Chapter A:

Introductory matters

Version 3.0, June 2021

OAIC

Contents

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

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 are able to exercise the CDR in relation to data that is covered by the CDR regime.

A.9 The CDR has commenced in the banking sector (known as 'Open Banking'). Next, CDR will be implemented in the energy sector.[2] It will then be introduced sector by sector across the broader economy as designated by the Minister.

About the privacy safeguards

A.10 The privacy safeguards are legally binding statutory provisions, which ensure the security and integrity of the CDR regime. The specific requirements for certain privacy safeguards are set out in the CDR Rules.

A.11 The privacy safeguards set out standards, rights and obligations in relation to collecting, using, disclosing and correcting CDR data for which there are one or more consumers:

- Privacy Safeguard 1: Open and transparent management of CDR data
- Privacy Safeguard 2: Anonymity and pseudonymity
- Privacy Safeguard 3: Seeking to collect CDR data from CDR participants
- Privacy Safeguard 4: Dealing with unsolicited CDR data from CDR participants
- Privacy Safeguard 5: Notifying of the collection of CDR data
- Privacy Safeguard 6: Use or disclosure of CDR data by accredited data recipients or designated gateways
- Privacy Safeguard 7: Use or disclosure of CDR data for direct marketing by accredited data recipients or designated gateways
- Privacy Safeguard 8: Overseas disclosure of CDR data by accredited data recipients
- Privacy Safeguard 9: Adoption or disclosure of government related identifiers by accredited data recipients
- Privacy Safeguard 10: Notifying of the disclosure of CDR data
- Privacy Safeguard 11: Quality of CDR data
- Privacy Safeguard 12: Security of CDR data, and destruction or de-identification of redundant CDR data
- Privacy Safeguard 13: Correction of CDR data

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

A.12 The privacy safeguards only apply to CDR data for which there are one or more 'CDR consumers'.[3] A CDR consumer can be an individual or a business enterprise.[4]

A.13 There are a number of factors that determine whether CDR data has a 'CDR consumer'.[5] In particular, for CDR data to have a CDR consumer, at least one person needs to be identifiable or reasonably identifiable from the CDR data or other information held by the relevant entity.[6] See paragraphs B.42 to B.66 in Chapter B (Key concepts) of the CDR Privacy Safeguard Guidelines for the full meaning of 'CDR consumer'.

A.14 The privacy safeguards do not apply where there is no CDR consumer[7] because, for example, there is no person that is identifiable or reasonably identifiable from the data. Product data is an example of CDR data for which there is no CDR consumer.

A.15 The privacy safeguards are structured to reflect the CDR data lifecycle. They are grouped into five subdivisions within Division 5 of Part IVD of the Competition and Consumer Act:

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

A.16 The requirements in each of these privacy safeguards interact with and complement each other.

How to use these guidelines

A.17 The structure of the Privacy Safeguard guidelines reflects the structure of the privacy safeguards: Privacy Safeguards 1 to 13 are each dealt with in separate chapters.

A.18 The number of the chapter corresponds to the number of the privacy safeguard.

A.19 Chapter B contains guidance on general matters, including an explanation of key concepts that are used throughout the privacy safeguards and the Privacy Safeguard guidelines.

A.20 Chapter C contains guidance on consent, which is the primary basis for collecting, using and disclosing CDR data under the CDR regime.

A.21 These guidelines should be read together with the full text of Division 5 of Part IVD of the Competition and Consumer Act and the CDR Rules.

---

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

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

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

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

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

Who must comply with the privacy safeguards?

A.22 The privacy safeguards apply to entities who are authorised or required under the CDR regime to collect, use or disclose CDR data for which there is at least one consumer. This includes:

- **accredited persons:** persons who have been granted accreditation by the Australian Competition and Consumer Commission to receive data through the CDR regime[8]
- **accredited data recipients:** accredited persons who have collected the CDR data from a data holder or another accredited data recipient[9]
- **data holders:** the holders of the original data that the transfer of data applies to, [10] and
- **designated gateways:** entities designated by the Minister as responsible for facilitating the transfer of information between data holders and accredited persons.[11]

A.23 Each of these types of entities are defined in the Competition and Consumer Act and discussed further in Chapter B (Key concepts).

A.24 Each privacy safeguard chapter specifies the type of entity to which it applies.

A.25 The privacy safeguards extend to acts, omissions, matters and things outside Australia.[12]

A.26 In respect of CDR data held within Australia, the privacy safeguards apply to all persons, including foreign persons.[13]

A.27 In respect of an act or omission relating to CDR data held outside Australia, the privacy safeguards only apply if the act or omission:[14]

- 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.

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

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

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

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

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

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

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

Which privacy protections apply in the CDR context?

CDR entity	Privacy safeguards that apply in the CDR context	APPs that apply in the CDR context
Accredited person	Privacy safeguards 1–4[15]	None. Privacy Safeguards 1–4 apply instead of the corresponding APPs.[16]
Accredited data recipient[17]	Privacy safeguards 1, 2 and 5–13	None. The APPs do not apply to an accredited data recipient of a consumer's CDR data in relation to that data.
Data holder	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

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

A.28 Section 56EC(4) of the Competition and Consumer Act sets out when a privacy safeguard applies instead of an Australian Privacy Principle (APP) under the *Privacy Act 1988* (Privacy Act).

A.29 The privacy safeguards apply only to CDR data for which there are one or more CDR consumers.[18]

---

[15] See ss 56EC(4), 56ED, 56EE(1)(b), 56EF and 56EG of the Competition and Consumer Act.

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

[17] An accredited person becomes an accredited data recipient for CDR data when:

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

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

A.30 As set out in paragraph A.13 above, for there to be a CDR consumer, at least one person must be identifiable or reasonably identifiable from the CDR data or other information held by the relevant entity. As such, where the consumer is an individual, CDR data protected by the privacy safeguards will contain information about an identified or reasonably identifiable individual, and will therefore also be 'personal information' under the Privacy Act.

A.31 To work out when the privacy safeguards apply, an entity needs to consider what capacity they are acting in – as a data holder, accredited person/accredited data recipient, or designated gateway.

A.32 In each chapter in these guidelines, the interaction between the privacy safeguard and corresponding APP is discussed.

Accredited persons and accredited data recipients

A.33 For an accredited person or accredited data recipient of CDR data, the privacy safeguards apply instead of the APPs in relation to the handling of the CDR data within the CDR system.[19]

Data holders

A.34 For data holders, the APPs will apply to CDR data that is also personal information with the exception of APPs 10 (quality of personal information) and 13 (correction of personal information). These two APPs are replaced by Privacy Safeguards 11 (quality of CDR data) and 13 (correction of CDR data) once the data holder is required or authorised to disclose the CDR data under the CDR Rules. Privacy Safeguard 10 does not have an APP equivalent and applies to data holders in addition to all other privacy protections.

A.35 Data holders must also comply with both APP 1 and Privacy Safeguard 1 which relate to open and transparent management of personal information and CDR data respectively. As explained above, these obligations apply concurrently and the obligations in Privacy Safeguard 1 do not displace the APP 1 obligations.

Designated gateways

A.36 The APPs will continue to apply to designated gateways for CDR data that is personal information except in relation to the use and disclosure of CDR data, including for direct marketing purposes, for which Privacy Safeguards 6 (use or disclosure of CDR data) and 7 (direct marketing) apply instead of APP 6 and APP 7, and the security of the CDR data, for which Privacy Safeguard 12 (security of CDR data) applies instead of APP 11.

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

---

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

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

What happens if an entity breaches the privacy safeguards?

A.38 The Information Commissioner has powers to investigate possible breaches of the privacy safeguards, either following a complaint by a consumer who is an individual or small business or on the Information Commissioner's own initiative.

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

A.40 The Information Commissioner has a range of enforcement powers and other remedies available. These powers include those available under:

- Part V of the Privacy Act,[20] for example the power to make a determination,[21] 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.[22]

A.41 The Australian Competition and Consumer Commission (ACCC) also have a strategic enforcement role where there are repeated or serious breaches. The Office of the Australian Information Commissioner (OAIC) and the ACCC have published a joint Compliance and Enforcement Policy for the CDR intended to help consumers and CDR entities understand the approach that the OAIC and ACCC will take to encourage compliance with the CDR Rules, legislation (including privacy safeguards and Consumer Data Standards) and how they will respond to breaches of the regulatory framework. The OAIC has also published a CDR Regulatory Action Policy which sets out the OAIC's priorities, goals and principles in regulating the CDR, and complements the joint Compliance and Enforcement Policy.

Where do I get more information?

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

[20] 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.

[21] Section 52 of the Privacy Act.

[22] Section 56EU of the Competition and Consumer Act. All privacy safeguards contain civil penalty provisions except for Privacy Safeguard 2.