Chapter 2:

Privacy Safeguard 2 —

Anonymity and pseudonymity

Consultation draft, October 2019

OAIC

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 Consumer Data 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 CDR consumer in relation to particular CDR data.

2.3 '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 one of the two exceptions applies.

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.

How Privacy Safeguard 2 interacts with the Privacy Act

2.5 It is important to understand how Privacy Safeguard 2 interacts with the Privacy Act and the Australian Privacy Principles (APPs).[1]

2.6 Like Privacy Safeguard 2, 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.

Summary of application of Privacy Safeguard 2 by CDR participant

CDR Entity	Privacy principle that applies to CDR data
Accredited person	**Australian Privacy Principle 2 (and, in practice, Privacy Safeguard 2)** Privacy Safeguard 2 does not apply to an accredited person. Notwithstanding, an accredited person should adhere to Privacy Safeguard 2 by providing the consumer with the option of not identifying themselves, or of using a pseudonym, when asking the consumer to provide their consent to collect and use CDR data. This is because an accredited person will become an accredited data recipient for a CDR consumer's CDR data upon collecting such CDR data.
Accredited data recipient	**Privacy Safeguard 2** Privacy Safeguard 2 applies instead of APP 2, meaning APP 2 will not apply to CDR data that has been received by an accredited data recipient through the CDR regime. APP 2 will continue to apply to any personal information handled by the accredited data recipient that is not CDR data.[2] This is because all accredited data recipients are subject to the Privacy Act and the APPs for any personal information, even if it is not CDR data.
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.

Why anonymity and pseudonymity are important

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

2.8 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] See s 6E(1D) of the Privacy Act.

What is the difference between anonymity and pseudonymity?

2.9 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 consents 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.

2.10 Pseudonymity means that a CDR 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

2.11 An accredited data recipient must provide a CDR consumer with the option of 'dealing' anonymously or pseudonymously with the entity, unless an exception applies.

2.12 The time of dealing is when an accredited data recipient asks for the consumer's consent to collect and use their CDR data.[3] Examples of 'dealing' with a consumer include:

- asking for the consumer's consent to collect and use their CDR data[4]
- communicating with the consumer (for example, when providing a CDR receipt to the consumer or ongoing notifications).[5]

2.13 The data standards provide that:

- identifying information will not be conveyed to the accredited data recipient 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 data recipient.

[3] See Chapter C: Key Concepts (Consent) and 'Valid Request' in Chapter 3 (Privacy Safeguard 3).

[4] See Chapter C: Key Concepts (Consent) and 'Valid Request' in Chapter 3 (Privacy Safeguard 3).

[5] See Consumer Data Rules 4.18 and 4.20.

Anonymity and pseudonymity in the banking sector

Generally, an accredited data recipient in the banking sector is not able to deal with a consumer on an anonymous basis. This is because:

- there may be obligations under law to verify the identity of the customer prior to providing goods or services and/or
- it is impracticable for a consumer to remain anonymous, given CDR data in the banking industry is highly granular and will likely reveal something which could identify them.

Exceptions

Requiring identification — required or authorised by law

2.14 Consumer Data Rule 7.3 provides that an accredited data recipient is not required to offer CDR consumers 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 CDR consumer in relation to particular CDR data'.

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

2.16 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.

2.17 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.[6]

2.18 The following are given as 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
- supplying a pre-paid mobile phone to a consumer where legislation requires identification.

Requiring identification — impracticability

2.19 Consumer Data Rule 7.3 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 CDR consumer who has not identified themselves.

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

2.20 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.

2.21 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
- changing internal systems or practices to include the option of anonymous or pseudonymous dealings, would be excessive in all the circumstances.