Chapter 2:

Privacy Safeguard 2 —

Anonymity and pseudonymity

Version 3.0, June 2021

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 data, unless an exception applies.

What does Privacy Safeguard 2 say?

2.1 Privacy Safeguard 2 provides that a consumer must have the option of not identifying themselves, or of using a pseudonym, when dealing with an accredited person (who is or who may become an accredited data recipient of the consumer's CDR data) in relation to that data.

2.2 'Anonymity' and 'pseudonymity' are different concepts. Privacy Safeguard 2 requires that both options be made available to consumers dealing with an accredited person unless an exception applies. The exceptions are set out in consumer data rule (CDR Rule) 7.3.

2.3 Consumer data rule (CDR Rule) 7.3 sets out that an accredited data recipient of a consumer's CDR data does not need to allow anonymity or pseudonymity where:[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 is required or authorised by or under a law, or a court/tribunal order, to deal with an identified consumer in relation to particular CDR data.

Who does Privacy Safeguard 2 apply to?

2.4 Privacy Safeguard 2 applies to accredited persons who are or who may become accredited data recipients of a consumer's CDR data.

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

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

How Privacy Safeguard 2 interacts with the Privacy Act

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

[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.

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

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

CDR entity	Privacy protections that apply in the CDR context
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.[3]
Accredited data recipient[4]	**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 data. APP 2 does not apply to the accredited data recipient in relation to that CDR data.[5]
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 paragraph 2.14 below.*

[3] See ss 56EC(4) and 56EE(1)(b) of the Competition and Consumer Act.

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

[4] 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.

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

Why anonymity and pseudonymity are important

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

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

What is the difference between anonymity and pseudonymity?

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

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

Providing anonymous and pseudonymous options

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

2.14 Examples of 'dealings' include:

- asking for the consumer's consent to collect, use and/or disclose their CDR data
- providing a consumer with a consumer dashboard

- communicating with the consumer (for example, when providing a CDR receipt to the consumer[6] or notifying of collection under Privacy Safeguard 5)[7]
- 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.[8]

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

Exceptions

Requiring identification — required or authorised by law

2.15 CDR Rule 7.3(a) provides that an accredited data recipient is not required to offer a consumer the option of dealing anonymously or pseudonymously if the recipient 'is required or authorised by law or by a court/tribunal order to deal with an identified consumer in relation to particular CDR data'.[9]

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

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

2.18 If an entity is 'authorised' by a law or order to deal with an identified consumer, the entity can require the consumer to identify themselves, but equally will have discretion to allow the consumer to deal with the entity anonymously or pseudonymously. The nature of any discretion, and whether it is appropriate to rely upon it, will depend on the terms of the law or order and the nature of the dealing.[10]

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

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

[6] See Chapter C (Consent).

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

[8] See Chapter C (Consent).

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

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

Requiring identification — impracticability

2.20 CDR Rule 7.3(b) provides that a consumer may not have the option of dealing anonymously or pseudonymously with an accredited data recipient if it is impracticable to deal with a consumer who has not identified themselves.[11]

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

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

- providing an anonymous option is impracticable, as the CDR data required to meet a consumer's request will almost certainly identify or reasonably identify the consumer (for example bank account or transaction details in the banking sector)
- the burden of the inconvenience, time and cost of dealing with an unidentified or pseudonymous consumer, or
- changing internal systems or practices to include the option of anonymous or pseudonymous dealings, would be excessive in all the circumstances.

Anonymity and pseudonymity in the banking sector

Generally, an accredited data recipient in the banking sector may not be able to deal with a consumer on an anonymous or pseudonymous basis.[12] 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.

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

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