Chapter A:

Introductory matters

Version 1.0, February 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 of 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 consumer.[15] 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.[16]

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.

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.

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

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.

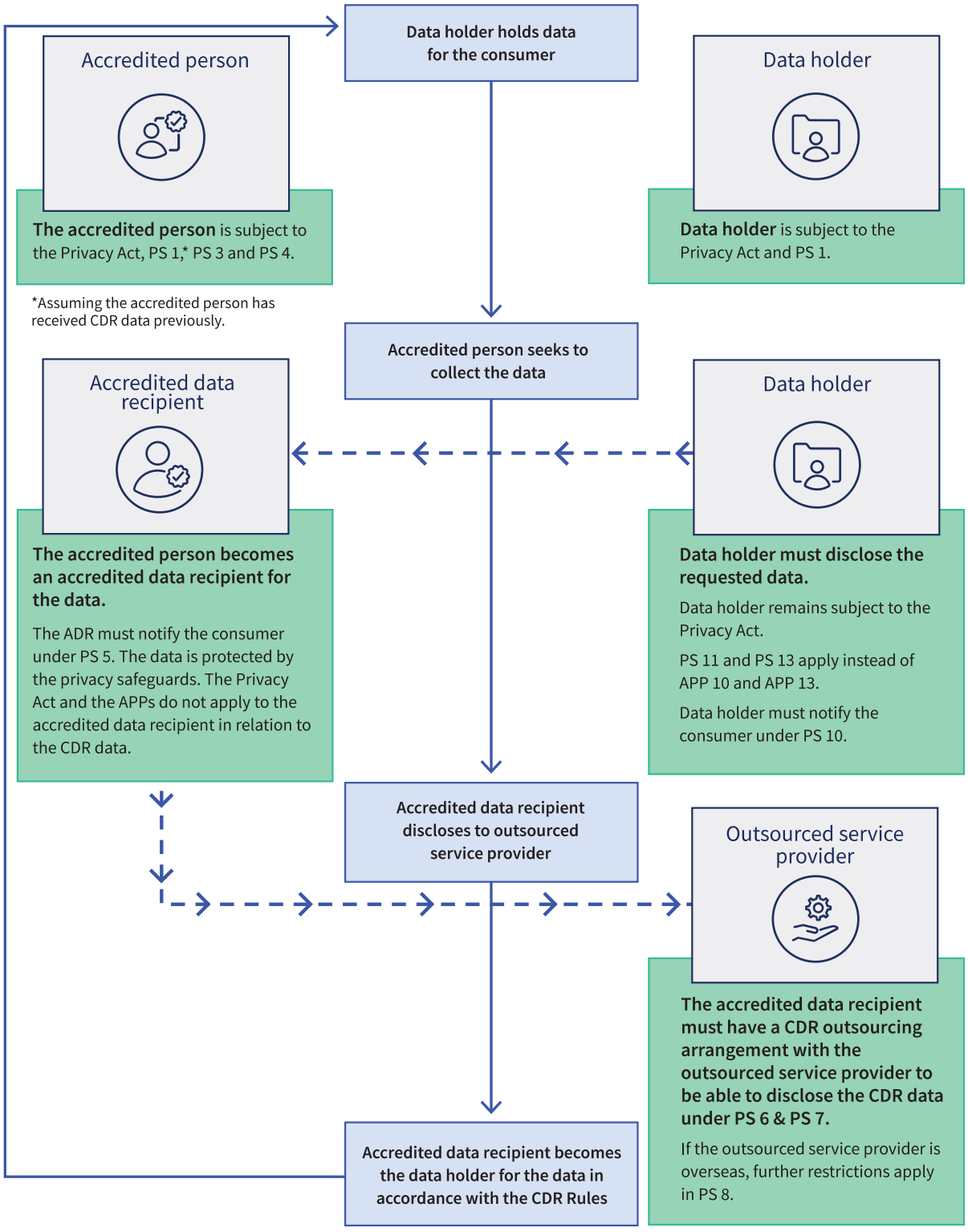
Designated gateways

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,[17] for example the power to make a determination,[18] 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.[19]

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.

[17] 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.

[18] Section 52 of the Privacy Act.

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