[20] CDR Rule 4.18(1).

[21] '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.

Consent

B.30 Consent must meet the requirements set out in the CDR Rules.

B.31 Consent is the primary basis on which an accredited person may collect and use CDR data.[22]

B.32 Consent also underpins how an accredited person or accredited data recipient may collect and use CDR data in the CDR regime.[23]

B.33 For further information, including the requirements by which an accredited person must seek consent from a consumer, see Chapter C (Consent).

Consumer, CDR consumer or 'eligible' CDR consumer

B.34 The 'CDR consumer' is the person who is able 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.

B.35 A CDR consumer is an identifiable or reasonably identifiable person to whom the CDR data relates, because of the supply of a good or service either to the person or an associate of the person. [24] A consumer can be an individual, another person such as a company, or a business enterprise.[25]

B.36 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.[26]

B.37 The CDR data that relates to the 'CDR consumer' must be held by:

- a data holder of the CDR data
- an accredited data recipient of the CDR data, or
- an entity that holds the data on behalf of a data holder or accredited data recipient of the CDR data.[27]

---

[22] 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 CDR data. See Chapter 6 (Privacy Safeguard 6) for further information regarding use of CDR data.

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

[24] 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.

[25] Section 56AI(4) of the Competition and Consumer Act; Explanatory Memorandum, *Treasury Laws Amendment (Consumer Data Right) Bill 2019*, paragraph 1.100.

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

[27] Section 56AI(3) of the Competition and Consumer Act.

B.38 Section 4B(1) of the Competition and Consumer Act does not apply for the purposes of determining whether a person is a 'CDR consumer'.[28] This section explains when a person is taken to have acquired particular goods or services as a consumer, outside of the CDR regime.

B.39 These guidelines use the term 'consumer' to refer to 'CDR consumer'.

Reasonably identifiable

B.40 For a person to be a 'CDR consumer', the person must be identifiable, or 'reasonably identifiable', from the CDR data or other information held by the entity.

B.41 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.56-B.58 for a discussion on the meaning of 'held') and
- whether it is practicable to use that information to identify the person.

B.42 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.43 See B.122-B.125 for a discussion on the meaning of 'reasonably'.

Relates to

B.44 For a person to be a 'CDR consumer', CDR data must 'relate to' that person.

B.45 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.[29] The relevant context in the CDR regime is the Competition and Consumer Act and the Privacy Act.

B.46 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.[30]

B.47 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.48 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

[28] Section 56AI(4) of the Competition and Consumer Act.

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

[30] Section 56AI(3)(a) of the Competition and Consumer Act.

goods or services which the data concerns (see the discussion of 'associate' at B.49-B.53 below).

B.49 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.[31]

B.50 By using the broad phrase 'relates to', the CDR regime captures meta-data.[32]

Associate

B.51 For a person to be a CDR consumer, CDR data must relate to that person because of the supply of a good or service to the person or one or more of that person's 'associates'.

B.52 In this context, 'associate' has the same meaning as in the *Income Tax Assessment Act 1936* (ITA Act).[33] Section 318 of the ITA Act defines 'associates' with respect to natural persons, companies, trustees and partnerships.[34]

B.53 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.54 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.55 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.

Held

B.56 CDR data that relates to a CDR consumer must be 'held' by:

- a data holder of the CDR data
- an accredited data recipient of the CDR data, or
- an entity that holds the data on behalf of a data holder or accredited data recipient of the CDR data.[35]

---

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

[32] 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.

[33] Section 56AI(3) of the Competition and Consumer Act.

[34] For the purposes of the CDR regime, associates of partnerships are not directly relevant, as a partnership is not a 'person'.

[35] Section 56AI(3) of the Competition and Consumer Act.

B.57 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)[36] that contains the information.[37] This definition is comparable to the definition of 'holds' in the Privacy Act.[38]

B.58 If a person has a right or power to deal with particular data, the person has effective control of the data and therefore 'holds' the data.

Eligible CDR consumer

B.59 While 'CDR consumer' is defined in the Competition and Consumer Act, only 'eligible' CDR consumers may make consumer data requests under the CDR Rules.

B.60 A consumer for the banking sector is 'eligible' if, at that time:

- for any consumer – the consumer has an account with the data holder that is open and set up in such a way that it can be accessed online, and
- for a consumer that is an individual – the consumer is 18 years or older.[39]

B.61 For guidance regarding 'consumers' and 'CDR consumers', see paragraphs B.34 – B.39.

Consumer dashboard, or dashboard

B.62 Each accredited person and each data holder must provide a 'consumer dashboard' for CDR consumers.

B.63 An accredited person's consumer dashboard is an online service that can be used by CDR consumers. Each dashboard is visible only to the accredited person and the relevant CDR consumer.

- CDR consumers can use their dashboard to manage consumer data requests and associated consents for the accredited person to collect and use CDR data.
- The service must also notify the consumer of information related to CDR data collected pursuant to a consent.

B.64 A data holder's consumer dashboard is an online service that can be used by each CDR consumer to manage authorisations to disclose CDR data in response to consumer data requests. The service must also notify the consumer of information related to CDR data disclosed pursuant to an authorisation.

B.65 These guidelines use the term 'dashboard' and 'consumer dashboard' interchangeably.

Consumer data request

B.66 A 'consumer data request' is either:

[36] 'Record' is defined in s 6(1) of the Privacy Act.

[37] Section 4(1) of the Competition and Consumer Act.

[38] Section 6(1) of the Privacy Act.

[39] Clause 2.1 of Schedule 3 to the CDR Rules.

- a request made directly by a CDR consumer to a data holder,[40] or
- a request made by an accredited person to a data holder, on behalf of a CDR consumer, in response to the consumer's valid request for the accredited person to seek to collect the consumer's CDR data.[41]

B.67 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.[42]

B.68 A request from an accredited person must be made through the data holder's accredited person request service and must relate only to data the person has consent from the consumer to collect and use. A request from an accredited person must comply with the data minimisation principle.[43]

B.69 Refer to Chapter C (Consent) for further information.

Direct request service

B.70 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.[44]

B.71 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.72 This service must conform with the data standards.

Accredited person request service

B.73 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.[45]

B.74 It also allows accredited persons to receive requested data in machine-readable form.

B.75 This service must conform with the data standards.

Valid consumer data request

B.76 A consumer data request is 'valid' if it is made directly by an eligible CDR consumer.[46]

---

[40] CDR Rule 3.3(1).

[41] CDR Rule 4.4(1).

[42] CDR Rule 3.3(1). For the banking sector, it is not currently possible for a consumer to make a consumer data request directly to a data holder. This is because the ACCC has exempted data holders in the banking sector from complying with the direct to consumer data sharing obligation in Rule 3.4(3) and all related CDR Rules until 1 November 2021. For further information about these exemptions, see the 'Consumer data right exemptions register' on the ACCC's website.

[43] CDR Rule 4.4(1).

[44] CDR Rule 1.13(2). For the banking sector, it is not currently possible for a consumer to make a consumer data request directly to a data holder. This is because the ACCC has exempted data holders in the banking sector from complying with the direct to consumer data sharing obligation in Rule 3.4(3) and all related CDR Rules until 1 November 2021. For further information about these exemptions, see the 'Consumer data right exemptions register' on the ACCC's website.

[45] CDR Rule 1.13(3).

[46] CDR Rule 3.3(3).

Valid request

B.77 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.78 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.[47]

B.79 An 'eligible' consumer for the banking sector is discussed above at paragraphs B.59 to B.61.

B.80 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 the CDR data to provide those goods or services
- the accredited person has asked the consumer to give their consent for the person to collect and use the CDR data in order to provide those goods or services and
- the CDR consumer has given consent in response to the accredited person's request (and that consent has not been withdrawn).[48]

B.81 Refer to Chapter 3 (Privacy Safeguard 3) for further information regarding valid requests.

CDR Rules

B.82 The consumer data rules (CDR Rules) refer to the *Competition and Consumer (Consumer Data Right) Rules 2020*.

B.83 The ACCC has the power to make rules,[49] with the consent of the Minister,[50] to determine how the CDR functions in each sector. CDR Rules may be made on all aspects of the CDR regime (as provided in Part IVD the Competition and Consumer Commission Act) including the privacy safeguards, accreditation of an entity, the Data Standards Body and the format of CDR data and the data standards.

Current

Current consent

B.84 Consent to collect and use particular CDR data is 'current' if it has not expired under CDR Rule 4.14.[51]

---

[47] CDR Rule 3.3(3). For the banking sector, it is not currently possible for a consumer to make a consumer data request directly to a data holder. This is because the ACCC has exempted data holders in the banking sector from complying with the direct to consumer data sharing obligation in Rule 3.4(3) and all related CDR Rules until 1 November 2021. For further information about these exemptions, see the 'Consumer data right exemptions register' on the ACCC's website.

[48] CDR Rule 4.3.

[49] Section 56BA(1) of the Competition and Consumer Act.

[50] Section 56BR of the Competition and Consumer Act.

[51] CDR Rule 1.7(1) (Definitions).

B.85 CDR Rule 4.14 provides that consent expires if:

- it is withdrawn
- the accredited person is notified by the data holder of the withdrawal of authorisation
- the period of consent has ended
- 12 months has passed after consent was given
- another CDR Rule provides that consent expires, or
- the accredited person's accreditation is revoked or surrendered.

Current authorisation

B.86 Authorisation to disclose particular CDR data to an accredited person is 'current' if it has not expired under CDR Rule 4.26.

B.87 CDR Rule 4.26 provides that authorisation expires if:

- it is withdrawn
- the consumer ceases to be eligible
- the data holder is notified by the accredited person of the withdrawal of consent to collect the CDR data
- the period of authorisation has ended
- authorisation was for a single occasion and the disclosure has occurred
- 12 months has passed after authorisation was given
- another CDR Rule provides that authorisation expires, or
- the accreditation of the accredited person to whom the data holder is authorised to disclose is revoked or surrendered.

Consumer Experience Guidelines

B.88 The Consumer Experience Guidelines set out guidelines for best practice design patterns to be used by entities seeking consent from consumers under the CDR regime.

B.89 The Consumer Experience Guidelines are made by the Data Standards Body and cover:

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

B.90 The Consumer Experience Guidelines contain supporting examples illustrating how a range of key CDR Rules can be implemented.

B.91 The Consumer Experience Guidelines are available on the Data Standards Body website, consumerdatastandards.gov.au.

Data holder

B.92 A person is a data holder of CDR data if the person holds the CDR data, is not a designated gateway for the data, began to hold the data after the earliest holding day, and any of the three cases below apply:[52]

- The person is specified or belongs to a class of persons specified in a designation instrument and neither the CDR data, nor any other CDR data from which the CDR data was directly or indirectly derived, was disclosed to the person under the CDR Rules.[53]
- 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.[54]
- 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.[55]

B.93 For further information on the privacy obligations for data holder, see the Guide to privacy for data holders.

Earliest holding day

B.94 A designation instrument must specify the 'earliest holding day' for a particular sector. This is the day on which data held by an entity may be CDR data.[56]

B.95 Under the designation instrument for the banking sector, the earliest holding day is 1 January 2017.[57]

Data minimisation principle

B.96 The data minimisation principle limits the scope and amount of CDR data an accredited person may collect and use.

B.97 An accredited person collects and uses CDR data in compliance with the data minimisation principle if:[58]

a. when making a consumer data request on behalf of a consumer, the person does not seek to collect:

---

[52] Section 56AJ(1) of the Competition and Consumer Act and CDR Rules 1.7(1) and 1.7(3).

[53] 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 4.8(2).

[54] 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 designation instrument 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.

[55] The conditions for the banking sector are contained in clause 7.2 of Schedule 3 to the CDR Rules.

[56] Section 56AJ(1)(b) of the Competition and Consumer Act.

[57] Section 5(3) of the designation instrument.

[58] CDR Rule 1.8.

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

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.

Data standards

B.98 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.99 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.[59]

B.100 The current data standards are available on CSIRO's Data61 Consumer Data Standards website, consumerdatastandards.gov.au and include the following:

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

Consumer Experience Standards

B.101 The 'Consumer Experience Standards' are data standards[60] 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.102 The Consumer Experience Standards are available on CSIRO's Data61 Consumer Data Standards website, consumerdatastandards.gov.au.

[59] Section 56FA(1) of the Competition and Consumer Act.

[60] Section 56FA(3) of the Competition and Consumer Act and CDR Rule 8.11.

Data Language Standards

B.103 The 'Data Language Standards' are data standards[61] regarding the types of CDR data and descriptions of those types to be used by CDR participants in making and responding to requests.

B.104 The Data Language Standards form part of the Consumer Experience Standards and are available on CSIRO's Data61 Consumer Data Standards website, consumerdatastandards.gov.au.

Designated gateway

B.105 A 'designated gateway' is a person is specified in a legislative instrument made under s 56AC(2) of the Competition and Consumer Act.[62]

B.106 There are currently no designated gateways in the CDR regime.

Designation instrument

B.107 A 'designation instrument' is a legislative instrument made by the Minister under section 56AC(2) of the Competition and Consumer Act.[63]

B.108 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.109 These guidelines use 'designation instrument' to refer to the designation instrument for the banking sector (the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019), dated 4 September 2019.

Disclosure

B.110 'Disclosure' is not defined in the Competition and Consumer Act or the Privacy Act.

B.111 Under the CDR regime 'disclose' takes its ordinary, broad meaning.

B.112 An entity discloses CDR data when it makes the data accessible or visible to others outside the entity.[64] 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.[65]

---

[61] Section 56FA(3) of the Competition and Consumer Act and CDR Rule 8.11.

[62] Section 56AL of the Competition and Consumer Act.

[63] Section 56AM(1) of the Competition and Consumer Act.

[64] Information will be 'disclosed' under the CDR regime regardless of whether an entity retains effective control over the data. This is different to the situation under the Privacy Act, where in some limited circumstances the provision of information from an entity to a contractor to provide services on behalf of the entity may be a use, rather than a disclosure. See paragraph B.144 in Chapter B: Key concepts of the APP Guidelines.

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

B.113 For example, an entity discloses CDR data when it transfers a copy of the data in machine-readable form to another entity.

B.114 '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.148–B.149 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.115 'Eligible' CDR consumers are discussed at paragraphs B.59–B.61.

Outsourced service provider

B.116 The CDR Rules provide that an 'outsourced service provider' is a person to whom an accredited person discloses CDR data under a 'CDR outsourcing arrangement'.[66]

B.117 Any provision of CDR data by an accredited data recipient to an outsourced service provider will be a disclosure.[67]

CDR outsourcing arrangement

B.118 A person discloses CDR data to another person under a 'CDR outsourcing arrangement' if it does so under a written contract between the discloser and the recipient under which the recipient: [68]

- will provide, to the discloser, goods or services using CDR data
- must take the steps in Schedule 2 to the CDR Rules to protect CDR data disclosed to it by the discloser, and any CDR data that it directly or indirectly derives from the CDR data, as if it were an accredited data recipient
- must not use or disclose any such CDR data other than in accordance with the contract

[66] CDR Rules 1.7(1) (Definitions) and 1.10.

[67] Whether an accredited data recipient retains effective control over the data does not affect whether data is 'disclosed'. This is different to the situation under the Privacy Act, where in some limited circumstances the provision of information from an entity to a contractor to provide services on behalf of the entity may be a use, rather than a disclosure. See paragraph B.144 in Chapter B: Key concepts of the APP Guidelines.

[68] CDR Rules 1.7(1) (Definitions) and 1.10.

- must not disclose such CDR data to another person otherwise than under a CDR outsourcing arrangement, and if it does so, it must ensure that the other person complies with the requirements of the CDR outsourcing arrangement, and
- must, if directed by the discloser:
  - delete (in accordance with the CDR data deletion process) or return to the discloser any CDR data disclosed to it by the discloser
  - provide to the discloser records of any deletion that are required to be made under the CDR data deletion process, and
  - direct any other person to which it has disclosed CDR data to take corresponding steps.

Purpose

B.119 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.[69]

B.120 The purpose of an act is the reason or object for which it is done.

B.121 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.[70] 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.122 'Reasonable' and 'reasonably' are used in the privacy safeguards and CDR Rules to qualify a test or obligation. An example is that a 'CDR consumer' is a person who is identifiable or 'reasonably' identifiable from certain CDR data or related information.[71]

B.123 '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.124 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.[72]

---

[69] Section 4F(1)(b) of the Competition and Consumer Act.

[70] Section 4F of the Competition and Consumer Act.

[71] Section 56AI(3)(c) of the Competition and Consumer Act.

[72] 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).

B.125 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',[73] and 'involves an evaluation of the known facts, circumstances and considerations which may bear rationally upon the issue in question'.[74] 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.126 The 'reasonable steps' test is an objective test and is to be applied in the same manner as 'reasonable' and 'reasonably'.

B.127 An entity must be able to justify that reasonable steps were taken.

Redundant data

B.128 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.[75]

Required consumer data

B.129 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.130 'Required consumer data' for the banking sector is defined in clause 3.2 of Schedule 3 to the CDR Rules.[76]

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

Australian law

B.131 'Australian law' has the meaning given to it in the Privacy Act. It means:

---

[73] *George v Rockett* (1990) 170 CLR 104, 112.

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

[75] Section 56EO(2) of the Competition and Consumer Act. Note that this section also applies to designated gateways, however there are currently no designated gateways in the CDR regime.

[76] 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.

- 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.[77]

Court/tribunal order

B.132 '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.[78]

B.133 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.134 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.135 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.136 The obligation will usually be indicated by words such as 'must' or 'shall' and may be accompanied by a sanction for non-compliance.

Authorised

B.137 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.138 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.139 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[79] 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.

---

[77] Section 6(1) of the Privacy Act.

[78] Section 6(1) of the Privacy Act.

[79] For example, s 316(1) of the *Crimes Act 1900* (NSW).

B.140 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.[80]

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

Required

B.141 A data holder is 'required' to disclose CDR data under the CDR Rules:

- in response to a valid consumer data request under CDR Rule 3.4(3), subject to CDR Rule 3.5
- 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 Rule 4.7, where the data holder has a current authorisation to disclose the data from the CDR consumer, and
- in response to a product data request under CDR Rule 2.3(1), subject to CDR Rule 2.5, where a data holder is required to disclose required product data under CDR Rule 2.4(3) (however the privacy safeguards do not apply to required product data).

B.142 An accredited data recipient is never 'required' to disclose CDR data under the CDR Rules.[81]

Authorised

B.143 A data holder may be 'authorised' to disclose CDR data to an accredited person by a CDR consumer.[82] Such an authorisation must be in accordance with Division 4.4 of the CDR Rules.

B.144 A data holder is also authorised to disclose voluntary product data in response to a product data request under CDR Rule 2.4(2), however the privacy safeguards do not apply to required product data.

B.145 An accredited data recipient is 'authorised' to disclose CDR data under the CDR Rules:

- to the CDR consumer under CDR Rule 7.5(1)(c)
- to an outsourced service provider under CDR Rule 7.5(1)(d), and
- to a third party if the CDR data is de-identified, under CDR Rule 7.5(1)(e).

[80] See *Coco v The Queen* (1994) 179 CLR 427.

[81] In their capacity as an accredited data recipient.

[82] CDR Rule 4.5.

Required product data

B.146 In the banking sector, 'required product data' means CDR data for which there are no CDR consumers, and which is:[83]

- 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.147 The privacy safeguards do not apply to required product data.[84]

Use

B.148 '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.110–B.114 above.

B.149 Generally, an entity 'uses' CDR data when it handles and manages that data within its effective control. Examples include the entity:

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

Voluntary consumer data

B.150 '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.151 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.[85]

---

[83] Clause 3.1(1) of Schedule 3 to the CDR Rules.

[84] Section 56EB(1) of the Competition and Consumer Act and s 6(1) of the Privacy Act.

[85] 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.

B.152 An example of voluntary consumer data is 'materially enhanced information', which is excluded from a specified class of information under section 10 of the designation instrument for the banking sector,[86] 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.153 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.[87]

B.154 The privacy safeguards do not apply to voluntary product data.[88]

[86] Section 10 of the designation instrument 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.

[87] Clause 3.1(2) of Schedule 3 to the CDR Rules.

[88] Section 56EB(1) of the Competition and Consumer Act.

Chapter C:

Consent —

The basis for collecting and using CDR data

Version 2.0, July 2020

OAIC

Contents

Key points

- An accredited person may only collect and use consumer data right (CDR) data with the consent of the consumer.
- An accredited person must ask for a consumer's consent in accordance with the consumer data rules (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 for consent must be compliant with the data standards and have regard to the Consumer Experience Guidelines.
- An accredited person must comply with the data minimisation principle when collecting or using CDR data.
- 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 and use of their CDR data.

C.2 Consumer consent for the collection and use of their data is the bedrock of the CDR regime. Consent enables consumers to be the decision makers in the CDR regime, ensuring that they can direct where their data goes in order to obtain the most value from it.

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

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

C.4 The CDR regime requires express consent from consumers for the collection and use of their CDR data by accredited persons. Consent must meet the requirements set out in the CDR Rules, and can only remain valid for a maximum period of 12 months. Without express consent, the accredited person is not able to collect or use CDR data.

C.5 However, under the Privacy Act, consent is not the primary basis upon which an entity may collect or use personal information.[1] In addition, where consent is involved, the consent can be either express or implied.[2]

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

[2] See section 6(1) of the Privacy Act and Chapter B: Key concepts of the APP Guidelines.

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 and use CDR data for which there are one or more consumers.[3]

C.9 Where an accredited person:

- offers a good or service through the CDR regime and
- needs to access a consumer's CDR data in order to provide such goods or services,

the accredited person must obtain the consumer's consent to the collection and use of their CDR data to provide the good or service.

C.10 An accredited person may only collect data in response to a 'valid request' from the consumer. The consumer's consent to the collection and use of their CDR data is a fundamental component of the 'valid request'.

C.11 Upon obtaining a 'valid request' from the consumer, the accredited person may seek to collect the consumer's CDR data from the relevant data holder/s of the CDR data. The accredited person collects this CDR data by making a 'consumer data request' to the relevant data holder/s.[4]

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

C.13 Consent also underpins how an accredited person may use CDR data under Privacy Safeguard 6. An accredited person may only use or disclose a consumer's CDR data in accordance with a current consent from the consumer.[5]

C.14 The flow chart at paragraph C.75 demonstrates how the role of 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.

---

[3] 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 CDR data. See Chapter 6 (Privacy Safeguard 6) for further information regarding use of CDR data.

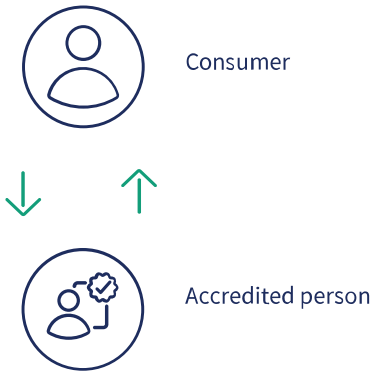
[4] For information regarding 'valid requests' and 'consumer data requests', see Chapter 3 (Privacy Safeguard 3). See also the flow chart underneath paragraph C.15 which demonstrates the points at which a valid request is given by the consumer and consumer data request is made on behalf of the consumer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

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

Consent and collection process for accredited persons

Obtaining consumer consent for the collection and use of CDR data

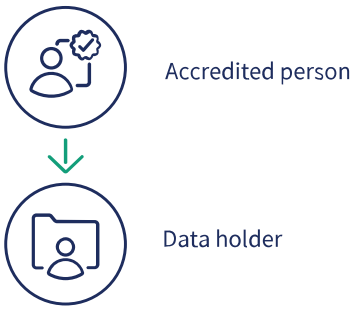
- Accredited person offers a good or service which requires CDR data
- Consumer wants to be provided the good or service
- Accredited person asks the consumer to consent to the collection and use of their CDR data for this purpose, for up to 12 months
- Consumer provides their express consent



The consumer has given the accredited person a valid request

Making a consumer data request on behalf of the consumer

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



Data holder sends the consumer's CDR data to the accredited person, after obtaining consumer authorisation to do so

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

Consents to collect and use CDR data

C.16 An accredited person must ask the consumer to give consent to collect and use CDR data in accordance with Division 4.3 of the CDR Rules.

C.17 The requirements in Division 4.3 are outlined below under 'Requirements for asking for consent', 'Restrictions on seeking consent' and 'How consents to collect and use CDR data must be managed'.

C.18 The CDR Rules state that the objective of Division 4.3 is to ensure that consent given by a consumer to collect and use CDR data is voluntary, express, informed, specific as to purpose, time limited and easily withdrawn.[6]

C.19 In obtaining a valid request from a consumer, an accredited person must comply with requirements[7] relating to:

- an accredited person's processes for asking for consent[8]
- information to be presented to the consumer when asking for consent[9]
- restrictions on seeking consent,[10] and
- providing information, including in relation to withdrawal[11] and expiry of consent.[12]

C.20 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.[13]

Requirements for asking for consent

General processes

C.21 An accredited person's processes for asking for consent must:

- accord with the data standards, and
- be as easy to understand as practicable, including by using concise language and, where appropriate, visual aids.[14]

[6] CDR Rule 4.9. The Explanatory Statement to the CDR Rules provides that the CDR Rules are intended to ensure that requests for consent to collect and use CDR data are transparent and that consumers understand the potential consequences of what they are consenting to.

[7] in Subdivision 4.3.2 of the CDR Rules.

[8] CDR Rule 4.10.

[9] CDR Rule 4.11.

[10] CDR Rule 4.12.

[11] CDR Rule 4.13.

[12] CDR Rule 4.14.

[13] 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.

[14] CDR Rule 4.10.

C.22 In ensuring processes are easy to understand, an accredited person must also have regard to the Consumer Experience Guidelines.[15]

C.23 An accredited person must not:

- include or refer to other documents so as to reduce comprehensibility in seeking consent. This makes the consent harder to understand, or
- bundle consents with other consents or permissions.[16] This practice has the potential to undermine the voluntary nature of the consent.

C.24 Each time an accredited person seeks a consumer's consent, they must allow the consumer to actively select or clearly indicate:[17]

- the particular types of CDR data to which they are consenting
- the specific uses of that CDR data, and
- whether the data will be:
  - collected on a single occasion and used over a specified period of time (not exceeding 12 months), or
  - collected on an ongoing basis and used over a specified period of time (not exceeding 12 months).

C.25 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.24 above
- ask for the consumer's express consent to any direct marketing they intend to undertake, and
- not pre-select these options.[18]

Where voluntary consumer data is involved

C.26 If a consumer's request covers voluntary consumer data,[19] the data holder may decide to charge the accredited person a fee. If the accredited person intends to pass on the fee to the consumer, the accredited person must make this clear to the consumer.

C.27 To do this, the accredited person must:

- clearly distinguish between the required consumer data and the voluntary consumer data they are seeking to collect
- inform the consumer of the amount of the fee, and the consequences if the consumer does not consent to the collection of the voluntary consumer data, and

[15] 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).

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

[17] CDR Rules 4.11(1)(b) and 4.12(1).

[18] CDR Rule 4.11.

[19] For information regarding 'required consumer data' and 'voluntary consumer data', see Chapter B (Key concepts).

- allow the consumer to actively select or otherwise clearly indicate whether they consent to the collection of that data.

Name and accreditation number

C.28 The accredited person must ensure that their name is clearly displayed in the consent request.

C.29 The accredited person's accreditation number must also be included in the consent request.[20] This number has been assigned to the accredited person by the Data Recipient Accreditor.

C.30 For more information on the Data Recipient Accreditor and the accreditation process and conditions, see the ACCC's Accreditation Guidelines.

Data minimisation principle

C.31 Collection of CDR data is limited by the data minimisation principle,[21] which provides that an accredited person:

- must not collect more data than is reasonably needed in order to provide the requested goods or services, including over a longer time period than is reasonably required, and
- may use the collected data only in accordance with the consent provided, and only as reasonably needed in order to provide the requested goods or services.[22]

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

C.32 The accredited person must explain how their collection and use is in line with the data minimisation principle.[23]

C.33 This explanation must include an outline of why the accredited person believes collecting the data is 'reasonably needed' to provide the relevant goods or services.[24]

- For example, the accredited person must explain how the data is necessary to deliver the service they are providing.[25]

[20] CDR Rule 4.11(3).

[21] CDR Rule 4.12(2).

[22] CDR Rule 1.8.

[23] CDR Rule 4.11(3)(c). For further information regarding the data minimisation principle, see Chapter B (Key concepts).

[24] CDR Rule 4.11(3)(c)(i).

[25] CDR Rule 4.11(3)(c).

C.34 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.[26]

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

Disclosure to outsourced service providers

C.36 Where the accredited person might disclose the consumer's CDR data to an outsourced service provider[28] (including one that is based overseas), the accredited person must:

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

Withdrawal of consent

C.37 The accredited person must explain to the consumer:

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

Treatment of redundant data

C.38 The accredited person must tell the consumer whether the accredited person has a general policy of:

- deleting redundant data
- de-identifying redundant data, or

[26] CDR Rule 4.11(3)(c)(i).

[27] CDR Rule 4.11(3)(c)(ii).

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

[29] 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. For further information, see Chapter 1 (Privacy Safeguard 1).

[30] CDR Rule 4.11(3)(g).

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

C.39 Where the accredited person will[32] or may[33] de-identify redundant data, the accredited person must also:

- allow the consumer to elect for their redundant data to be deleted, [34] including by outlining the consumer's right to elect for this to occur and providing instructions for how the consumer can make the election[35]
- 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[36]
- 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,[37] and
- if applicable, provide the consumer with examples of how the accredited person could use the redundant data once de-identified.[38]

C.40 See Chapter 12 (Privacy Safeguard 12) for further information on the treatment of redundant data (i.e. destruction or de-identification).

De-identification of CDR data

C.41 Where an accredited person asks for the consumer's consent to de-identify some or all of the CDR data for the purpose of disclosing (including by selling) the de-identified data, the accredited person must tell the consumer:[39]

- what the CDR de-identification process is[40]
- that the accredited person would disclose (for example, by sale) the de-identified data to one or more other persons
- the classes of persons to whom the accredited person would disclose the de-identified data (for example, to market research organisations or university research centres)
- the purpose/s for which the accredited person would disclose the de-identified data (for example, to sell the de-identified data or to provide to a university for research), and

[31] CDR Rule 4.11(3)(h).

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

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

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

[35] CDR Rule 4.11(3)(h).

[36] CDR Rule 4.17(2)(a), 4.17(2)(b).

[37] CDR Rule 4.17(2)(a).

[38] CDR Rule 4.17(2)(c).

[39] CDR Rule 4.15.

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

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

C.42 Where the accredited person is seeking consent to de-identify some or all of the consumer's CDR data for the purpose of disclosing (including by selling) the de-identified data, the accredited person must explain how the collection and use (i.e. de-identification) of the CDR data is in line with the data minimisation principle (see paragraphs C.31 – C.35).

C.43 This necessarily involves explaining how de-identification and disclosure of the consumer's CDR data is reasonably needed to provide the goods or services to the consumer.[41]

Restrictions on seeking consent

C.44 CDR Rule 4.12 provides that when seeking consent from a consumer, an accredited person must not ask for consent to:[42]

- collect and use CDR data for a period exceeding 12 months
- collect or use the data in a manner that is in breach of the data minimisation principle[43]
- sell the CDR data (unless the CDR data will be de-identified in accordance with the prescribed de-identification process, and the accredited person has complied with the requirements in paragraphs C.41–C.43 above), or
- 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.[44]

C.45 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:[45]

- 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.

[41] This is because an accredited person is required under CDR Rule 4.11(3)(c) to indicate how it would comply with the data minimisation principle in relation to CDR data it seeks consent to de-identify. See paragraphs C.31–C.35. See Chapter 12 (Privacy Safeguard 12) for information about de-identification.

[42] CDR Rule 4.12.

[43] The data minimisation principle is discussed in Chapter B (Key concepts), and at paragraph C.31.

[44] 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.

[45] CDR Rule 4.12(4).

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 to collect and use CDR data must be managed

Consumer dashboards

C.46 An accredited person must provide a consumer dashboard for each consumer who has provided consent to the collection and use of their CDR data.

C.47 An accredited person's consumer dashboard is an online service that can be used by each consumer to manage consumer data requests[46] and associated consents for the accredited person to collect and use CDR data.

C.48 The consumer dashboard should be provided to the consumer as soon as practicable after the accredited person receives the relevant consumer data request.[47]

C.49 The consumer dashboard must contain the following details of each consent to collect and use CDR data that has been given by the consumer:[48]

- the CDR data to which the consent relates
- the specific use or uses for which the consumer has given consent
- the date on which the consumer gave consent
- whether the consent was for the collection of CDR data on a single occasion or over a period of time
- if the consumer consented to collection of CDR data over a period of time – what that period is and how often data has been (and is expected to be) collected over that period
- if the consent is current – when it will expire
- if the consent is not current – when it expired, and

[46] See Chapter B (Key concepts).

[47] This is to assist the accredited person in complying with its obligation under Privacy Safeguard 5 and Rule 7.4 to update the consumer's dashboard 'as soon as practicable' after the collection of CDR data to notify the consumer of certain matters. See Chapter 5 (Privacy Safeguard 5) of the CDR Privacy Safeguard Guidelines for further information.

[48] CDR Rule 1.14(3).

- 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 data holder/s of the CDR data that was collected.[49]

C.50 The consumer dashboard must have a functionality that allows the consumer, at any time, to:[50]

- withdraw 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.51 These functionalities must be simple and straightforward to use, and prominently displayed.

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.52 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.[51] For further information, see Chapter B (Key concepts) and the Guide to privacy for data holders.

Consumers may withdraw consent

C.53 A consumer who has given consent for an accredited person to collect and use their CDR data may withdraw the consent at any time.

C.54 Where a consumer withdraws consent, the accredited person must notify the data holder of the withdrawal in accordance with the data standards.[52]

C.55 An accredited person must allow a consumer to withdraw consent by:

- using the accredited person's consumer dashboard, or
- using a simple alternative method of communication made available by the accredited person.[53]

[49] 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).

[50] CDR Rule 1.14(c).

[51] CDR Rule 1.15.

[52] CDR Rule 4.13(2).

[53] CDR Rule 4.13.

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.[54]

C.56 The functionality to withdraw consent on the consumer dashboard must be simple and straightforward to use, and prominently displayed.[55]

C.57 The alternative method of communicating the withdrawal of consent must be simple.[56] 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.58 An accredited person may wish to ensure their alternative method of communication is consistent with existing channels already made available to its customers,[57] for example through their telephone helpline.

Effect of withdrawing consent

C.59 The main consequence of the withdrawal of consent is that the consent expires,[58] and CDR data can no longer be collected. Information about when consent expires is contained in the following section.

C.60 In addition, once a consumer withdraws 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).[59]

C.61 If a consumer withdraws consent using the accredited person's consumer dashboard, the withdrawal is immediately effective.[60]

C.62 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.[61]

C.63 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,

---

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

[55] CDR Rule 1.14(c).

[56] CDR Rule 4.13(1).

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

[58] CDR Rule 4.26(1)(b).

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

[60] CDR Rule 4.14(1).

[61] CDR Rule 4.13(2).

the accredited person must be able to justify any delay in giving effect to the consumer's communication of withdrawal.

C.64 'Giving effect' to the withdrawal includes updating the consumer dashboard to reflect that the consent has expired,[62] as required by CDR Rule 4.19.[63]

C.65 Where a consumer has elected for their CDR data to be deleted upon becoming redundant data, their withdrawal of consent will not affect this election.[64]

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.66 Where a consent expires, the CDR data that the accredited person is required to delete or de-identify in accordance with Privacy Safeguard 12 is likely to become redundant data unless an exception applies.[65]

C.67 CDR Rule 4.14 provides that consent expires in the following circumstances:

- **If the consent is withdrawn**: if a withdrawal notice is given via the consumer dashboard, the consent expires immediately.[66] 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.[67]
- **When the accredited person is notified by the data holder of the withdrawal of authorisation:** upon notification from the data holder that the consumer has withdrawn authorisation, the consent expires immediately.[68]
- **At the end of the period of consent (no longer than 12 months after consent was given):** consent expires at the end of the specified period for which the consumer gave consent for the accredited person to collect and use the CDR data. This specified period cannot be longer than 12 months.[69]

[62] See CDR Rule 1.14(3)(g).

[63] 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.

[64] CDR Rule 4.13(3) provides that withdrawal of 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).

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

[66] CDR Rule 4.14(1).

[67] CDR Rule 4.14(1).

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

[69] 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.

- **If another CDR Rule provides that consent expires:** for example, a consent to collect CDR data expires once a person becomes a data holder rather than an accredited data recipient for the CDR data.[70]
- If the accredited person's accreditation is revoked or surrendered: consent expires when the revocation or surrender takes effect.[71]

Notification requirements

C.68 An accredited person must also comply with the following notification requirements under the CDR Rules:

- **CDR receipt:** There is a requirement to provide a notice in the form of a CDR receipt to the consumer after receiving a consumer consent or withdrawal of consent. A CDR receipt is a notice given by an accredited person to a consumer who has consented to the accredited person collecting and using their CDR data, or given to a consumer who has withdrawn such a consent.[72]
- **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.[73]
- **Update consumer's dashboard:** There is a general obligation to update the consumer's consumer dashboard as soon as practicable after the information required to be contained on the consumer dashboard changes.[74]
- **Ongoing notification:** There is an ongoing notification requirement regarding the currency of the consumer's consent.[75] CDR Rule 4.20 requires an accredited person to notify the consumer that their consent is still current where 90 days have elapsed since the latest of the following events:[76]
  - the consumer consenting to the collection and use of their CDR data
  - the consumer last using their consumer dashboard, or
  - the accredited person last sending the consumer a notification that their consent is still current.

C.69 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

[70] As a result of clause 7.2(3)(a) of Schedule 3 to the CDR Rules and section 56AJ(4) of the Competition and Consumer Act.

[71] For further information, see the ACCC's Accreditation Guidelines.

[72] 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.

[73] 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).

[74] CDR Rule 4.19.

[75] CDR Rule 4.20.

[76] CDR Rules 4.20(2) and (3) 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.

required for that dashboard.[77] 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.[78]

Authorisation

C.70 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.71 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 applicable data standards.

C.72 For the banking sector, for requests that relate to joint accounts, in some cases, the data holder might need to seek an authorisation from the other joint account holder.[79]

C.73 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.

C.74 The flow chart below demonstrates the role of authorisation in the key information flow between a consumer, accredited person and data holder.

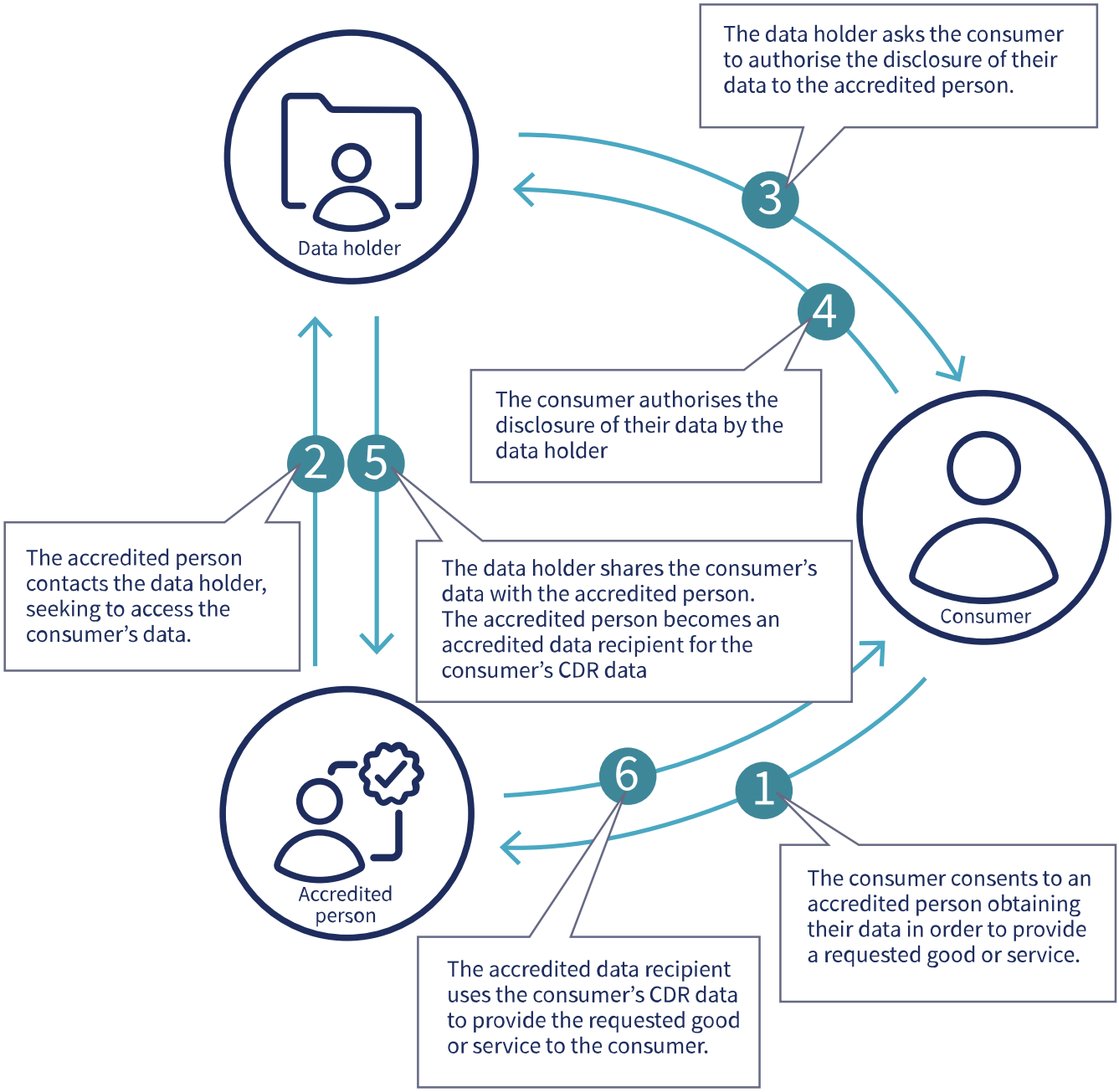
C.75 For further information on authorisation, see the Guide to privacy for data holders.

[77] CDR Rule 4.27.

[78] 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).

[79] See clause 4.5 of Schedule 3 to the CDR Rules.

Overview: key information flow in the CDR regime



Chapter 1:

Privacy Safeguard 1 —

Open and transparent management of CDR data

Version 2.0, July 2020

OAIC

Contents

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 data recipients, data holders and designated gateways) to handle CDR data in an open and transparent way.
- All CDR entities must take steps as are reasonable in the circumstances to implement practices, procedures and systems that will ensure they comply with the CDR regime, and are able to deal with related inquiries and complaints from consumers.
- All CDR entities must have a clearly expressed and up-to-date policy about how they manage CDR data. The policy must be provided free of charge and made available in accordance with the 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 data recipients.

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

How Privacy Safeguard 1 interacts with the Privacy Act and APP 1

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.[1]

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
Accredited person / accredited data recipient	**Privacy Safeguard 1 and APP 1** All accredited persons must comply with APP 1 in relation to the handling of personal information.[2] Entities should be aware that when an accredited person collects *any* CDR data, the person will also become an accredited data recipient and must then comply with: • Privacy Safeguard 1 in relation to the handling of CDR data, and • APP 1 in relation to the handling of personal information that is not CDR data. As APP 1 and Privacy Safeguard 1 both apply generally to an entity's handling of data, accredited data recipients must have systems, practices and procedures in place to ensure compliance with both the privacy safeguards and the APPs (including having both a CDR policy and privacy policy in place).[3] **Note**: While Privacy Safeguard 1 does not apply to accredited persons before they have collected any CDR data, the OAIC recommends that accredited persons consider their Privacy Safeguard 1 obligations early, so that they will meet their obligations under Privacy Safeguard 1 and CDR Rule 4.11(3) as soon as they start to seek to collect CDR data.

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

[2] All accredited persons are subject to the Privacy Act and the APPs in relation to information that is personal information but is not CDR data. Section 6E(1D) of the Privacy Act.

[3] CDR Rule 4.11(3) requires accredited persons to provide certain information from their CDR policy to the consumer when seeking consent to collect and use CDR data.

CDR entity	Privacy protections that apply in the CDR context
Designated gateway	**APP 1 and Privacy Safeguard 1** A designated gateway must comply with: • Privacy Safeguard 1 in relation to the handling of CDR data, and • APP 1 in relation to the handing of personal information (if they are an APP entity). 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).
Data holder	**APP 1 and Privacy Safeguard 1** A data holder must comply with: • Privacy Safeguard 1 in relation to the handling of CDR data, and • APP 1 in relation to the handing of personal information (if they are an APP entity). 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).[4]

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.[5] 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.

[4] See section 56AJ of the Competition and Consumer Act for the meaning of data holder.

[5] For example, accredited data recipients are required to establish a formal governance framework for managing information security risks under the Privacy Safeguard 12 CDR Rules.

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.[6]

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 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 data recipient), this will also affect what constitutes reasonable steps, and the entity will need to put in place mechanisms to ensure it complies with the CDR regime in all its different CDR entity capacities.

[6] Section 56ED(1) of the Competition and Consumer Act.

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 must comply with all 13 privacy safeguards, while a data holder needs to comply only with Privacy Safeguards 1, 10, 11 and 13. 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 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 data recipients have obligations to report regularly regarding their compliance with Privacy Safeguard 12,[7] and provide privacy and security training to staff.[8]
- Data holders have obligations relating to consumer data request services, and the authorisation and disclosure of CDR data.[9]
- Both accredited data recipients and data holders have obligations to provide consumers with access to copies of records upon request.[10]
- In the banking sector, both accredited data recipients 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.[11]

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 (such as cloud-based service providers for hosting services or data centres and backup providers), the reasonable

[7] 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.

[8] 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 Part 2 of Schedule 2 to the CDR Rules, in relation to Privacy Safeguard 12.

[9] 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.

[10] 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.

[11] See CDR Rule 5.12(1) (for accredited data recipients) and Part 6 of the CDR Rules (for data holders).

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.[12]

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 meet obligations under Privacy Safeguard 1 to ensure compliance with the particularities of the CDR regime.

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.

---

[12] 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.

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 data recipients should consider their obligations to implement strong minimum information security controls under Privacy Safeguard 12.[13]
- 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.[14]
- 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 data recipients already have obligations under Privacy Safeguard 12 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.[15]
- 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.[16] In relation to correction, CDR entities should consider their obligations under Privacy Safeguard 13 to respond to correction requests from consumers.[17]

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.

[13] See Schedule 2 to the CDR Rules, Chapter 12 (Privacy Safeguard 12) and the ACCC's Supplementary Accreditation Guidelines on Information Security available on the ACCC's Accreditation Guidelines page.

[14] 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 data recipients) and Part 6 of the CDR Rules (for data holders).

[15] See Part 2 of Schedule 2 to the CDR Rules.

[16] See CDR Rule 1.13. For further information regarding consumer data request services, see the Guide to privacy for data holders.

[17] 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 data recipients are required to provide regular assurance reports (an audit report) and attestation statements concerning compliance with certain information security requirements under Privacy Safeguard 12.[18]

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 data recipient in addition to being a data holder?[19]
- 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?[20]
- Online platforms — has the entity changed the online platforms used to communicate with CDR consumers, for example by creating a new mobile application?[21]

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).

[18] These obligations are contained in 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.

[19] Different CDR regime obligations apply depending on what capacity an entity is acting in. See paragraphs 1.16 to 1.18 for further information.

[20] An outsourced service provider is a person 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.

[21] 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.[22]
- 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.[23] The Information Commissioner may, but has not, approved a form for the CDR policy.[24]

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.[25]

1.46 There are different requirements depending on whether the CDR entity is an 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 data recipient), the entity can either have a single CDR policy that outlines how CDR data is handled in both capacities, or a separate CDR policy for each capacity.

---

[22] 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.

[23] CDR Rule 7.2(2).

[24] Section 56ED(3)(b) of the Competition and Consumer Act and CDR Rule 7.2(1).

[25] 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 data recipients

1.50 Privacy Safeguard 1 requires that accredited data recipients must include the following in their CDR policy:

- the classes[26] of CDR data held. The designation instrument sets out three classes of information for the banking sector: customer information,[27] product use information,[28] and information about a product[29]
- how the CDR data is held
- 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[30]
- events about which the entity will notify the consumers of such CDR data,[31] and
- when the entity must delete or de-identify CDR data in accordance with a request by a consumer.

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

---

[26] The classes of information are set out in the designation instrument for the relevant sector.

[27] Specified in section 6 of the designation instrument.

[28] Specified in section 7 of the designation instrument.

[29] Specified in section 8 of the designation instrument.

[30] An accredited data recipient is not authorised under the CDR Rules to disclose to any person except directly to the consumer or to an outsourced service provider.

[31] The events about which an accredited person will notify a consumer will include when a consumer gives consent to the person collecting and using their CDR data or withdraws such a consent, the collection of a consumer's CDR data, any ongoing notification requirements concerning a consumer's consent, any response to a consumer's correction request under Privacy Safeguard 13 and any eligible data breach affecting a consumer under the Notifiable Data Breach scheme.

- A statement indicating the consequences to the consumer if they withdraw a consent to collect or to use CDR data. This could include information about any early cancellation fees.
- A list of outsourced service providers, the nature of their services, the CDR data and classes of CDR data that may be disclosed.
- Where the entity is likely to disclose CDR data overseas to a service provider who is not accredited, a list of countries in which the overseas persons are likely to be based (if it is practicable to specify those countries in the policy).
- Where the entity proposes to store CDR data other than in Australia or an external territory, the countries in which the entity proposes to store CDR data.
- Where the entity seeks or intends that it will seek consent from consumers to de-identify their CDR data in accordance with CDR Rule 4.11(3)(e):
    - why the entity asks for consents to de-identify CDR data
    - how the entity de-identifies CDR data, including a description of techniques that it uses to de-identify CDR data, and
    - if the entity ordinarily discloses (by sale or otherwise) de-identified CDR data to one or more persons: the fact of this disclosure; the classes of persons such data is ordinarily disclosed to; and the purposes for which the accredited data recipient discloses de-identified CDR data.
- When and how the entity destroys 'redundant data', and how a consumer may ask for the entity to destroy their CDR data when it becomes redundant data.
- Where the entity has a general policy of de-identifying CDR data once it becomes redundant data:
    - if the entity uses the de-identified CDR data, examples of how the entity ordinarily uses de-identified CDR data
    - how the entity de-identifies CDR data, including a description of techniques that it uses to de-identify CDR data, and
    - if the entity ordinarily discloses (by sale or otherwise) de-identified CDR data to one or more persons: the fact of this disclosure, the classes of persons to whom such data is ordinarily disclosed, and the purposes for which the entity discloses de-identified CDR data.
- 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,[32] 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
  - 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.[33] 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.[34]

---

[32] 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.

[33] Section 56ED(7) of the Competition and Consumer Act.

[34] CDR Rule 7.2(8).

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 The CDR Rules provide that, if requested by consumer, the CDR entity must give the consumer a copy of the policy electronically or hard copy as requested by the consumer.

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,[35] 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.[36] As a consumer who is an individual may also access their data through APP 12 or seek correction of their data under APP 13 (where the data holder has not been authorised or required to disclose that data), the CDR policy must explain these alternative processes to those under the CDR regime.

[35] CDR Rule 7.2(2).

[36] Section 56ED(4)(a) of the Competition and Consumer Act.

Chapter 2:

Privacy Safeguard 2 —

Anonymity and pseudonymity

Version 1.0, February 2020

Contents

Key points

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

What does Privacy Safeguard 2 say?

2.1 Privacy Safeguard 2 provides that a consumer must have the option of not identifying themselves, or of using a pseudonym, when dealing with an accredited data recipient in relation to the CDR data.

2.2 'Anonymity' and 'pseudonymity' are different concepts. Privacy Safeguard 2 requires that both options be made available to consumers dealing with an accredited data recipient unless 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 does not need to allow anonymity or pseudonymity where:

- it is impracticable to deal with a consumer who has not identified themselves or has used a pseudonym in relation to the CDR data, or
- the accredited data recipient is required or authorised by or under a law, or a court/tribunal order, to deal with an identified consumer in relation to particular CDR data.

Who does Privacy Safeguard 2 apply to?

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

2.5 Data holders and designated gateways must ensure that they are adhering to their obligations under the *Privacy Act 1988* (the Privacy Act) and the Australian Privacy Principles (APPs), including APP 2 when dealing with individuals.

How Privacy Safeguard 2 interacts with the Privacy Act

2.6 It is important to understand how Privacy Safeguard 2 interacts with the Privacy Act and the APPs.[1]

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

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

CDR entity	Privacy protections that apply in the CDR context
Accredited person	**Australian Privacy Principle 2** APP 2 applies to an accredited person when dealing with an individual prior to the collection of the CDR data.[2] Privacy Safeguard 2 will apply from the point of collection of a consumer's CDR data.
Accredited data recipient	**Privacy Safeguard 2** Privacy Safeguard 2 applies instead of APP 2 to dealings with consumers upon the collection of each consumer's CDR data through the CDR regime. APP 2 will continue to apply to any dealings with an individual in relation to matters that do not relate to the CDR data.[3]
Designated gateway	**Australian Privacy Principle 2** Privacy Safeguard 2 does not apply to a designated gateway. However, a designated gateway may have obligations relating to Privacy Safeguard 2 where an accredited data recipient provides the option of anonymity or pseudonymity to a consumer through a designated gateway for the CDR data.
Data holder	**Australian Privacy Principle 2** Privacy Safeguard 2 does not apply to a data holder.

Note: *Examples of dealings with consumers are set out in paragraphs 2.15 and 2.16 below.*

Why anonymity and pseudonymity are important

2.8 Anonymity and pseudonymity are important privacy concepts. They enable consumers to choose the extent to which they are identifiable by the accredited data recipient.

2.9 There can be benefits to anonymity and pseudonymity, as consumers may be more likely to inquire about products and services under the CDR regime if they are able to do so without being identified. It can also reduce the risk of a data breach as less consumer data is collected.

[2] For consumers who are not individuals, APP 2 will not apply to dealings between an accredited person and the consumer. However, in order to be able to give the consumer the option of pseudonymity or of not identifying themselves (as required by Privacy Safeguard 2), an accredited person should ensure the same options given to individuals are provided to non-individuals in respect of dealings prior to the collection of the consumer's CDR data. This is because Privacy Safeguard 2 will apply to dealings between the consumer and the accredited person in relation to the consumer's data after it is collected (as the accredited person will be an accredited data recipient for the consumer's CDR data).

[3] Section 6E(1D) of the Privacy Act.

What is the difference between anonymity and pseudonymity?

2.10 Anonymity means that a consumer may deal with an accredited data recipient without providing any personal information or identifiers. The accredited data recipient should not be able to identify the consumer at the time of the dealing or subsequently. An example of an anonymous dealing is when a consumer has consented to the transfer of CDR data about their current service with no identifying information, to enquire generally about a service an accredited data recipient can provide, and after receiving the consumer's CDR data, the accredited data recipient continues to deal with the consumer without any identifying information.

2.11 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

2.12 An accredited data recipient must provide each consumer with the option of using a pseudonym, or not identifying themselves, when dealing with the accredited data recipient in relation to the CDR data.

2.13 The data standards allow for the consumer's identity to remain unknown to the accredited person throughout the consent and collection process under the CDR regime.

2.14 The data standards provide that:

- identifying information will not be conveyed to the accredited person unless the consumer agrees, and
- information provided by the consumer for the purposes of authentication with the data holder will not be seen by the accredited person.

2.15 Examples of 'dealings' between an accredited person and a consumer include:

- asking for the consumer's consent to collect and use their CDR data
- providing a consumer with a consumer dashboard, and
- communicating with the consumer (for example, when providing a CDR receipt to the consumer or ongoing notifications).[4]

2.16 Examples of 'dealings' between an accredited data recipient and a consumer include:

- communicating with the consumer regarding the collection of their CDR data (for example, providing a notice under Privacy Safeguard 5)[5]

[4] See Chapter C (Consent).

[5] See Chapter 5 (Privacy Safeguard 5).

- 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.[6]

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 2.17 to 2.24 following.

Exceptions

Requiring identification — required or authorised by law

2.17 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'.

2.18 The meaning of 'required or authorised by law or court/tribunal order' is discussed in Chapter B (Key concepts).

2.19 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.

2.20 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.[7]

2.21 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
- opening a bank account for a consumer, or providing other financial services where legislation requires the consumer to be identified, or
- supplying a pre-paid mobile phone to a consumer where legislation requires identification.

Requiring identification — impracticability

2.22 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.

2.23 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.

[6] See Chapter C (Consent).

[7] For further information, see Chapter B (Key concepts).

2.24 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.[8] 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.

[8] 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 1.0, February 2020

OAIC

Contents

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 that relates to 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:[1]

- 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.[2]

3.2 Under the CDR Rules:

- the valid request must meet specific requirements, including compliance with the CDR Rules regarding consent,[3] and
- accredited persons must have regard to the data minimisation principle,[4] 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.[5]

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

---

[1] Note: The privacy safeguards only apply to CDR data for which there are one or more CDR consumers (section 56EB(1) of the Competition and Consumer Act). This means that Privacy Safeguard 3 does not prevent an accredited person from seeking to collect CDR data for which there is no CDR consumer from a CDR participant.

CDR data will be CDR data for which there is no consumer in circumstances including where the person is not identifiable or 'reasonably identifiable' from the CDR data or other information held by the entity where the CDR data does not 'relate to' the person (see Chapter B (Key Concepts)).

[2] Section 56EF of the Competition and Consumer Act.

[3] CDR Rule 4.3.

[4] CDR Rule 4.12(2).

[5] Section 56EF(2) of the Competition and Consumer Act.

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 does Privacy Safeguard 3 interact with the Privacy Act?

3.8 It is important to understand how Privacy Safeguard 3 interacts with the Privacy Act and the APPs.[6]

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
Accredited person / accredited data recipient	**Privacy Safeguard 3 and APP 3** Privacy Safeguard 3 applies to accredited persons from the point when they seek to collect CDR data. APP 3 will continue to apply to personal information collected that is not CDR data.[7]
Designated gateway	**APP 3** Privacy Safeguard 3 does not apply to a designated gateway.
Data holder	**APP 3** Privacy Safeguard 3 does not apply to a data holder.

[6] 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.

[7] All accredited persons are subject to the Privacy Act and the APPs in relation to information that is personal information but is not CDR data. See s 6E(1D) of the Privacy Act.

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 means explicitly requesting another entity to provide CDR data, or taking active steps to collect CDR data.

3.12 The main way in which an accredited person will 'seek to collect' CDR data under the CDR Rules is by making a 'consumer data request' to a data holder 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 9 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'.[8] 'Record'[9] and 'generally available publication'[10] 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.

3.15 An accredited person is currently only authorised to seek to collect CDR data from a data holder.

What is a 'valid request?'

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

- the request is for the accredited person to provide goods or services
- the accredited person needs the consumer's CDR data[11] to provide the requested goods or services
- the accredited person asks for the consumer's consent to the collection of their CDR data, in accordance with Subdivision 4.3.2 of the CDR Rules (see paragraphs 3.18–3.21 for further information), and

[8] Section 4(1) of the Competition and Consumer Act.

[9] 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.

[10] 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.

[11] Note that the data may be required consumer data or voluntary consumer data for these purposes.

- the consumer expressly consents to this collection of their CDR data.

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 that the person is a consumer for CDR data, is making a valid request or has satisfied other criteria for the disclosure of CDR data.[12]

Process for asking for consent

3.18 Subdivision 4.3.2 of the CDR Rules outlines the requirements for consent for the purposes of making a valid request for collection 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 select or specify the types of data to which they provide consent and provide express consent for the accredited person to collect the selected data. Additional requirements apply where the accredited person is seeking consent to de-identify CDR data (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 by communicating it in writing to the accredited person or by using the consumer dashboard.
- 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[13] 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 3.16 above), and the consumer's consent for the accredited person to collect and use their CDR data is current,[14] the accredited person may request the relevant data holder to disclose some or all of the CDR data that:

[12] Sections 56BN and 56BO of the Competition and Consumer Act.

[13] CDR Rule 4.10(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).

[14] 'Current consent' is discussed in Chapter B (Key concepts).

- is the subject of the relevant consent to collect and use CDR data, and
- it is able to collect and use in compliance with the data minimisation principle.[15]

3.23 In doing so, the accredited person makes a 'consumer data request' to a data holder on behalf of the consumer.[16] The accredited person may make consumer data requests to more than one data holder where the relevant CDR data required to provide the requested goods or services is held by different data holders. The accredited person may also need to make repeated consumer data requests over a period of time in order to provide the requested goods or services.

3.24 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 that relates to a longer time period than reasonably needed, in order to provide the requested goods or services.[17]

3.25 The accredited person must make the consumer data request:

- using the data holder's accredited person request service, and
- in accordance with the data standards.[18]

3.26 An accredited person complies with Privacy Safeguard 3 after giving a data holder a consumer data request in the manner set out above.[19]

Data minimisation principle

3.27 Collection of CDR data is limited by the data minimisation principle,[20] which requires that an accredited person:

- must not collect more data than is reasonably needed in order to provide the requested goods or services, 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.

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 data holder a consumer data request.

3.29 The data minimisation principle is discussed further in Chapter B (Key concepts).

[15] CDR Rule 4.4(1).

[16] CDR Rule 4.4(2).

[17] CDR Rules 1.8(a) and 4.4(1)(d).

[18] CDR Rule 4.4(3).

[19] The effect of CDR Rule 4.4(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) is not a 'consumer data request'.

[20] CDR Rule 4.12(2).

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.

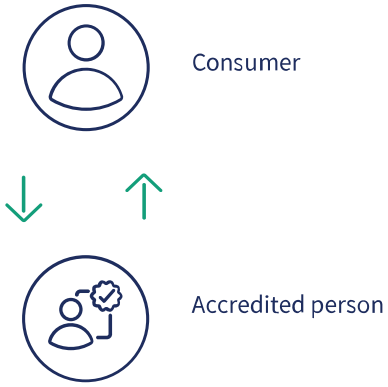
MiddleMan has asked Athena for her consent to collect information about her transaction history from the data holder (in addition to other data), when this information would not be required to determine her eligibility for the service.

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 sought to collect Athena's CDR data from a data holder otherwise than in accordance with the CDR Rules.

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



The consumer has given the accredited person a valid request

Making a consumer data request on behalf of the consumer

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

Data holder sends the consumer's CDR data to the accredited person, after obtaining consumer authorisation to do so

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

Interaction with other privacy safeguards

Privacy Safeguard 4

3.30 The privacy safeguards distinguish between an accredited person collecting solicited CDR data (Privacy Safeguard 3) and unsolicited CDR data (Privacy Safeguard 4).

3.31 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)).

3.32 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

3.33 Privacy Safeguard 5 requires an accredited person who has 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 1.0, February 2020

Contents

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 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.[1]

4.3 This obligation applies regardless of whether the accredited person collects the CDR data directly from a data holder or indirectly through a designated gateway.[2]

Why is it important?

4.4 The objective of Privacy Safeguard 4 is to ensure that CDR data collected by an accredited person is afforded appropriate privacy protection, 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.

[1] Section 56EG(1) of the Competition and Consumer Act. Note: The privacy safeguards only apply to CDR data for which there are one or more consumers (section 56EB(1) of the Competition and Consumer Act). This means that Privacy Safeguard 4 does not require an accredited person to destroy unsolicited CDR data for which there is no consumer (for instance, unrequested information about a product).

[2] Section 56EG(2) of the Competition and Consumer Act.

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

4.8 It is important to understand how Privacy Safeguard 4 interacts with the Privacy Act and APPs.[3]

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.[4]

CDR Entity	Privacy protections that apply in the CDR context
Accredited person / accredited data recipient	**Privacy Safeguard 4 and APP 4** Privacy Safeguard 4 applies to accredited persons from the point when they collect CDR data. APP 4 will continue to apply to personal information collected that is not CDR data.[5]
Designated gateway	**APP 4** Privacy Safeguard 4 does not apply to a designated gateway.
Data holder	**APP 4** Privacy Safeguard 4 does not apply to a data holder.

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
- 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).[6]

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

[4] See Chapter 3: APP 3 – Collection of solicited personal information of the APP Guidelines.

[5] All accredited persons are subject to the Privacy Act and the APPs in relation to information that is personal information but is not CDR data. See s 6E(1D) of the Privacy Act.

[6] 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.

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.[7]

Meaning of 'purportedly under the CDR Rules'

4.14 Privacy Safeguard 4 applies to CDR data collected 'purportedly under the CDR Rules'[8]

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.[9]

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 data holder.

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. *cont*

[7] Section 56EG(1)(a) of the Competition and Consumer Act.

[8] Section 56EG(1)(a)(i) of the Competition and Consumer Act.

[9] Section 56EG(1)(a)(ii) of the Competition and Consumer Act.

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 entity 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 entity can take technical and resource considerations into account. However, it is the responsibility of the entity to justify any delay in destroying unsolicited CDR data.

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

Not required to retain the data

4.24 The obligation to destroy unsolicited data does not apply to CDR data that an entity is required to retain by or under an Australian law or court/tribunal order.[10]

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 data holder unless in response to a valid request from a consumer, and in compliance with the CDR Rules (see Chapter 3 (Privacy Safeguard 3)).

[10] Section 56EG(1)(b) of the Competition and Consumer Act.

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).

Chapter 5:

Privacy Safeguard 5 —

Notifying of the collection of CDR data

Version 2.0, July 2020

OAIC

Contents

Key points

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

What does Privacy Safeguard 5 say?

5.1 If an accredited person collects CDR data under Privacy Safeguard 3, the accredited person must notify the consumer of the collection by taking the steps identified in the consumer data rules (CDR Rules).[1]

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 person 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.

5.4 For information about the concept of 'collects' refer to Chapter B (Key concepts).

Why is this important?

5.5 Notification of collection of CDR data is an integral element of the CDR regime as it provides confirmation to the consumer that their CDR data has been collected in accordance with their valid request.

5.6 This ensures consumers are informed when their CDR data is collected and builds trust between consumers and CDR participants.

Who does Privacy Safeguard 5 apply to?

5.7 Privacy Safeguard 5 applies to accredited persons. It does not apply to data holders or designated gateways.

5.8 Data holders and designated gateways must ensure that they are adhering to their obligations under the *Privacy Act 1988* (the Privacy Act) and the Australian Privacy Principles (APPs), including APP 3 and APP 5, when collecting personal information.

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.

[1] Section 56EH of the Competition and Consumer Act.

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

5.10 It is important to understand how Privacy Safeguard 5 interacts with the Privacy Act and the APPs.[2]

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
Accredited person / accredited data recipient	**Privacy Safeguard 5** Privacy Safeguard 5 applies instead of APP 5 to CDR data that has been collected by an accredited data recipient in accordance with Privacy Safeguard 3. APP 5 will continue to apply to: • personal information collected that is not CDR data, [3] and • CDR data that is not collected in accordance with Privacy Safeguard 3.[4]
Designated gateway	**APP 5** Privacy Safeguard 5 does not apply to a designated gateway.
Data holder	**APP 5** Privacy Safeguard 5 does not apply to a data holder.

How must notification be given?

5.13 An accredited person must provide the notification by updating the consumer dashboard for a consumer to include the matters discussed in paragraphs 5.23 to 5.36 as soon as practicable after CDR data relating to that consumer is collected.[5]

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 and use of their CDR data. Accredited persons are required by CDR Rule 1.14 to include within the consumer's

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

[3] All accredited persons are subject to the Privacy Act and the APPs in relation to information that is personal information but is not CDR data. See s 6E(1D) of the Privacy Act.

[4] With the exception of personal information that is also CDR data received by an accredited person who is a small business operator under the Privacy Act (see section 6E(1D) of the Privacy Act).

[5] CDR Rule 7.4.

dashboard certain details of each consent to collect and use CDR data that has been given by the consumer. [6]

5.15 Further guidance about the consumer dashboard is set out in Chapter B (Key concepts) and Chapter C (Consent).

Who must be notified?

5.16 The accredited person must notify the consumer who gave the consent to collect the CDR data.

5.17 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 person is required by CDR Rule 7.4 to update only the consumer dashboard of the requesting joint account holder.

When must notification be given?

5.18 An accredited person must notify the consumer as soon as practicable after the CDR data is collected.

5.19 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).

5.20 The test of practicability is an objective test. It is the responsibility of the accredited person to be able to justify any delay in notification.

5.21 In determining what is 'as soon as practicable', the accredited person may take the following factors into account:

- time and cost involved, when combined with other factors
- technical matters, and
- any individual needs of the consumer (for example, additional steps required to make the content accessible).

5.22 An accredited person 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 person.

Privacy tip: Accredited persons should ensure that they have systems and processes in place to allow for real-time and automated notification.

[6] This includes the CDR data to which the consent relates and when the consent will expire.

What matters must be included in the notification?

5.23 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 of the CDR data.[7]

5.24 Accredited persons 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.

5.25 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 person should ensure that the notification is as simple and easy to understand as possible. To do this, an accredited person 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 person could consider providing a condensed summary of key matters in the notification and linking to more comprehensive information or, where it may assist the consumer, a full log of access.

What CDR data was collected

5.26 The accredited person must notify the consumer of what CDR data was collected.

5.27 In doing so, the accredited person should ensure CDR data is described in a manner that allows the consumer to easily understand what CDR data was collected.

5.28 The accredited person must use the Data Language Standards when describing what CDR data was collected.[8] 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.

[7] CDR Rule 7.4.

[8] 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.

When the CDR data was collected

5.29 The accredited person must notify the consumer of when the CDR data was collected.

'One-off' collection[9]

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

Ongoing collection[10]

5.31 The accredited person 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 consent expires.

5.32 Where an accredited person is unsure of the end date they may put the date consent expires, but must update the end date as soon as practicable after it becomes known.[11]

5.33 The accredited person 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 [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 [data holder] up to three times per day').

The data holder of the CDR data

5.34 In its notification to the consumer, the accredited person must indicate from whom the CDR data was collected. There may be multiple data holders.

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.

Watson and Co updates Zoe's consumer dashboard on 1 July 2020 to include the following notification statement: *cont*

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

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

[11] 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.

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

5.35 In addition to the Privacy Safeguard 5 notification requirements in relation to collection, there are other notification requirements relating to consent that must be complied with:

- providing CDR receipts to the consumer (CDR Rule 4.18)
- general obligation to update the consumer dashboard (CDR Rule 4.19), and
- ongoing notification requirements for consumer consents (CDR Rule 4.20).

5.36 For further information regarding these notification requirements, see Chapter C (Consent).

How does Privacy Safeguard 5 interact with the other privacy safeguards?

5.37 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)).

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

Chapter 6:

Privacy Safeguard 6 —

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

Version 1.0, February 2020

OAIC

Contents

Key points

- Privacy Safeguard 6, together with consumer data rules (CDR Rules) 7.5 and 7.7, sets out the obligations and restrictions on accredited data recipients in the use and disclosure of Consumer Data Right (CDR) data.
- Generally, accredited data recipients and designated gateways can use or disclose CDR data only where required or authorised under the CDR Rules. The consumer must consent to these uses of their CDR data.
- CDR Rule 7.5(1) outlines the permitted uses or disclosures of CDR data.
- CDR Rule 7.5(2) prohibits certain uses or disclosures of CDR data.

What does Privacy Safeguard 6 say?

Accredited data recipients

6.1 An accredited data recipient must not use or disclose CDR data unless the:[1]

- 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 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.

[1] Note: The privacy safeguards apply only to CDR data for which there are one or more CDR consumers (s 56EB(1) of the Competition and Consumer Act). This means that Privacy Safeguard 6 does not prevent an accredited data recipient from using or disclosing CDR data for which there is no CDR consumer.

CDR data will be CDR data for which there is no consumer in circumstances including where the person is not identifiable or 'reasonably identifiable' from the CDR data or other information held by the entity, and where the CDR data does not 'relate to' the person (see Chapter B (Key Concepts)).

Who does Privacy Safeguard 6 apply to?

6.4 Privacy Safeguard 6 applies to accredited data recipients and designated gateways.

6.5 It does not apply to data holders. However, data holders should ensure that they adhere to their obligations under the *Privacy Act 1988* (the Privacy Act) and the Australian privacy Principles (APPs), including APP 6, when using or disclosing personal information.[2]

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

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

6.6 It is important to understand how Privacy Safeguard 6 interacts with the Privacy Act and the APPs.[3]

6.7 APP 6 relates to the use or disclosure of personal information. [4]

CDR entity	Privacy protections that apply in the CDR context
Accredited person / accredited data recipient	**Privacy Safeguard 6** Privacy Safeguard 6 applies instead of APP 6 to the use or disclosure of CDR data that has been disclosed to an accredited data recipient under the CDR Rules. APP 6 will continue to apply to the use or disclosure of personal information by an accredited person or accredited data recipient where the data is not CDR data.[5]
Designated gateway	**Privacy Safeguard 6** Privacy Safeguard 6 applies instead of APP 6 to the use and disclosure of CDR data.[6] APP 6 continues to apply to the use and disclosure of personal information that is not CDR data.
Data holder	**APP 6** Privacy Safeguard 6 does not apply to a data holder.

[2] 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.

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

[4] 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.

[5] All accredited persons are subject to the Privacy Act and the APPs in relation to information that is personal information but is not CDR data. See s 6E(1D) of the Privacy Act.

[6] Section 56EC(4)(d) of the Competition and Consumer Act.

Why is it important?

6.8 Consumer consent for uses of their CDR data, including subsequent disclosure, is at the heart of the CDR regime.

6.9 By adhering to Privacy Safeguard 6 an accredited data recipient or designated gateway will ensure consumers have control over what their CDR data is being used for and who it is 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.[7]

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.[8]

6.13 An accredited data recipient or designated gateway 'discloses' CDR data when it makes it accessible or visible to others outside the entity.[9] This focuses on the act done by the disclosing party, and not on the actions or knowledge of the recipient. There will be a disclosure in these circumstances even where the information is already known to the recipient. For further discussion of disclosure, see Chapter B (Key concepts).

6.14 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
- publishes the CDR data on the internet, whether intentionally or not
- accidentally provides CDR data to an unintended recipient

[7] The term 'use' is also not defined in the Privacy Act.

[8] The term 'disclose' is also not defined in the Privacy Act.

[9] Information will be 'disclosed' under the CDR regime regardless of whether an entity retains effective control over the data. This is different to the situation under the Privacy Act, where in some limited circumstances the provision of information from an entity to a contractor to provide services on behalf of the entity may be a use, rather than a disclosure. See paragraph B.144 in Chapter B: Key concepts of the APP Guidelines.

- 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.

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

6.15 This section outlines when an accredited data recipient may use or disclose CDR data.[10]

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

6.17 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.

Permitted uses or disclosures 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 in order 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
- ✓ Using or disclosing CDR data where required or authorised by law

Prohibited uses or disclosures of CDR data

- ✗ Selling CDR data, unless the data has been de-identified in accordance with the CDR Rules
- ✗ Using CDR data to identify, compile insights or build a profile about a person who isn't the consumer, unless this is required to provide the consumer with the requested goods or services and the consumer has consented

[10] 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 6.19 onwards.

Use or disclosure required or authorised under the CDR Rules

6.18 Privacy Safeguard 6 provides that an accredited data recipient of CDR data must not use or disclose CDR data unless the use or disclosure is required or authorised under the CDR Rules.[11]

6.19 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 consent from the consumer (other than a direct marketing consent)
- directly or indirectly deriving CDR data from the collected CDR data in accordance with the above use
- disclosing to the consumer any of their CDR data for the purpose of providing the existing goods or services[12]
- 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
- disclosing (by sale or otherwise) to any person, CDR data that has been de-identified in accordance with the CDR data de-identification process.

6.20 CDR Rule 7.5(2) prohibits the following uses or disclosures of CDR data:

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

6.21 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.[13]

6.22 The permitted uses and disclosures (in paragraph 6.20) are discussed further in this chapter.

---

[11] 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 Rule 7.7).

[12] 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.

[13] For further information regarding restrictions on seeking consent, see Chapter C (Consent).

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

6.23 An accredited data recipient is authorised to use CDR data in accordance with a current consent from the consumer to provide goods or services requested by the consumer.[14]

6.24 The relevant uses are those uses to which the consumer expressly consented when the consumer provided a valid request for the accredited person to collect their CDR data from a data holder. Valid requests are discussed further in Chapter 3 (Privacy Safeguard 3).

6.25 For information regarding how consents to collect and use CDR data must be managed, see Chapter C (Consent).

Example

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

SpendLess runs Oliver's transaction data through an algorithm to ascertain what other SpendLess products Oliver might be interested in.

When providing his valid request to SpendLess, 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 consent, and this use would therefore not be a permitted use under CDR Rule 7.5(1)(a).[15]

Using CDR data in compliance with the data minimisation principle

6.26 An accredited data recipient must comply with the data minimisation principle when using the CDR data to provide goods or services requested by the consumer.[16]

6.27 An accredited data recipient complies with the data minimisation principle if, when providing the requested goods or services, 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.[17]

6.28 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).

[14] CDR Rule 7.5(1)(a).

[15] 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).

[16] CDR Rule 7.5(1)(a).

[17] CDR Rule 1.8(b).

Risk point: An accredited person should pay careful attention to its processes and systems to ensure it complies with the data minimisation principle in all of its 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.

Deriving or indirectly deriving CDR data

6.29 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.[18]

6.30 This is a permitted disclosure under CDR Rule 7.5(1) and does not require the consent of the consumer.

6.31 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.[19]

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

Disclosing CDR data to the consumer

6.33 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.[20]

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

6.35 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

6.36 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

[18] CDR Rule 7.5(1)(b).

[19] CDR Rule 4.12(4).

[20] CDR Rule 7.5(1)(c).

- 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.[21]

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).

6.37 The consumer's CDR data includes data collected from the data holder in response to the consumer's request. The consumer's CDR data also includes data that has been directly and/or indirectly derived from their CDR data.

6.38 Disclosure of a consumer's CDR data by an accredited data recipient to an outsourced service provider for the purpose outlined in paragraph 6.35 is a permitted disclosure under CDR Rule 7.5(1) that does not require the consent of the consumer.[22]

6.39 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,[23] and
- include certain information about outsourced service providers in its CDR policy.[24]

6.40 An outsourced service provider is a person to whom an accredited data recipient discloses[25] CDR data under a CDR outsourcing arrangement.[26]

---

[21] CDR Rule 7.5(1)(d).

[22] However, the accredited data recipient must ensure it has complied with the requirements set out in paragraph 6.40.

[23] CDR Rule 4.11(3)(f). See Chapter 3 (Privacy Safeguard 3).

[24] CDR Rule 7.2(4). See Chapter 1 (Privacy Safeguard 1).

[25] Any provision of CDR data by an accredited data recipient to an outsourced service provider will be a disclosure. Whether an accredited data recipient retains effective control over the data does not affect whether data is 'disclosed'. This is different to the situation under the Privacy Act, where in some limited circumstances the provision of information from an entity to a contractor to provide services on behalf of the entity may be a use, rather than a disclosure. See paragraph B.144 in Chapter B: Key concepts of the APP Guidelines.

[26] CDR Rule 1.10. 'CDR outsourcing arrangement' is discussed in Chapter B (Key Concepts).

6.41 An accredited data recipient who discloses CDR data to a person under a CDR outsourcing arrangement must ensure that the person complies with its requirements under the arrangement.[27]

6.42 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.

6.43 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.

6.44 Where an accredited person has disclosed CDR data to a person under a CDR outsourcing arrangement, any use or disclosure of that data by the person (or their subcontractor) will be taken to have been by the accredited person. This occurs regardless of whether the use or disclosure is in accordance with the arrangement.[28]

6.45 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.[29] See Chapter 8 (Privacy Safeguard 8) for more information.

6.46 For further information, see Chapter B (Key Concepts), 'Outsourced service providers'.

Disclosing de-identified CDR data

6.47 An accredited data recipient is permitted to disclose to any person, by sale or otherwise, CDR data that has been de-identified in accordance with the CDR data de-identification process,[30] which is set out in CDR Rule 1.17.[31]

6.48 However, before de-identifying in accordance with 1.17, the accredited data recipient must have first:

- received consent from the consumer to de-identify some or all of the collected CDR data for the purpose of disclosing (including by selling) the de-identified data,[32] and
- provided the consumer with additional information relating to the de-identification of CDR data.[33]

[27] CDR Rule 1.16.

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

[29] 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.

[30] CDR Rule 7.5(1)(e).

[31] The CDR data de-identification process is set out in CDR Rule 1.17. If the CDR data cannot be de-identified to the 'required extent', the accredited data recipient must not disclose the CDR data to any person for this purpose, whether by sale or otherwise. For information regarding the CDR data de-identification process, see Chapter 12 (Privacy Safeguard 12). Chapter 12 (Privacy Safeguard 12) also provides guidance on the requirement for an accredited data recipient to destroy or de-identify redundant CDR data.

[32] CDR Rule 4.11(3)(e).

[33] CDR Rule 4.15.

6.49 An accredited data recipient must ensure it complies with the CDR data de-identification process when de-identifying CDR data.[34] De-identification is discussed further in Chapter 12 (Privacy Safeguard 12).

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

6.50 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.[35]

6.51 For the purposes of Privacy Safeguard 6, an Australian law does not include the APPs under the Privacy Act.[36]

6.52 'Australian law' and 'court/tribunal order' are discussed in Chapter B (Key concepts).

6.53 The accredited data recipient must keep a written note of any uses or disclosures made on this ground.

6.54 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

6.55 The restrictions on using or disclosing CDR data in Privacy Safeguard 6 are additional to Privacy Safeguard 7 (see Chapter 7 (Privacy Safeguard 7)) and Privacy Safeguard 8 (see Chapter 8 (Privacy Safeguard 8)).

6.56 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.

6.57 Privacy Safeguard 8 prohibits the accredited data recipient from disclosing CDR data to an overseas recipient unless an exception applies.

6.58 Privacy Safeguard 7 operates to the exclusion of Privacy Safeguard 6[37] (which means that direct marketing uses or disclosures cannot be authorised under Privacy Safeguard 6), while Privacy Safeguard 8 operates as a restriction in addition to Privacy Safeguard 6.[38]

---

[34] CDR Rule 1.17.

[35] Section 56EI(1)(c) of the Competition and Consumer Act.

[36] Sections 56EI(1) (Note 3) and 56EC(4)(a) of the Competition and Consumer Act.

[37] Section 56E(3) of the Competition and Consumer Act.

[38] See Note 2 of s 56EK 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 1.0, February 2020

OAIC

Contents

Key points

- Privacy Safeguard 7 prohibits accredited data recipients and designated gateways from using or disclosing 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 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.

What does Privacy Safeguard 7 say?

7.1 Privacy Safeguard 7 prohibits the use or disclosure of CDR data for direct marketing by accredited data recipients and designated gateways, unless the use or disclosure is required or authorised under the CDR Rules in accordance with the valid consent of the consumer.

7.2 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). These include uses or disclosures relating to:

- information about upgraded or alternative goods or services
- an offer to renew the existing goods or services being provided to the consumer, and
- information about the benefits of the existing goods or services.

Why is it important?

7.3 To provide a positive consumer experience and ensure consumer control over their data, consumers should not be subjected to unwanted direct marketing.

7.4 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?

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

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

How Privacy Safeguard 7 interacts with the Privacy Act

7.7 It is important to understand how Privacy Safeguard 7 interacts with the Privacy Act and the APPs.[1]

7.8 APP 7 sets out when an APP entity is prohibited from using or disclosing personal information for the purpose of direct marketing.

CDR entity	Privacy protections that apply in the CDR context
Accredited person / accredited data recipient	**Privacy Safeguard 7** Privacy Safeguard 7 applies instead of APP 7 to the use or disclosure of CDR data for direct marketing where the CDR data has been collected by an accredited data recipient under the CDR regime. APP 7 will continue to apply to direct marketing activities involving personal information by an accredited person or accredited data recipient where the data is not CDR data.[2]
Designated gateway	**Privacy Safeguard 7** Privacy Safeguard 7 applies instead of APP 7 in relation to the use and disclosure of CDR data for direct marketing. [3] APP 7 will continue to apply to direct marketing activities involving personal information that is not CDR data.
Data holder	**APP 7** Privacy Safeguard 7 does not apply to a data holder.

What is direct marketing?

7.9 '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.[4]

7.10 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.

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

[2] All accredited persons are subject to the Privacy Act and the APPs in relation to information that is personal information but is not CDR data. See s 6E(1D) of the Privacy Act.

[3] Section 56EC(4)(d) of the Competition and Consumer Act.

[4] For the purposes of APP 7, the phrase has been interpreted to take its ordinary meaning of marketing addressed directly to individuals (*Shahin Enterprises Pty Ltd v BP Australia Pty Ltd* [2019] SASC 12 [113] (Blue J)). It involves the use or disclosure of personal information to communicate directly with an individual to promote goods and services (Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 81).

7.11 An example of direct marketing by an entity includes sending an email to a consumer promoting financial products using the consumer's CDR data.[5]

7.12 '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).[6]

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).

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.[7]

[5] For information regarding 'valid requests', see Chapter 3 (Privacy Safeguard 3).

[6] Explanatory Statement to the CDR Rules.

[7] This would be 'direct marketing' even where the offers were about other products related to the requested product.

When is direct marketing allowed?

7.13 Generally, an entity is not permitted to engage in direct marketing under the CDR regime.

7.14 However, the CDR Rules permit an accredited data recipient 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'.[8]

7.15 The 'existing goods or services' refer to the goods or services requested by the consumer.[9]

7.16 A 'direct marketing consent' is a consent requested in accordance with CDR Rule 4.11(1)(c)(iii), which requires an accredited person to ask for the consumer's express consent to any direct marketing they intend to undertake when asking the consumer to consent to the collection and use of their CDR data.[10]

7.17 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 'existing goods or services'
  - an offer to renew existing goods or services when they expire, or
  - information about the benefits of existing goods or services
- 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
  - to the extent reasonably needed to do those things.

7.18 A direct marketing consent expires at the time that a consent to collect and use expires.

Information about upgraded or alternative goods or services

7.19 Sending the consumer information about upgraded[11] or alternative[12] goods or services is direct marketing.[13] 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 CDR Rule 4.11(1)(c)(iii).

---

[8] 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 7.12.

[9] CDR Rule 7.5(1)(a).

[10] CDR Rules 7.5(4) and 4.11(1)(c)(iii). For guidance regarding requirements for asking for consent, see Chapter C (Consent).

[11] 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.

[12] 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.

[13] CDR Rule 7.5(3)(a)(i).

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

7.20 Sending the consumer an offer to renew the existing goods or services is direct marketing.[14] 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)[15] from the consumer under CDR Rule 4.11(1)(c)(iii).

7.21 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 and use of their CDR data for the relevant good or service. This because an accredited person may collect CDR data only in response to a valid request from the consumer.[16]

Information about the benefits of existing goods or services

7.22 Sending the consumer information about the benefits of the existing goods or services being used by the consumer is direct marketing.[17] An accredited data recipient may only engage in

[14] CDR Rule 7.5(3)(a)(ii).

[15] The direct marketing consent will expire when the consumer's consent to collect and use particular CDR data expires, if the consumer does not withdraw it beforehand. Consent is discussed in Chapter C (Consent).

[16] The consumer's consent to the collection and use of their CDR data is a fundamental component of the 'valid request'. For information regarding valid requests and the requirements for seeking consent, see Chapter C (Consent).

[17] CDR Rule 7.5(3)(a)(iii).

this form of direct marketing if it has obtained a direct marketing consent (which is still current) [18] from the consumer under CDR Rule 4.11(1)(c)(iii).

Using the CDR data as reasonably needed

7.23 Using CDR data for the purpose of sending the information or renewal offer outlined above in paragraphs 7.19, 7.20 and 7.22,[19] including by analysing the data to decide what, if any, information will be sent, is direct marketing.

7.24 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.

7.25 The CDR data must only be used as reasonably needed for that purpose.

Privacy tip: As a matter of best practice, all direct marketing communications should easily allow the consumer to opt out of receiving direct marketing communications. For instance, an email communication should allow the consumer to click an embedded link through which they may notify the accredited data recipient of their intention to opt out.

Disclosure to an outsourced service provider

7.26 'Outsourced service provider' is discussed in Chapter B (Key concepts).

7.27 An accredited data recipient is permitted to disclose[20] CDR data to an outsourced service provider for the purpose of sending the information or renewal offer (outlined above in paragraphs 7.19, 7.20 and 7.22),[21] or to use the CDR data (as outlined above in paragraph 7.23).[22]

7.28 An accredited data recipient may only disclose CDR data to the extent reasonably needed for these purposes.[23]

7.29 Under this permitted disclosure, accredited persons may engage third parties (who fall within the meaning of 'outsourced service provider')[24] to undertake direct marketing activities on their behalf, where such activities are permitted under CDR Rule 7.5(3).

7.30 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:

---

[18] The direct marketing consent will expire when the consumer's consent to collect and use particular CDR data expires, if the consumer does not withdraw it beforehand. Consent is discussed in Chapter C (Consent).

[19] CDR Rule 7.5(3)(b).

[20] Any provision of CDR data by an accredited data recipient to an outsourced service provider will be a disclosure. Whether an accredited data recipient retains effective control over the data does not affect whether data is 'disclosed'. This is different to the situation under the Privacy Act, where in some limited circumstances the provision of information from an entity to a contractor to provide services on behalf of the entity may be a use, rather than a disclosure. See paragraph B.144 in Chapter B: Key concepts of the APP Guidelines.

[21] CDR Rule 7.5(3)(b).

[22] CDR Rule 7.5(3)(c)(i).

[23] CDR Rule 7.5(3)(c)(ii).

[24] See CDR Rule 1.10. 'Outsourced service provider' is discussed in Chapter B (Key concepts).

- 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.[25]

7.31 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 Safeguard8)).

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 persons 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.[26]

Interaction with other privacy safeguards

7.32 The prohibition against direct marketing in Privacy Safeguard 7 is complemented by Privacy Safeguard 6 (see Chapter 6 (Privacy Safeguard 6)) and Privacy Safeguard 8 (see Chapter 8 (Privacy Safeguard 8)).

7.33 Privacy Safeguard 6 prohibits an accredited data recipient from using or disclosing data unless required or authorised under the CDR Rules or another Australian law or court or tribunal order.

7.34 Privacy Safeguard 8 restricts disclosures of CDR data made to recipients located overseas.

Interaction with other legislation

7.35 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.

7.36 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,[27] 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.

7.37 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.

[25] CDR Rule 7.2(4). See Chapter 1 (Privacy Safeguard 1).

[26] This will assist the accredited person in directing an outsourced service provider under CDR Rule 1.10(2)(b)(iii).

[27] 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 2.0, July 2020

OAIC

Contents

Key points

- Privacy Safeguard 8 sets out the circumstances in which an accredited data recipient can disclose consumer data right (CDR) data to a recipient located overseas.
- Under Privacy Safeguard 8, an accredited data recipient must not disclose CDR 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, an accredited data recipient must not disclose CDR 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[1] 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.

[1] 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.[2]

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.

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

8.9 It is important to understand how Privacy Safeguard 8 interacts with the Privacy Act and the APPs.[3]

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
Accredited person / accredited data recipient	**Privacy Safeguard 8** Privacy Safeguard 8 applies instead of APP 8 to the overseas disclosure of CDR data where the CDR data has been collected by an accredited data recipient under the CDR regime. APP 8 will continue to apply to overseas disclosures of personal information by an accredited person or accredited data recipient where the data is not CDR data.[4]

[2] CDR Rules 1.10, 1.16, 7.5(1)(d) and 7.6. For more information on CDR outsourcing arrangement, please refer to Chapter B (Key concepts).

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

[4] All accredited persons are subject to the Privacy Act and the APPs in relation to information that is personal information but is not CDR data. See s 6E(1D) of the Privacy Act.

CDR entity	Privacy protections that apply in the CDR context
Designated gateway	**APP 8** Privacy Safeguard 8 does not apply to a designated gateway.
Data holder	**APP 8** 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. 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.[5]

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.

What is an overseas recipient?

8.15 Under Privacy Safeguard 8, an overseas recipient is a person,[6] 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.

When can CDR data be disclosed to an overseas recipient?

8.16 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 consumer data rules that relate to disclosure of CDR data (to the extent they are applicable to the relevant disclosure).[7]

---

[5] Any provision of CDR data to an outsourced service provider located overseas is a disclosure. This is different to the arrangements under the Privacy Act, where in limited circumstances providing personal information to an overseas contractor to perform services on behalf of an APP entity may be a use, rather than a disclosure of information. Whether an accredited data recipient retains effective control over the data does not affect whether data is 'disclosed'. See paragraph 8.14 in Chapter 8 of the APP Guidelines: APP 8 — Cross-border disclosure of personal information, for more information.

[6] Being a body corporate, body politic or individual.

[7] Privacy Safeguard 6 and the CDR Rules relating to permitted uses and disclosures (CDR Rules 7.5 and 7.6), Privacy Safeguard 7 and the CDR Rules relating to disclosure of CDR data for direct marketing (CDR Rules 7.8 and 7.5(3)), Privacy Safeguard 9 relating to disclosure of government related identifiers, and the CDR outsourcing arrangements (CDR Rules 7.5(1)(d) and 7.6).

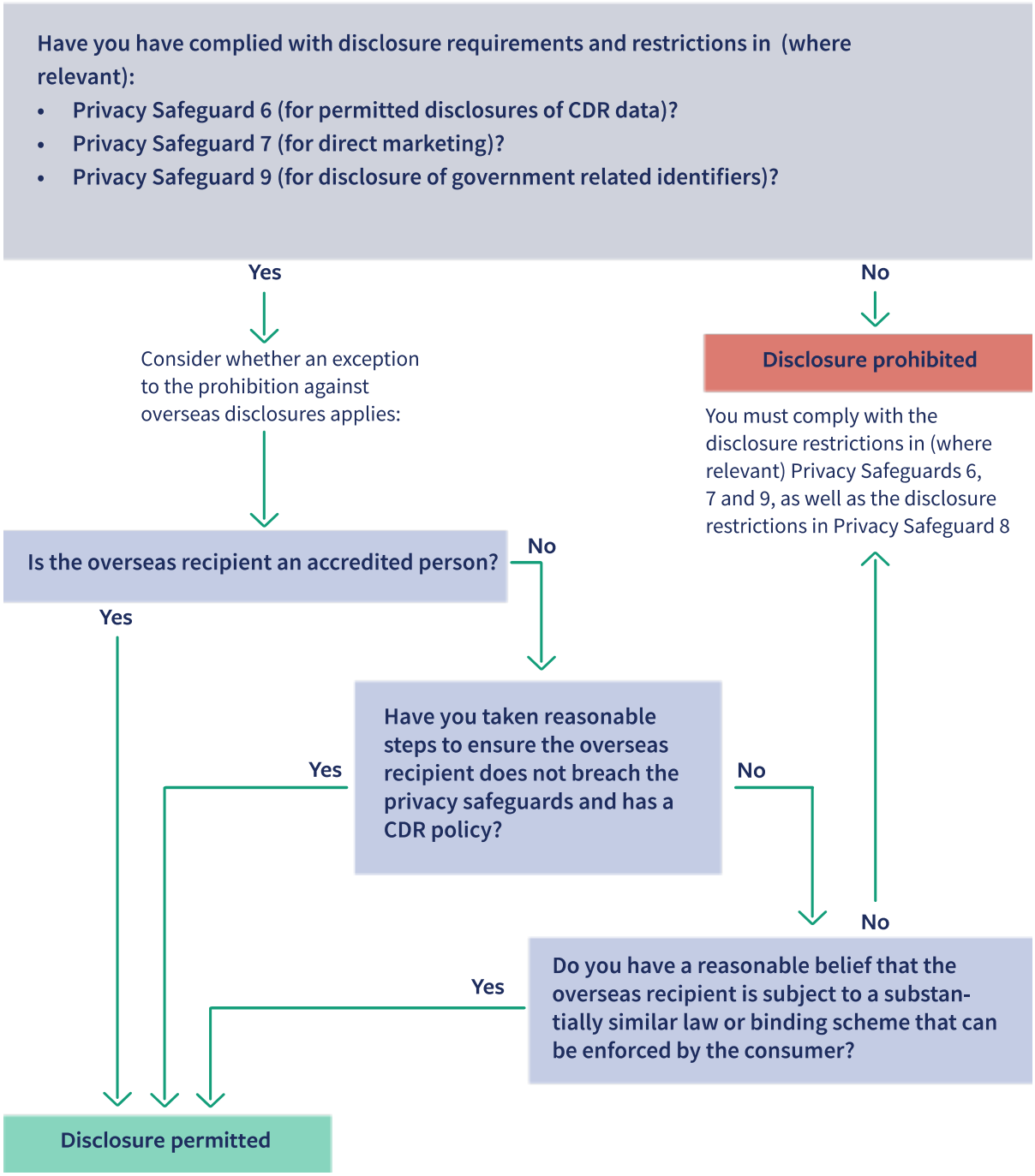
8.17 Privacy Safeguard 8 provides that an accredited data recipient must not disclose CDR data to a person located overseas unless one of the following four exceptions applies:

- 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[8] 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.

8.18 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 relevant exceptions under Privacy Safeguard 8.

[8] 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?



Exception 1 — Disclosing CDR data to an overseas recipient who is an accredited person

8.19 An accredited data recipient may disclose CDR data to an overseas recipient if the person is an accredited person.

8.20 The term 'accredited person' is discussed in Chapter B (Key concepts).

8.21 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.

8.22 The CDR Rules and the ACCC's Accreditation Guidelines provide more information about the requirements and process for accreditation.

8.23 Accreditation is considered sufficient protection to ensure compliance with the privacy safeguards.[9]

Exception 2 — Disclosing CDR data after taking 'reasonable steps' to ensure an overseas recipient does not breach the privacy safeguards

8.24 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.

8.25 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.

8.26 Examples for persons acting on behalf of the overseas recipient could include employees, directors, officers, or subcontractors.

What are 'reasonable steps'?

8.27 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.[10]

8.28 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

[9] Explanatory Memorandum, *Treasury Laws Amendment (Consumer Data Right) Bill 2019*, section 1.348.

[10] CDR Rules 1.10, 1.16 7.5(1)(d) and 7.6. For more information on CDR outsourcing arrangement, please refer to Chapter B (Key concepts).

- steps taken by the accredited data recipient to monitor compliance with the contract
- the accredited data recipient's relationship with the overseas recipient. More rigorous steps may be required when an entity discloses CDR data to an overseas recipient for the first time
- the nature of the overseas recipient, including the maturity of its processes and systems, and familiarity with CDR legislation (which may be derived from previous engagements with other CDR entities)
- the possible adverse consequences for a consumer if the CDR data is mishandled by the overseas recipient. More rigorous steps may be required as the risk of adversity increases
- the nature of the CDR data being disclosed. Where CDR data is sensitive in nature (and could, for example, cause financial or physical harm to a consumer if mishandled), it should be subject to more rigorous protections in the contractual arrangements
- existing technical and operational protections implemented by the overseas recipient to protect the CDR data (where these are not equivalent to the security requirements set out in Privacy Safeguard 12 and in Schedule 2 of the CDR Rules), and
- the practicability of taking protective steps, including time and cost involved. However, a CDR entity is not excused from ensuring that an overseas recipient is compliant with CDR legislation by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take particular steps will depend on whether the burden is excessive in all the circumstances.

Example

YC Pty Ltd is an accredited person that provides banking services and products to customers. YC Pty Ltd seeks to engage a contractor located overseas, Analysed Data Services, in order to offer certain data analytics services to its customers using their payments transactions data.

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

8.29 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'?

8.30 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.

8.31 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'?

8.32 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.

8.33 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'?

8.34 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.

8.35 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?

8.36 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.

8.37 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.

8.38 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?

8.39 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[11] and/or does not have a CDR policy.[12]

8.40 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.

[11] 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).

[12] Section 56EK(2) of the Competition and Consumer Act.

8.41 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.[13]

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 8.39 - 8.41.

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.

8.42 There are also other conditions in the CDR Rules that affect when an accredited data recipient is liable when making an overseas disclosure. Importantly, CDR Rule 7.6(2) provides that the accredited data recipient will be liable for the acts or omissions of an outsourced service provider (or its subcontractors).

How does Privacy Safeguard 8 interact with the other privacy safeguards?

Privacy Safeguard 6

8.43 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.

8.44 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

8.45 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

8.46 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).

[13] Please note the similar liability position under CDR Rule 7.6 relating to outsource service providers where the use or disclosure of CDR data by the outsource service provider (or by one of its subcontractors) is taken to be use or disclosure of the accredited data recipient whether or not in accordance with the CDR outsourcing arrangement between the parties.

Chapter 9:

Privacy Safeguard 9 —

Adoption or disclosure of government related identifiers by accredited data recipients

Version 1.0, February 2020

OAIC

Contents

Key points

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

What does Privacy Safeguard 9 say?

9.1 Privacy Safeguard 9 prohibits an accredited data recipient that has collected consumer data right (CDR) data which includes a government related identifier of a consumer for the 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 consumer data rules (CDR Rules), or
  - Australian Privacy Principle (APP) 9.3, which allows an entity to adopt, use or disclose a government related identifier of an individual as prescribed by regulations made under the Privacy Act.

9.2 Privacy Safeguard 9 only concerns government related identifiers of individuals.

9.3 In this Chapter, a government related identifier of a CDR consumer included with the CDR consumer's CDR data is referred to as a 'CDR consumer government related identifier'.

Why is it important?

9.4 The objective of Privacy Safeguard 9 is to restrict use of government related identifiers so that they do not become universal identifiers, which could jeopardise privacy by enabling CDR data from different sources to be matched and linked in ways that a consumer may not agree with or expect.

Who does Privacy Safeguard 9 apply to?

9.5 Privacy Safeguard 9 applies to accredited data recipients. It does not apply to data holders or designated gateways. 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.[1]

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
Accredited person / accredited data recipient	**Privacy Principle 9** Privacy Safeguard 9 applies instead of APP 9 to the handling of government related identifiers contained within CDR data collected by an accredited data recipient under the CDR regime.[2] APP 9 will continue to apply to the handling of government related identifiers collected by an accredited person or accredited data recipient within data that is not CDR data.[3]
Designated gateway	**APP 9** Privacy Safeguard 9 does not apply to a designated gateway.
Data holder	**APP 9** Privacy Safeguard 9 does not apply to a data holder.

Meaning of government related identifier

9.8 'Government related identifier' has the meaning given to it in the Privacy Act.[4]

9.9 Privacy Safeguard 9 only concerns government related identifiers of individuals.

9.10 This safeguard only applies to consumers who are individuals. 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). An identifier of an individual who is a sole trader or who runs a small business will be captured by Privacy Safeguard 9.

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

[2] Section 56EC(4)(d) of the Competition and Consumer Act.

[3] All accredited persons are subject to the Privacy Act and the APPs in relation to information that is personal information but is not CDR data. See s 6E(1D) of the Privacy Act.

[4] Sections 56EL(1)(b) and 56EL(2)(b) of the Competition and Consumer Act.

'Identifiers'

9.11 An 'identifier' of an individual is defined in subsection 6(1) of the Privacy Act as a number, letter or symbol, or a combination of any or all of those things, that is used to identify the individual or to verify the identity of the individual.

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

- an individual's name
- an individual's ABN, and
- anything else prescribed by the regulations made under the Privacy Act.[5] This provides flexibility to exclude any specified type of identifier from the definition, and therefore the operation of both Privacy Safeguard 9 and APP 9, as required.

'Government related identifier'

9.13 A 'government related identifier' of an individual is defined in subsection 6(1) of the Privacy Act as an identifier that has been assigned by:

- an agency[6]
- a State or Territory authority[7]
- an agent of an agency, or a State or Territory authority, acting in its capacity as agent, or
- a contracted service provider for a Commonwealth contract,[8] or a State contract,[9] acting in its capacity as contracted service provider for that contract.

9.14 The following are examples of government related identifiers:

- Medicare numbers
- Centrelink reference numbers[10]
- driver licence numbers issued by State and Territory authorities, and
- Australian passport numbers.

9.15 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.[11] These other laws

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

[6] 'Agency' is defined in s 6(1) of the Privacy Act.

[7] 'State or Territory authority" is defined in s 6C(3) of the Privacy Act.

[8] 'Commonwealth contract' is defined in s 6(1) of the Privacy Act to mean a contract, to which the Commonwealth or an agency is or was a party, under which services are to be, or were to be, provided to an agency.

[9] 'State contract' is defined in s 6(1) of the Privacy Act to mean a contract, to which a State or Territory or State or Territory authority is or was a party, under which services are to be, or were to be, provided to a State or Territory authority.

[10] 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.

[11] For more information about the legislative regimes, visit the OAIC's Tax File Numbers page and Healthcare Identifiers page https://www.oaic.gov.au.

apply in addition to Privacy Safeguard 9, i.e. a breach of the *Privacy (Tax File Number) Rule 2015* may be both an interference with the privacy of an individual under the Privacy Act and 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

9.16 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.[12] In addition, an accredited data recipient must not include the government related identifier when it discloses CDR data unless an exception applies.

'Adopt'

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

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

Example

Stephanie, an accountant and accredited person, receives a consumer's driver licence number when it is disclosed to Stephanie in response to a consumer data request. Stephanie then uses the identifier to refer to that consumer in her own identification system.

As Stephanie has adopted a CDR consumer government related identifier, she may be in breach of Privacy Safeguard 9.

'Use'

9.19 The term 'use' is discussed in Chapter B (Key concepts).

9.20 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

[12] 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.

- 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'

9.21 The term 'disclose' is discussed in Chapter B (Key concepts).

9.22 An accredited data recipient or designated gateway 'discloses' CDR data when it makes it accessible or visible to others outside the entity.[13]

Exceptions

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

9.23 An accredited data recipient may use a CDR consumer government related identifier, adopt it as its own identifier or include it when disclosing CDR data if this is required or authorised by or under an Australian law or a court/tribunal order.[14]

9.24 The meaning of 'required or authorised by or under an Australian law or a court/tribunal order' is discussed in Chapter B (Key concepts).

9.25 The Australian law or court/tribunal order should specify:

- a particular government related identifier
- the entities or classes of entities permitted to adopt, use or disclose it, and
- the particular circumstances in which they may adopt, use or disclose it.

Prescribed by regulations

9.26 An accredited data recipient may use a CDR consumer government related identifier, adopt it as its own identifier of the consumer, or include it when disclosing CDR data if:

- the identifier is prescribed by regulations
- the entity is an organisation, or belongs to a class of organisations, prescribed by regulations, and
- the adoption or use occurs in the circumstances prescribed by the regulations.[15]

9.27 Regulations may be made under the Privacy Act to prescribe these matters.[16]

---

[13] Information will be 'disclosed' under the CDR regime regardless of whether an entity retains effective control over the data. This is different to the situation under the Privacy Act, where in some limited circumstances the provision of information from an entity to a contractor to provide services on behalf of the entity may be a use, rather than a disclosure. See paragraph B.144 in Chapter B: Key concepts of the APP Guidelines.

[14] Section 56EL(1)(c) of the Competition and Consumer Act.

[15] Section 56EL(1)(d) of the Competition and Consumer Act and APP 9.3.

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

Interaction with other privacy safeguards

Privacy Safeguards 3 and 4

9.28 Privacy Safeguard 9 does not specifically address the collection of government related identifiers. However, if an accredited person collects a government related identifier that is considered to be CDR data, they must comply with other privacy safeguards, including Privacy Safeguard 3 and Privacy Safeguard 4. These privacy safeguards are discussed in Chapters 3 and 4 respectively.

Chapter 10:

Privacy Safeguard 10 —

Notifying of the disclosure of CDR data

Version 2.0, July 2020

OAIC

Contents

Key points

- Where a data holder discloses consumer data right (CDR) data to an accredited person, the data holder 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.[1]

10.2 Where an accredited data recipient discloses CDR data, they must notify the consumer by taking the steps identified in the CDR Rules.[2]

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, a data holder 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.

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. It does not apply to designated gateways.

10.8 Although Privacy Safeguard 10 applies to accredited data recipients, there are currently no CDR Rules requiring accredited data recipients to notify consumers about the disclosure of CDR data.

[1] 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).

[2] Section 56EM(2) of the Competition and Consumer Act.

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

Who must be notified?

10.10 The data holder must notify each of the consumers for the CDR data that has been disclosed.[3]

10.11 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.[4] In this case, the data holder must notify both the requesting and non-requesting joint account holders. However, a data holder will not be required to notify the non-requesting joint account holder/s where the data holder considers this necessary to prevent physical or financial harm or abuse.[5]

10.12 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.

How must notification be given?

10.13 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)[6] to include the matters discussed in paragraphs 10.21 to 10.31 as soon as practicable after CDR data relating to that consumer is disclosed.[7]

10.14 The 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)[8] where a consumer data request has been made on their behalf by an accredited person. Data holders are required by CDR Rule 1.15 to include within the consumer's dashboard certain details of each authorisation to disclose CDR data that has been given by the consumer. [9]

10.15 Further guidance about the consumer dashboard is set out in Chapter B (Key concepts) and the Guide to privacy for data holders.

---

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

[4] For details regarding the inclusion of CDR data that relates to a joint account under the CDR regime, see the phasing summary table to the CDR Rules.

[5] CDR Rule 7.9 and clause 4.6 of Schedule 3 to the CDR Rules.

[6] Where the CDR data disclosed relates to a joint account and the data holder has provided an equivalent consumer dashboard (see clause 4.4 of Schedule 3 to the CDR Rules), the data holder must also notify the non-requesting joint account holder by updating their consumer dashboard to include those same matters as soon as practicable after the CDR data is disclosed.

[7] CDR Rule 7.9.

[8] See clause 4.4 of Schedule 3 to the CDR Rules.

[9] This includes the CDR data to which the authorisation relates and when the authorisation will expire.

When must notification be given?

10.16 A data holder must notify the consumer/s as soon as practicable after the CDR data is disclosed.[10]

10.17 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).

10.18 The test of practicability is an objective test. It is the responsibility of the data holder to be able to justify any delay in notification.

10.19 In determining what is 'as soon as practicable', the data holder 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).

10.20 A data holder is 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?

10.21 The minimum matters that must be included 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 data recipient of the CDR data.[11]

10.22 Data holders 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.

10.23 Guidance on each of the minimum matters follows.

[10] CDR Rule 7.9.

[11] CDR Rule 7.9.

Risk point: Consumers may not read or understand a notification if it is complex.

Privacy tip: A data holder should ensure that the notification is as simple and easy to understand as possible. To do this, a data holder 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, the data holder 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

10.24 The data holder must notify the consumer of what CDR data was disclosed.

10.25 In doing so, the data holder should ensure the CDR data is described in a manner that allows the consumer to easily understand what CDR data was disclosed.

10.26 The data holder must use the Data Language Standards when describing what CDR data was disclosed. [12] This will aid consumer comprehension by ensuring consistency between how CDR data was described in the authorisation-seeking process and how CDR data is described in the consumer dashboard.

When the CDR data was disclosed

10.27 The data holder must notify the consumer when the CDR data was disclosed.

'One-off' disclosure:[13]

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

Ongoing disclosure:[14]

10.29 The data holder 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 data holder will make its final disclosure. This end date might not necessarily be the same as the date authorisation expires.

[12] 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 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.

[13] 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.

[14] This is where the accredited person made a consumer data request on behalf of the consumer for collection of CDR data over a specified period of time.

10.30 Where a data holder is unsure of the end date they may put the date authorisation expires, but must update the end date as soon as practicable after it becomes known.[15]

The accredited data recipient of the CDR data

10.31 In its notification to the consumer, the data holder must indicate to whom the CDR data was disclosed.

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 could notify Zoe of the disclosure of her CDR data in accordance with CDR Rule 7.9.

Other notification requirements under the CDR Rules

10.32 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.[16]

Disclosure to a designated gateway

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

[15] CDR Rule 4.27 requires a data holder to update the consumer dashboard as soon as practicable after the information required to be contained on the dashboard changes.

[16] CDR Rule 4.27.

10.33 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.[17]

10.34 There are currently no CDR Rules made for this circumstance.

Interaction with other Privacy Safeguards

10.35 CDR participants must comply with Privacy Safeguard 1 by taking reasonable steps to implement practices, procedures and systems that will ensure they comply with the CDR regime, including Privacy Safeguard 10. See Chapter 1 (Privacy Safeguard 1).

10.36 Privacy Safeguard 11 mandates the steps by which a data holder must advise a consumer where the data holder has disclosed CDR data that was incorrect. See Chapter 11 (Privacy Safeguard 11).

[17] CDR Rules may be made in relation to the notification requirements for that disclosure.

Chapter 11:

Privacy Safeguard 11 —

Quality of CDR data

Version 2.0, July 2020

OAIC

Contents

Key points

- Privacy Safeguard 11, together with consumer data rule (CDR Rule) 7.10, sets out obligations for data holders and accredited data recipients 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 who are disclosing CDR data when authorised or required 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.

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 a data holder who has disclosed CDR data that was incorrect at the time of disclosure to an accredited person to provide the consumer with a written notice that identifies the accredited person and the CDR data that was incorrect, states the date of the disclosure, and states that the data holder must disclose the corrected data to that accredited person if the consumer requests them to do so.

Why is it important?

11.4 The objective of Privacy Safeguard 11 is to ensure consumers have trust in and control over the quality of their CDR data disclosed as part of the CDR regime.

11.5 Privacy Safeguard 11 does this by ensuring entities are disclosing CDR data that is accurate, up to date and complete, and by giving consumers control over their data by allowing them to require entities to correct any inaccuracies in their data after it is shared.

11.6 This allows consumers to enjoy the benefits of the CDR regime, such as receiving competitive offers from other service providers, as the data made available to sector participants can be relied on.

Who does Privacy Safeguard 11 apply to?

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

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

How does Privacy Safeguard 11 interact with the Privacy Act?

11.8 It is important to understand how Privacy Safeguard 11 interacts with the *Privacy Act 1988* (the Privacy Act) and Australian Privacy Principles (APPs).[1]

11.9 APP 10 requires APP entities to take reasonable steps to ensure the quality of personal information in certain circumstances.

11.10 APP 10 requires an APP entity to take reasonable steps to ensure the quality of personal information at the time of the *collection* and *use* as well as the disclosure of the information.

11.11 Although Privacy Safeguard 11 applies only in relation to the *disclosure* of CDR data, good practices and procedures to ensure the quality of personal information collected, used and disclosed under APP 10 will also help to ensure the quality of CDR data that is disclosed under the CDR regime.

11.12 Data holders should also be aware that APP 13 (correction of personal information) obligations under the Privacy Act continue to apply in certain circumstances.[2] That is, where a consumer has not requested the data holder to correct the CDR data under Privacy Safeguard 13, the data holder must continue to comply with APP 13 and take steps that are reasonable to correct CDR data that is also personal information, where it is out of date, inaccurate, incomplete, irrelevant or misleading for the purpose for which it is held.[3] Taking reasonable steps under APP 13, independently of any request, can help to enhance the quality of information and support compliance with Privacy Safeguard 11.

CDR entity	Privacy protections that apply in the CDR context
Accredited person / accredited data recipient	**Privacy Safeguard 11** Privacy Safeguard 11 applies instead of APP 10 to CDR data that has been collected by an accredited person under the CDR regime. APP 10 will continue to apply to any personal information collected by an accredited person or accredited data recipient that is not CDR data. [4]

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

[2] See Chapter 13 (Correction of CDR data) for information on when APP 13 applies instead of Privacy Safeguard 13.

[3] See Chapter 13 (Correction of personal information) of the OAIC's APP Guidelines for further information.

[4] All accredited persons are subject to the Privacy Act and the APPs in relation to information that is personal information but is not CDR data. See s 6E(1D) of the Privacy Act.

CDR entity	Privacy protections that apply in the CDR context
Data holder	**Privacy Safeguard 11** Privacy Safeguard 11 applies instead of APP 10 to disclosures of CDR data that are required or authorised under the CDR Rules. APP 10 continues to apply to: • personal information collected that is not CDR data, and • disclosures of CDR data that is personal information, where the data holder is not required or authorised to disclose the data under the CDR rules (for example, disclosures to a third-party service provider).
Designated gateway	**APP 10** Privacy Safeguard 11 does not apply to a designated gateway.

What are the quality considerations?

11.13 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).

11.14 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.

11.15 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

Bright Bank is a data holder and is regularly authorised and/or required to disclose consumers' CDR data under the CDR Rules.

Bright Bank receives a consumer data request regarding a customer's account balance and details, including the balance, interest rates, fees and discounts.

Bright Bank holds this data for the purposes of providing a bank account service to the customer.

When Bright Bank is required or authorised to disclose a consumer's CDR data under the CDR Rules, 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.

11.16 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.[5]

11.17 The following analysis of each term draws on the ordinary meaning of the terms and the APP Guidelines.[6] As the analysis indicates, there is overlap in the meaning of the terms.

Accurate

11.18 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.

11.19 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.[7] 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.

11.20 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

11.21 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.[8]

11.22 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.

---

[5] 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)).

[6] See Chapter 10: APP 10 — Quality of personal information of the APP Guidelines.

[7] Data derived from CDR data continues to be 'CDR data': see s 56AI of the Competition and Consumer Act.

[8] Such an assessment will likely be 'materially enhanced information' under section 10 of the designation instrument and therefore not 'required consumer data' under the CDR Rules.

11.23 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

11.24 CDR data is incomplete if it presents a partial or misleading picture of a matter of relevance, rather than a true or full picture.

11.25 An example is data from which it can be inferred that a consumer owes a debt, which in fact has been repaid. The CDR data will be incomplete under Privacy Safeguard 11 if the data is held, for instance, for the purpose of determining the borrowing capacity of the consumer. Where the CDR data is held for a different purpose for which the debt is irrelevant, the fact that the debt has been repaid may not of itself render the CDR data incomplete. If, however, the accredited person has requested a consumer's CDR data for a specific period, and in that period the consumer owed a debt which is recorded in the CDR data, and that debt was repaid in a later period, the CDR data will still be 'complete' in respect of that specific period.

Taking reasonable steps to ensure the quality of CDR data

When must an entity take reasonable steps?

11.26 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.
- **for accredited data recipients:** at the time the entity discloses CDR data when required or authorised under the CDR Rules.

11.27 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.

11.28 Entities should also be aware that Privacy Safeguard 11 only requires an accredited data recipient to take reasonable steps when disclosing CDR data under the 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).

11.29 The obligation to take reasonable steps to ensure the quality of CDR data applies to accredited data recipients when disclosing CDR data:

- to the consumer under CDR Rules 7.5(1)(c) or 7.5(3), and
- to an outsourced service provider under CDR Rule 7.5(1)(d).

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.

What constitutes 'reasonable steps'?

11.30 The requirement to ensure the quality of CDR data is qualified by a 'reasonable steps' test.

11.31 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.
- **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.

11.32 In some circumstances, it will be reasonable for an accredited data recipient to take no steps to ensure the quality of CDR data. For example, where an accredited data recipient collects CDR data from a data holder known to be reliable, it may be reasonable to take no steps to ensure the quality of that data. It is the responsibility of the entity to be able to justify that this is reasonable.

Examples of reasonable steps

11.33 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.[9]
- 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'.[10]

Advising a consumer when disclosed CDR data is incorrect

11.34 CDR Rule 7.10 sets out the notice requirements with which a data holder must comply after disclosing incorrect CDR data to an accredited person. These notice requirements are summarised in paragraphs 11.36 to 11.47 below.

11.35 CDR Rule 7.10 does not apply to accredited data recipients. There is no CDR Rule in relation to accredited data recipients advising consumers that disclosed CDR data was incorrect.[11]

Data holders

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

11.36 A data holder must advise a consumer that some or all of the CDR data was incorrect if the entity:[12]

[9] 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.

[10] See s 56AI of the Competition and Consumer Act.

[11] An accredited data recipient is currently only authorised under the CDR Rules to disclose CDR data to the consumer or an outsourced service provider (CDR Rule 7.5(1)). A consumer may make a correction request to an accredited data recipient under Privacy Safeguard 13.

For guidance regarding the situation where an accredited data recipient realises CDR data disclosed was incorrect, see paragraph 11.51.

For further information regarding disclosure, see Chapter 6 (Privacy Safeguard 6). For further information regarding correction, see Chapter 13 (Privacy Safeguard 13).

[12] Section 56EN(3) of the Competition and Consumer Act.

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

11.37 A data holder may become aware of inaccuracies in a range of ways – for example, as a result of a periodic audit, or pursuant to a correction request made under Privacy Safeguard 13 (Correction of CDR data).

11.38 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 a data holder provide to the consumer when incorrect CDR data has been disclosed?

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

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

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

How must a notice be provided?

11.41 CDR Rule 7.10 requires a data holder to notify the consumer by electronic means after disclosing incorrect data.

11.42 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.

11.43 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 data holders give notification to the consumer?

11.44 Data holders must provide notices to the consumer as soon as practicable, but no more than five business days after the data holder becomes aware that some or all of the disclosed data was incorrect.

11.45 The test of practicability is an objective test. The data holder should be able to justify that it is not practicable to give notification promptly after becoming aware of the disclosure of incorrect CDR data.[13]

[13] 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.

11.46 In adopting a timetable that is 'practicable', an entity can take technical and resource considerations into account. However, it is the responsibility of the data holder to justify any delay in providing the notice.

11.47 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.

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.

Accredited data recipients

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

11.48 For accredited data recipients, there is no CDR Rule in relation to advising consumers that disclosed CDR data was incorrect. This is because an accredited data recipient may only disclose CDR data if required or authorised under another Australian law or court/tribunal order,[14] or under the CDR Rules to the consumer or an outsourced service provider.

11.49 If an accredited data recipient discloses CDR data:

- to the consumer or an outsourced service provider in accordance with the CDR Rules,[15] or
- as required or authorised under another Australian law or court/tribunal order,

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

11.50 However, accredited data recipients have obligations under Privacy Safeguard 13 to respond to requests from consumers to correct their CDR data. See Chapter 13 (Privacy Safeguard 13) for further information.

11.51 In addition, where an accredited data recipient realises that it has disclosed CDR data to an outsourced service provider that was incorrect at the time of disclosure, the accredited data recipient must, if applicable:

- disclose the corrected CDR data to relevant outsourced service providers, or
- ensure that relevant outsourced service providers take steps to correct the CDR data, and
- direct these outsourced service providers to destroy or de-identify the incorrect CDR data.[16]

[14] Section 56EI(1)(c) of the Competition and Consumer Act.

[15] CDR Rule 7.5(1). For further information, see Chapter 6 (Privacy Safeguard 6).

[16] If CDR data collected by an accredited person, or CDR data derived from it, is disclosed to an outsourced service provider, any use or disclosure of that CDR data by the outsourced service provider (whether or not in accordance with the underlying CDR outsourcing arrangement) is taken to have been by the accredited person (CDR Rule 7.6).

As such, an accredited data recipient must ensure outsourced service providers have correct CDR data as part of meeting their obligations under Privacy Safeguard 11 to ensure CDR data is accurate, up to date and complete. See CDR Rule 1.10 for information regarding the accredited person's ability to direct the outsourced service provider to take certain actions.

Disclosing corrected CDR data to the original recipient

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

11.52 Privacy Safeguard 11 requires a data holder to disclose corrected CDR data to the original recipient[17] of the disclosure if:[18]

- 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 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 under 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).

11.55 This means that if a data holder includes a qualifying statement with CDR data rather than correcting it in response to a request from the consumer to correct the data, and the CDR data had been disclosed to an accredited person before the qualifying statement was included, then Privacy Safeguard 11 requires the data holder to (in response to a consumer's request) re-disclose that CDR data, which now includes the qualifying statement, to that accredited person.

Record keeping requirements

11.56 If an entity discloses corrected CDR data in accordance with Privacy Safeguard 11,[19] 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.

11.57 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.[20] If corrected data is disclosed, the data holder must keep and

[17] 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).

[18] 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.

[19] Section 56EN(4) of the Competition and Consumer Act.

[20] CDR Rule 9.3(1)(d). For further information on record keeping requirements for data holders, see the Guide to privacy for data holders.

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'.

11.58 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.[21] This means that, similarly to data holders, accredited data recipients must keep and maintain a record of both the initial collection of the incorrect CDR data and the subsequent collection of the corrected CDR data, in circumstances where corrected CDR data is disclosed under s 56EN(4).

How does Privacy Safeguard 11 interact with the other privacy safeguards?

Privacy Safeguard 5

11.59 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.

11.60 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

11.61 Privacy Safeguard 10 requires data holders to notify a consumer of the disclosure of their CDR data by updating the consumer's dashboard.

11.62 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. *cont*

[21] CDR Rule 9.3(2)(e).

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

11.63 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

11.64 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.

11.65 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.[22]

11.66 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.

[22] 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 1.0, February 2020

OAIC

Contents

Key points

- Securing CDR data is an integral element of the consumer data right (CDR) regime.
- Privacy Safeguard 12 places requirements on accredited data recipients and designated gateways to ensure CDR data is protected from misuse, interference and loss, as well as from unauthorised access, modification or disclosure. The specific steps that these entities must take to protect CDR data are in the consumer data rules (CDR Rules).
- In addition, if an accredited data recipient or a designated gateway no longer needs the CDR data for purposes permitted by privacy safeguards or the 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 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 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 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 national 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 Dealing with 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 and designated gateways. 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: *Currently, there are no designated gateways in the CDR regime responsible for facilitating the transfer of information between data holders and accredited persons (see Chapter B (Key concepts) for the meaning of designated gateway).*

Accreditation guidelines on information security

12.10 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.[1]

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
Accredited person / Accredited data recipient	**Privacy Safeguard 12** Privacy Safeguard 12 applies instead of APP 11 to CDR data collected by an accredited data recipient under the CDR regime. APP 11 will continue to apply to the security of personal information held by an accredited person or accredited data recipient that is not CDR data. [2] **Note:** All accredited persons must also demonstrate compliance with Privacy Safeguard 12 to maintain accreditation under the CDR regime. [3]
Designated gateways	**Privacy Safeguard 12** Privacy Safeguard 12 applies instead of APP 11 in relation to the security of CDR data.[4] APP 11 will continue to apply to any personal information held that is not CDR data.
Data holders	**APP 11** Privacy Safeguard 12 does not apply to data holders.

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

[2] All accredited persons are subject to the Privacy Act and the APPs in relation to information that is personal information but is not CDR data. See s 6E(1D) of the Privacy Act.

[3] See the ACCC's Supplementary Accreditation Guidelines on Information Security for more information.

[4] Section 56EC(4)(d) of the Competition and Consumer Act.

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. [5]
- **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.[6]
- **Unauthorised access:** occurs where CDR data is accessed by someone who is not permitted to do so. This includes unauthorised access by an employee of the accredited data recipient or designated gateway, or an independent contractor, as well as unauthorised access by an external third party. For example, unauthorised access would occur if a computer network is compromised by an external attacker resulting in CDR data being accessed without authority.
- **Unauthorised modification:** occurs where CDR data is altered by someone who is not permitted to do so, or where the data is altered in a way that is not permitted. For example, unauthorised modification would occur if an employee of an accredited

[5] Privacy Safeguard 6 sets out when an accredited data recipient of CDR data or a designated gateway of CDR data is permitted to use that CDR data (see Chapter 6 (Privacy 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)).

[6] Loss does not apply to intentional destruction or de-identification of CDR data undertaken in accordance with the CDR Rules.

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.

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.

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[7] 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.[8] An accredited data recipient may also utilise existing frameworks, requirements and models in developing their information security governance framework and defining security areas.[9]

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.

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

[8] For further information, see the ACCC's Supplementary Accreditation Guidelines on Information Security.

[9] 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.[10]

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.[11] 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.[12]

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.[13] These committees or forums should include membership from across key business areas, particularly where the entity's CDR data environment is large or complex,[14] 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

[10] Clause 1.3(2) of Schedule 2 to the CDR Rules.

[11] 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.

[12] The ACCC's Supplementary Accreditation Guidelines on Information Security.

[13] The ACCC's Supplementary Accreditation Guidelines on Information Security.

[14] 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.[15]

12.35 The information security policy must include information about[16]:

- 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.[17]

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.

---

[15] Clause 1.3(3) of Schedule 2 to the CDR Rules.

[16] Clause 1.3(3) of Schedule 2 to the CDR Rules.

[17] 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.[18]

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.[19]

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.[20]

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 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.

[18] Clause 1.3(4) of Schedule 2 to the CDR Rules.

[19] See the ACCC's Supplementary Accreditation Guidelines on Information Security.

[20] 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.[21]

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

[21] 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 provide goods or services to a consumer, the accredited data recipient must ensure their contract with the outsourced service provider requires them to take the steps outlined in Schedule 2 as if the outsourced service provider were an accredited data recipient.[22]

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

- assessing whether the information security capabilities of the outsourced service provider, having regard to the nature of the goods or services provided in relation to

[22] CDR Rule 1.10(2)(b)(i).

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.[23]

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.[24]

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.[25]

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
- the likelihood of failure of controls having regard to the results of previous testing.[26]

---

[23] CDR Rule 1.10(2).

[24] Clause 1.5(2) of Schedule 2 to the CDR Rules.

[25] Clause 1.6(1)(a) of Schedule 2 to the CDR Rules.

[26] Clause 1.6(1)(b) of Schedule 2 to the CDR Rules.

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.[27] 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.[28]

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.[29]

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.[30]

12.64 The accredited data recipient must review the sufficiency of its testing program:

a. when there is a material change to the nature and extent of threats to its CDR data environment or to its CDR data environment, as soon as practicable, or

b. where no such material changes occur, at least annually.[31]

Step 5: Manage and report security incidents

12.65 An accredited data recipient must have procedures and practices in place to detect, record, and respond to information security incidents as soon as practicable.[32] 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.[33]

12.67 The accredited data recipient's CDR data security response plans must include procedures for:

a. managing all relevant stages of an incident, from detection to post-incident review

b. notifying CDR data security breaches to the Information Commissioner and to consumers as required under Part IIIC of the Privacy Act,[34] and

[27] Clause 2.1(2) of Schedule 1 to the CDR Rules.

[28] Clause 1.6(2) of Schedule 2 to the CDR Rules.

[29] Clause 1.6(3) of Schedule 2 to the CDR Rules.

[30] Clause 1.6(4) of Schedule 2 to the CDR Rules.

[31] Clause 1.6(4) of Schedule 2 to the CDR Rules.

[32] Clause 1.7(1) of Schedule 2 to the CDR Rules.

[33] Clause 1.7(2) of Schedule 2 to the CDR Rules.

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

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.[35]

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.[36]

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'.[37]

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.[38]

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.[39]

[35] Clause 1.7(3) of Schedule 2 to the CDR Rules.

[36] Clause 1.7(4) of Schedule 2 to the CDR Rules.

[37] Section 56ES of the Competition and Consumer Act.

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

[39] 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.[40] 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.

[40] 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.[41]

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.[42]

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:[43]

- 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.[44]

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.[45]

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.

---

[41] See section 56EO(2)(a) of the Competition and Consumer Act.

[42] CDR Rule 5.23(4).

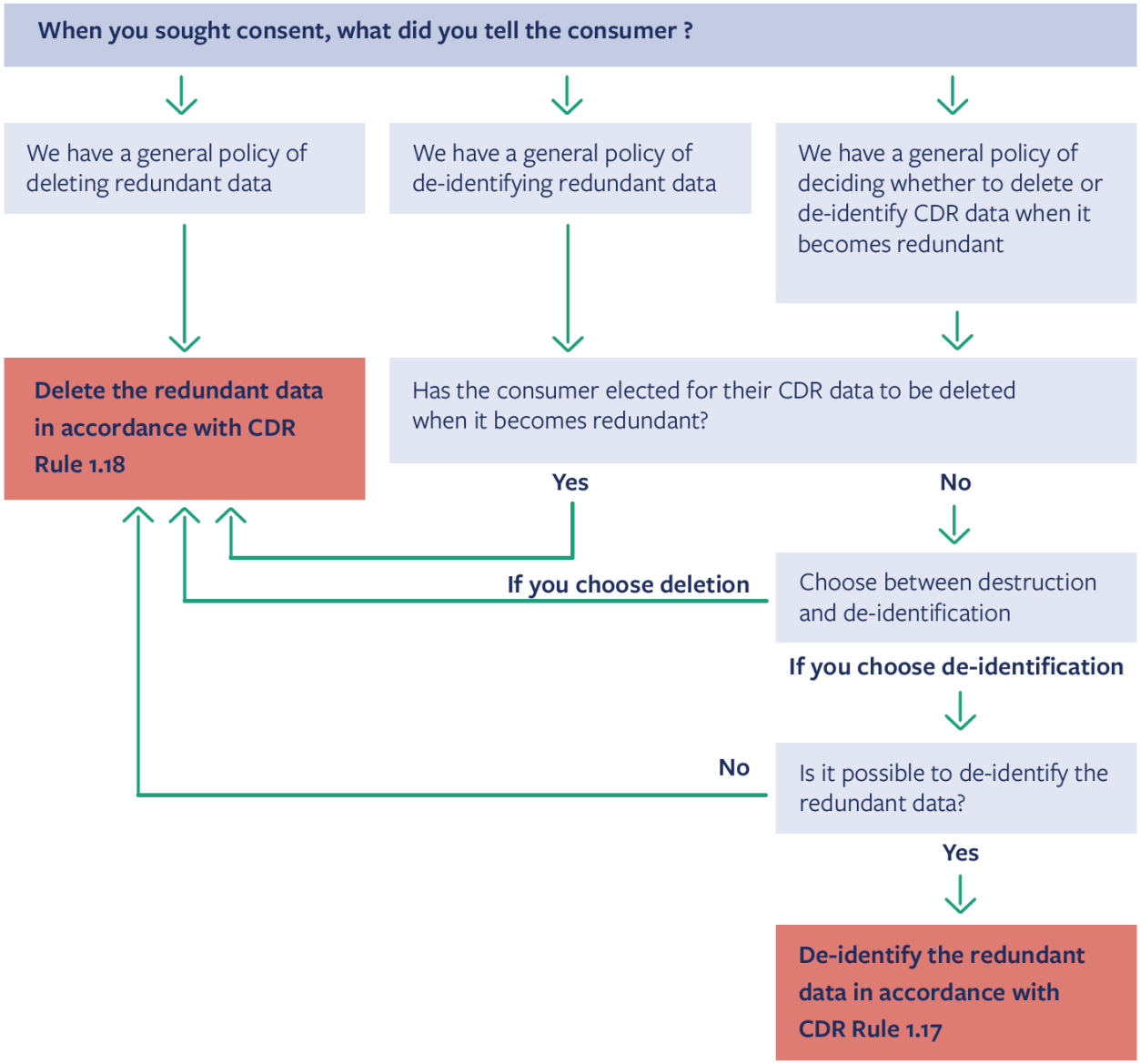
[43] See section 56EO(2) of the Competition and Consumer Act.

[44] See section 56BAA of the Competition and Consumer Act and CDR Rule 1.17A.

[45] 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 to collect and use their CDR data,[46] 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.[47]

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). [48]

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.[49]

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).

---

[46] CDR Rule 4.11(3).

[47] CDR Rule 4.17(1).

[48] CDR Rule 4.16. See also 'reasonably identifiable' in Chapter B (Key concepts).

[49] 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.[50] 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.[51]

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

[50] CDR Rule 1.18

[51] CDR Rule 1.17(1).

released into an open environment, or what controls and safeguards apply to the data access environment).[52]

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[53], they can then proceed to de-identify the data in accordance with the 'CDR data de-identification process' set out in the CDR Rules.[54] 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'.[55]

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.[56] The CDR data deletion process is set out in CDR Rule 1.18.

12.103 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

[52] CDR Rule 1.17(2)(f).

[53] See paragraphs 12.91 to 12.99.

[54] CDR Rule 1.17.

[55] CDR Rule 1.17(4).

[56] CDR Rule 7.13.

- 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'

12.104 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.[57]

12.105 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?

12.106 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).

12.107 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[58]
- commits to take reasonable steps to irretrievably destroy the data if, or when, this becomes possible.

[57] CDR Rule 1.18(a).

[58] This should go beyond the minimum access controls specified in the CDR Rules.

12.108 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.

Make a record to evidence the deletion

12.109 The accredited data recipient must also make a record to evidence the deletion.[59]

12.110 The accredited data recipient must also direct any other person to which it has disclosed[60] that CDR data to:

- delete, to the extent reasonably practicable, any copies of that CDR data, or any CDR data directly or indirectly derived from it, that it holds
- make a record to evidence the steps taken to delete the CDR data, and
- notify the person who gave the direction to delete.[61]

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

12.111 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).[62]

12.112 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.[63]

12.113 As soon as practicable after undertaking the de-identification process, the accredited data recipient must record the process including:

---

[59] CDR Rule 1.18(b).

[60] Currently, an accredited data recipient is only authorised to disclose CDR data to an outsourced service provider or the consumer to which the CDR data relates (CDR Rule 7.5(1)).

[61] CDR Rule 1.18(c). Where the accredited data recipient has disclosed the relevant CDR data to an outsourced service provider, CDR Rule 1.18(c)(iii) requires the outsourced service provider to notify the accredited data recipient that the deletion has occurred.

[62] 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.

[63] CDR Rule 1.17(3).

- details of the assessment that it is possible to de-identify the relevant data to the required extent
- that the relevant data was de-identified to that extent
- how the relevant data was de-identified, including specifying the technique that was used, and
- any persons to whom the de-identified data is disclosed.

12.114 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.

Outsourced service providers

12.115 Accredited data recipients undertaking the de-identification process must also direct any outsourced service providers[64] to return or delete the redundant data, as well as any data directly or indirectly derived from the redundant data. [65]

12.116 Where the accredited data recipient receives redundant data from an outsourced service provider, it must de-identify the data in accordance with the CDR de-identification process, as it would with any other redundant data.

12.117 The accredited data recipient is responsible for ensuring these directions are made to any other person who has received the data. If the outsourced service provider has also disclosed the data to another person, the accredited data recipient must 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.[66]

Other relevant security obligations

Privacy safeguards

12.118 Compliance with the privacy safeguards as a whole will promote security and reduce the risk of CDR data being accidently 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.

12.119 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 (see Chapter 1 (Privacy Safeguard 1)).

12.120 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)).

---

[64] For information on outsourced service providers, see Chapter B (Key concepts).

[65] CDR Rule 7.12(2)(b).

[66] CDR Rule 7.12(2)(b)(ii).

12.121 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.

Chapter 13:

Privacy Safeguard 13 —

Correction of CDR data

Version 2.0, July 2020

OAIC

Contents

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 to:
  - respond to correction requests made by consumers in respect of 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 who:

- receive a request from a consumer to correct 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, to the extent it considers appropriate:

- correct the CDR data, or
- qualify the data by including a statement with it, and
- give the consumer a notice setting out how the entity responded to the request, as well as the complaint mechanisms available to the consumer.

13.3 CDR Rule 7.14 prohibits charging a fee for responding to or actioning a correction request.

Why is it important?

13.4 The objective of Privacy Safeguard 13 is to ensure consumers have trust in and control over the accuracy of their CDR data that is disclosed and used as part of the CDR regime.

13.5 For consumers to have proper control over their data, they must be given the power to require the entities that have disclosed or collected their data to correct inaccuracies in that data.

13.6 Privacy Safeguard 13 does this by ensuring entities are required to correct CDR data in certain circumstances when requested to do so by the consumer.

13.7 This allows consumers to enjoy the benefits of the CDR regime, such as receiving competitive offers from other service providers, as the data made available to sector participants can be relied upon.

Who does Privacy Safeguard 13 apply to?

13.8 Privacy Safeguard 13 applies to data holders and accredited data recipients for the CDR data. It does not apply to designated gateways.

13.9 Importantly, Privacy Safeguard 13 only applies to the CDR data a data holder was required or authorised to disclose under the CDR Rules.[1]

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

How Privacy Safeguard 13 interacts with the Privacy Act

13.10 It is important to understand how Privacy Safeguard 13 interacts with the *Privacy Act 1988* (the Privacy Act) and Australian Privacy Principles (APPs).[2]

13.11 APP 13 requires an APP entity to correct personal information held by the entity in certain circumstances.

CDR entity	Privacy protections that apply in the CDR context
Accredited person / accredited data recipient	**Privacy Safeguard 13** Privacy Safeguard 13 applies instead of APP 13 to CDR data collected by an accredited data recipient under the CDR regime.[3] APP 13 will continue to apply to any personal information held by an accredited person or accredited data recipient that is not CDR data.[4]

[1] Section 56EP(1)(c) of the Competition and Consumer Act.

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

[3] Section 56EC(4)(a) of the Competition and Consumer Act.

[4] All accredited persons are subject to the Privacy Act and the APPs in relation to information that is personal information but is not CDR data. See s 6E(1D) of the Privacy Act.

CDR entity	Privacy protections that apply in the CDR context
Data holder	**Privacy Safeguard 13 or APP 13** 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 authorised or required to disclose it under the CDR Rules. APP 13 will continue to apply to: • CDR data that is personal information in all other circumstances, and • personal information that is not CDR data. **Note:** Where the consumer has not made a correction request or the CDR data has not previously been disclosed, a data holder who is an APP entity continues to have obligations under APP 13. Specifically, the data holder 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.
Designated gateway	**APP 13** Privacy Safeguard 13 does not apply to designated gateways.

When must an entity correct CDR data?

13.12 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.[5]

Actioning and responding to correction requests

Acknowledging receipt of correction requests

13.13 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.

13.14 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.

13.15 However, it is not a requirement that this acknowledgement be in writing or through the dashboard. For example, acknowledgement provided by other electronic means or over the

[5] For data holders, this obligation only arises if the entity was required or authorised under the CDR Rules to disclose the CDR data.

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).

13.16 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

13.17 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.

to the extent that the entity considers appropriate.

13.18 An entity must first consider the extent to which it considers it appropriate to act to correct or qualify the information. Once it determines this, it must undertake either to correct the data or to include a qualifying statement with the data. Such corrections or qualifying statements must make the data accurate, up to date, complete and not misleading (to the best of the entity's knowledge).

13.19 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.

13.20 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.

13.21 An entity should also be prepared in an appropriate case to search its own records and other readily accessible sources that it reasonably expects to contain relevant information, to find any information in support of, or contrary to, the consumer's request. However, an entity need not conduct a full, formal investigation into the matters about which the consumer requests correction. The extent of the investigation required will depend on the circumstances, including the seriousness of any adverse consequences for the consumer if the CDR data is not corrected as requested.

When action is not necessary in response to a request

13.22 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.

13.23 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.[6]

13.24 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),[7] 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.

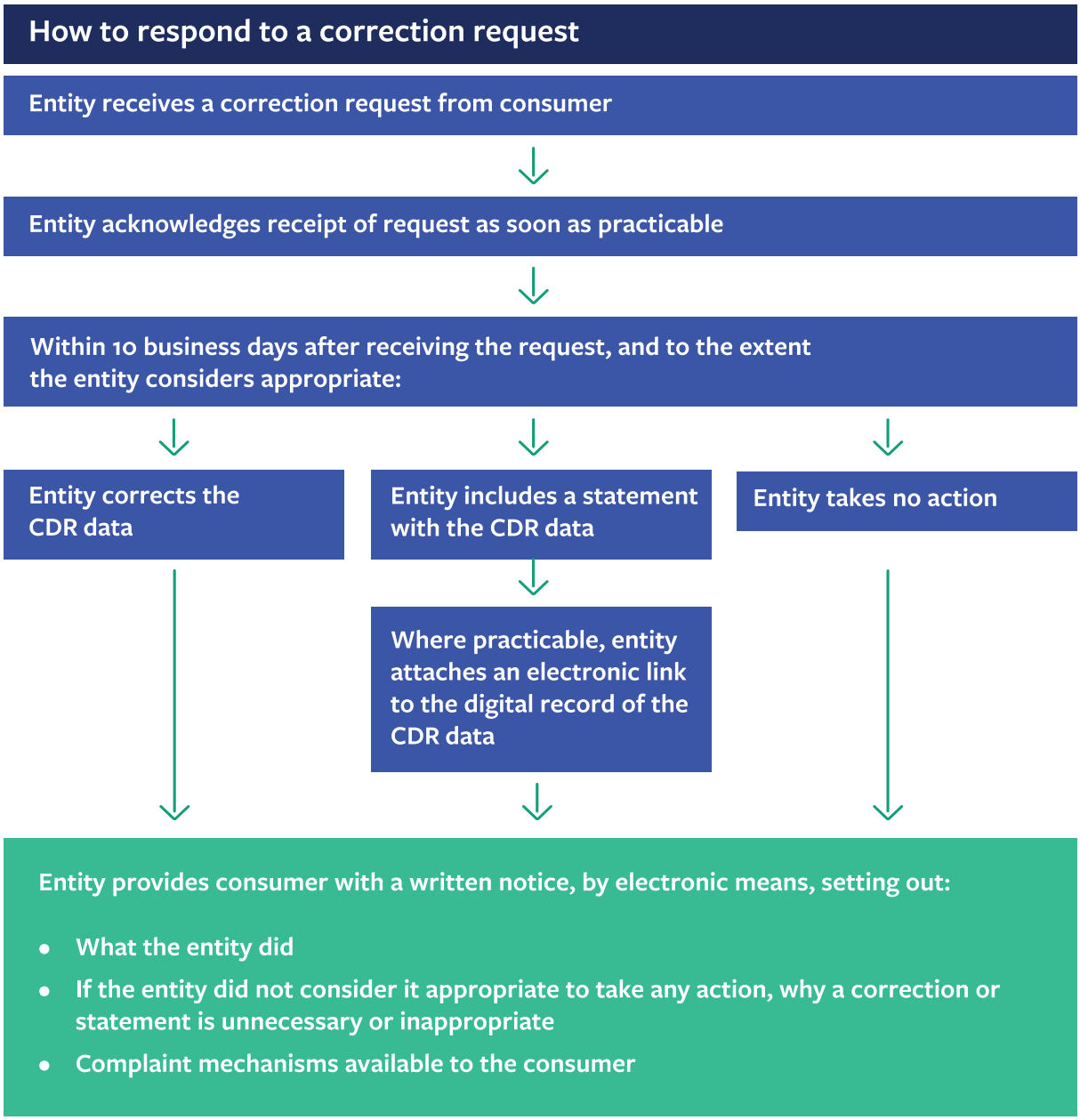
CreditCardFinder determines that because the CDR data was collected from BankaLot and CreditCardFinder has no method of independently determining the correctness of the data, it is not appropriate for it to make any corrections or include any qualifying statements with the data.

CreditCardFinder then gives Jessica a notice through her consumer dashboard that states this finding, and that if Jessica wants the data to be corrected, she should request that BankaLot make the relevant correction. *cont*

[6] Section 56EP(3)(b) of the Competition and Consumer Act.

[7] 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.

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 must a correction notice be provided to consumers?

13.25 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 13.29 below.

13.26 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.

13.27 The written notice may be in the body of an email or in an electronic file attached to an email.

13.28 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?

13.29 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.

13.30 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,[8] and any external dispute resolution schemes recognised by the Australian Competition and Consumer Commission under s 56DA(1) of the Competition and Consumer Act.

13.31 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?

13.32 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'.[9] 'Held' is discussed in Chapter B (Key concepts).

13.33 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.

13.34 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.[10] 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

[8] Section 56ET(4) of the Competition and Consumer Act.

[9] Section 56EP(3)(a)(ii) of the Competition and Consumer Act.

[10] Section 56EP(4) of the Competition and Consumer Act.

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).

13.35 These four terms are not defined in the Competition and Consumer Act or the Privacy Act.[11]

13.36 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*.[12] As the analysis indicates, there is overlap in the meaning of the terms.

Accurate

13.37 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.

13.38 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.[13] 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.

13.39 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

13.40 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.[14]

13.41 CDR data about a past event may have been up to date at the time it was recorded but has been overtaken by a later development. Whether that data is up to date will depend on the purpose for which it is held. If, for instance, a consumer has had their second child but their CDR data records them as only having one child, the CDR data will still be up to date if the data that records the consumer as having one child is held simply for the purpose of recording whether the consumer is a parent.

---

[11] 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 an example of an entity determining the purpose for which it holds CDR data at paragraph 11.15.

[12] See Chapter 10: APP 10 — Quality of personal information of the APP Guidelines.

[13] Data derived from CDR data continues to be 'CDR data': see s 56AI of the Competition and Consumer Act.

[14] Such an assessment will likely be 'materially enhanced information' under section 10 of the designation instrument and therefore not 'required consumer data' under the CDR Rules.

13.42 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

13.43 CDR data is incomplete if it presents a partial or misleading picture of a matter of relevance, rather than a true or full picture.

13.44 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

13.45 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.

13.46 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). Angelica has consented to XYZ collecting and using the 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 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

13.47 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

13.48 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.

13.49 Where an accredited person has collected CDR data, and then collects corrected data after the data holder complies with the consumer's requests to correct and disclose corrected data under Privacy Safeguards 11 and 13, the accredited person must notify that consumer under Privacy Safeguard 5 in respect of both collections.

Privacy Safeguard 10

13.50 Privacy Safeguard 10 requires a data holder to notify a CDR consumer of the disclosure of their CDR data by updating the consumer's dashboard.

13.51 Where a data holder has disclosed CDR data and then discloses corrected data as the result of the consumer's requests to correct and disclose corrected data under Privacy Safeguards 11 and 13, the data holder must notify that consumer under Privacy Safeguard 10 in respect of both disclosures.

Privacy Safeguard 11

13.52 A correction request made under Privacy Safeguard 13 may trigger a CDR entity's obligations under Privacy Safeguard 11 (Quality of CDR data).

13.53 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.

13.54 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.

13.55 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.[15]

Privacy Safeguard 12

13.56 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.

[15] Section 56EN(3) of the Competition and Consumer Act.