Chapter 2:

Privacy Safeguard 2 —

Anonymity and pseudonymity

Consultation draft, September 2022

OAIC

Contents

Key points

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

What does Privacy Safeguard 2 say?

2.1 Privacy Safeguard 2 provides that a consumer must have the option of not identifying themselves, or of using a pseudonym, when dealing with an accredited person (who is or who may become an accredited data recipient of the consumer's CDR data) in relation to that 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 person unless an exception applies. The exceptions are set out in subrule 7.3(1) of the consumer data ~~rule~~rules (CDR ~~Rule) 7.3.~~Rules).

2.3 ~~Consumer data rule (~~ Subrule 7.3(1) of the CDR ~~Rule) 7.3~~Rules sets out that an accredited data recipient or accredited person who may become an accredited data recipient of a consumer's CDR data does not need to allow anonymity or pseudonymity where:[1]

- ~~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~~the entity 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~~.~~, or
- if the entity is an accredited data recipient, it is impracticable to deal with a consumer who has not identified themselves or has used a pseudonym in relation to the CDR data.

Who does Privacy Safeguard 2 apply to?

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

~~2.5 It does not apply to data holders or designated gateways.~~

~~2.6~~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),~~APPs, including APP 2 when dealing with individuals.

2.6 As a non-accredited entity, a CDR representative is not directly bound by Privacy Safeguard 2. However, under the terms of the CDR representative arrangement with their CDR

[1] ~~The exceptions in CDR Rule 7.3 do not apply to an accredited person who is not yet an accredited data recipient of CDR data.~~

principal,[2] a CDR representative is required to comply with Privacy Safeguard 2 in its handling of service data as if it were the CDR principal.[3,4] A CDR principal breaches subrule 7.3(2) of the CDR Rules if its CDR representative fails to comply with Privacy Safeguard 2 as if it were an accredited person (regardless of whether the CDR representative's actions accord with the CDR representative arrangement).[5]

How Privacy Safeguard 2 interacts with the Privacy Act

2.7 It is important to understand how Privacy Safeguard 2 interacts with the Privacy Act and the APPs.[6]

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

CDR entity	Privacy protections that apply in the CDR context
Accredited person who may become an accredited data recipient	**Privacy Safeguard 2** When an accredited person is dealing with a CDR consumer's data, and may become an accredited data recipient of that CDR data (for example, because they are seeking to collect it), Privacy Safeguard 2 applies. APP 2 does not apply to the accredited person in relation to dealings with the consumer regarding that CDR data.[7]
Accredited data recipient[8]	**Privacy Safeguard 2** An accredited data recipient of CDR data must comply with Privacy Safeguard 2 when dealing with the CDR consumer in relation to their CDR

[2] A CDR representative arrangement is a written contract between a CDR representative and their CDR principal that meets the minimum requirements listed in the CDR Rules, subrule 1.10AA(2).

[3] CDR Rules, paragraph 1.10AA(2)(d)(i)(A).

[4] See Chapter B (Key concepts) for more information on 'CDR principal', 'CDR representative', 'CDR representative arrangement' and 'service data'.

[5] CDR Rules, subrules 7.3(2) and 7.3(3).

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

[7] See ~~ss 56EC(4) and 56EE(1)(b) of the~~ Competition and Consumer Act~~.~~, subsection 56EC(4) and paragraph 56EE(1)(b).

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

[8] 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~~CDR Rules, and
- the person is neither a data holder, nor a designated gateway, for the first mentioned CDR data. See s ~~56EK~~56AK of the Competition and Consumer Act.

	data. APP 2 does not apply to the accredited data recipient in relation to that CDR data.[9]
Designated gateway	~~Australian Privacy Principle 2~~ APP 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[10]	~~Australian Privacy Principle 2~~ APP 2 Privacy Safeguard 2 does not apply to a data holder.

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

Why anonymity and pseudonymity are important

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

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

What is the difference between anonymity and pseudonymity?

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

[9] The APPs do not apply to an accredited data recipient of the CDR data in relation to the CDR data (~~s 56EC(4) of the~~ Competition and Consumer Act~~)~~., subsection 56EC(4)).

[10] In this chapter, references to data holders include AEMO. See Chapter B for further information about how the privacy safeguards apply to AEMO.

2.12 Pseudonymity means that a consumer may use a name, term or descriptor that is different to the consumer's actual name (e.g. an email address that does not contain the consumer's actual name). However, unlike anonymity, the use of a pseudonym does not necessarily mean that a consumer cannot be identified. The consumer may choose to divulge their identity, or to provide the CDR data necessary to identify them, such as an address.

Providing anonymous and pseudonymous options

2.13 An accredited person (who is or who may become an accredited data recipient of the consumer's CDR data) must provide each consumer with the option of using a pseudonym, or not identifying themselves, when dealing with the accredited person in relation to that data.

2.14 Examples of 'dealings' include:

- asking for the consumer's consent to collect, use and/or disclose their CDR data
- providing a consumer with a consumer dashboard
- communicating with the consumer (for example, when providing a CDR receipt to the consumer[11] or notifying of collection under Privacy Safeguard 5)[12]
- 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.[13]

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

Exceptions

Requiring identification — required or authorised by law

2.15 ~~CDR Rule~~Paragraph 7.3(1)(a) of the CDR Rules provides that an accredited person who is or may become 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'.[14]

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

[11] See Chapter C (Consent).

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

[13] See Chapter C (Consent).

[14] The exception in ~~CDR Rule~~paragraph 7.3(~~a~~)1)(a) in the CDR Rules does not apply to an accredited person who is not yet an accredited data recipient of CDR data.

2.17 If an accredited data recipient is 'required' by a law or order to deal only with an identified consumer, it will be necessary for the consumer to provide adequate identification.

2.18 If an entity is 'authorised' by a law or order to deal with an identified consumer, the entity can require the consumer to identify themselves, but equally will have discretion to allow the consumer to deal with the entity anonymously or pseudonymously. The nature of any discretion, and whether it is appropriate to rely upon it, will depend on the terms of the law or order and the nature of the dealing.[15]

2.19 The following are examples of where a law or order may require or authorise an accredited data recipient to deal only with an identified consumer:

- discussing or accessing ~~the consumer's banking details with the~~certain consumer~~, such as~~ information (e.g. bank account information~~,~~), or
- opening ~~a bank account~~certain accounts for a consumer, or providing other ~~financial~~ services where legislation requires the consumer to be identified.

Requiring identification — impracticability

2.20 ~~CDR Rule~~Paragraph 7.3(1)(b) of the CDR Rules 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.[16]

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

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

- ~~providing an anonymous option is impracticable, as~~ the CDR data required to meet a consumer's request will almost certainly identify or reasonably identify the consumer (for example ~~bank~~ account, payment 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.

Example: 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.[17] This may be for a range of reasons,

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

[16] The exception in ~~CDR Rule~~paragraph 7.3(~~b~~)1)(b) of the CDR Rules does not apply to an accredited person who is not yet an accredited data recipient of CDR data.

[17] Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019, paragraph 1.322.

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.