

Chapter 9:

# Privacy Safeguard 9 —

## Adoption or disclosure of government related identifiers by accredited data recipients

Consultation draft, October 2019

# Contents

<b>Key points</b>	<b>3</b>
<b>What does Privacy Safeguard 9 say?</b>	<b>3</b>
<b>Why is it important?</b>	<b>3</b>
<b>Who does Privacy Safeguard 9 apply to?</b>	<b>3</b>
<b>How Privacy Safeguard 9 interacts with the Privacy Act</b>	<b>4</b>
Summary of application of Privacy Safeguard 9 by CDR entity	4
<b>Meaning of government related identifier</b>	<b>4</b>
‘Identifiers’	5
‘Government related identifier’	5
<b>Adopting, using or disclosing a government related identifier</b>	<b>6</b>
‘Adopt’	6
‘Use’	6
‘Disclose’	7
Exceptions	7
<b>Interaction with other Privacy Safeguards</b>	<b>8</b>
Privacy Safeguard 4	8

## Key points

- Privacy Safeguard 9 sets out a prohibition on accredited data recipients adopting, using or disclosing government related identifiers unless required or authorised:
  - under another Australian law or
  - as prescribed by regulations made under the Privacy Act.
- A government related identifier is a number, letter or symbol, or a combination of any or all of those things, that has been assigned by certain government entities and is used to identify the individual or to verify the identity of the individual.
- An individual cannot consent to the adoption, use or disclosure of their government related identifier.

## What does Privacy Safeguard 9 say?

- 9.1 Privacy Safeguard 9 prohibits an accredited data recipient that has collected CDR data which includes a government related identifier of a CDR consumer for the CDR data, from:
- adopting the government related identifier as its own identifier of the CDR consumer, or otherwise using the government related identifier, or
  - disclosing CDR data which includes the government related identifier
- unless authorised or required by or under:
- an Australian law other than the Consumer Data Rules, or
  - Australian Privacy Principle (APP) 9.3, which allows an entity to adopt, use or disclose a government related identifier of an individual as prescribed by regulations.
- 9.2 Privacy Safeguard 9 only concerns government related identifiers of individuals.
- 9.3 In this Chapter, a government related identifier of a CDR consumer included with the CDR consumer's CDR data is referred to as a 'CDR consumer government related identifier'.

## Why is it important?

- 9.4 The objective of Privacy Safeguard 9 is to restrict use of government related identifiers so that they do not become universal identifiers, which could jeopardise privacy by enabling CDR data from different sources to be matched and linked in ways that a CDR consumer may not agree with or expect.

## Who does Privacy Safeguard 9 apply to?

- 9.5 Privacy Safeguard 9 applies to accredited data recipients. It does not apply to data holders or designated gateways.

# How Privacy Safeguard 9 interacts with the Privacy Act

- 9.6 It is important to understand how Privacy Safeguard 9 interacts with the *Privacy Act 1988* (Privacy Act) and the APPs.<sup>1</sup>
- 9.7 Like Privacy Safeguard 9, APP 9 prohibits an APP entity from adopting, using or disclosing a government related identifier unless an exception applies.

## Summary of application of Privacy Safeguard 9 by CDR entity

CDR entity	Privacy principle that applies to CDR data
<b>Accredited data recipient</b>	<p><b>Privacy Safeguard 9</b></p> <p>Privacy Safeguard 9 applies instead of APP 9,<sup>2</sup> meaning APP 9 will not apply to government related identifiers adopted, used or disclosed under the CDR regime.</p> <p>All accredited data recipients are subject to the Privacy Act and the APPs for their handling of personal information that is not CDR data. 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.<sup>3</sup></p> <p>APP 9 will continue to apply to any government related identifier of an individual where collected in the entity’s capacity as an APP entity.</p>
<b>Designated gateway</b>	<p><b>Australian Privacy Principle 9</b></p> <p>Privacy Safeguard 9 does not apply to a designated gateway.</p>
<b>Data holder</b>	<p><b>Australian Privacy Principle 9</b></p> <p>Privacy Safeguard 9 does not apply to a data holder.</p>

## Meaning of government related identifier

- 9.8 ‘Government related identifier’ has the meaning given to it in the Privacy Act<sup>4</sup>.
- 9.9 Privacy Safeguard 9 only concerns government related identifiers of individuals.
- 9.10 This only applies to CDR consumers who are natural persons (including individuals, sole trader or the partner of a partnership but not to corporations). For example, the Australian

<sup>1</sup> The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies.

<sup>2</sup> 56EC(4)(a). Section 56EC(4) provides that the APPs do not apply to an accredited data recipient of CDR data in relation to the CDR data. An accredited person who holds CDR data that was disclosed to the person under the Consumer Data Rules falls within the definition of ‘accredited data recipient’ for that data (unless they are a data holder or designated gateway for the data) (see s 56AK).

<sup>3</sup> See s 6E(1D) of the Privacy Act.

<sup>4</sup> 56EL(1)(b); 56EL(2)(b).

Business Number (ABN) of a body corporate would not be subject to Privacy Safeguard 9 (and note that the ABN of an individual is not an ‘identifier’ under s 6(1) of the Privacy Act).

## ‘Identifiers’

9.11 An ‘identifier’ of an individual is defined in subsection 6(1) of the Privacy Act as a number, letter or symbol, or a combination of any or all of those things, that is used to identify the individual or to verify the identity of the individual.

9.12 The following are explicitly excluded from the definition of identifier:

- an individual’s name,
- an individual’s ABN
- anything else prescribed by the regulations made under the Privacy Act.<sup>5</sup> This provides flexibility to exclude any specified type of identifier from the definition, and therefore the operation of both Privacy Safeguard 9 and APP 9, as required.

## ‘Government related identifier’

9.13 A ‘government related identifier’ of an individual is defined in subsection 6(1) of the Privacy Act as an identifier that has been assigned by:

- an agency<sup>6</sup>
- a State or Territory authority<sup>7</sup>
- an agent of an agency, or a State or Territory authority, acting in its capacity as agent, or
- a contracted service provider for a Commonwealth contract,<sup>8</sup> or a State contract,<sup>9</sup> acting in its capacity as contracted service provider for that contract.

9.14 The following are examples of government related identifiers:

- Medicare numbers,
- Centrelink Reference numbers,
- driver licence numbers issued by State and Territory authorities and
- Australian passport numbers.

---

<sup>5</sup> See the Federal Register of Legislation <<https://www.legislation.gov.au>> for up-to-date versions of the regulations made under the Privacy Act.

<sup>6</sup> ‘Agency’ is defined in s 6(1) of the Privacy Act.

<sup>7</sup> ‘State or Territory authority’ is defined in s 6C(3) of the Privacy Act.

<sup>8</sup> ‘Commonwealth contract’ is defined in s 6(1) of the Privacy Act to mean a contract, to which the Commonwealth or an agency is or was a party, under which services are to be, or were to be, provided to an agency.

<sup>9</sup> ‘State contract’ is defined in s 6(1) of the Privacy Act to mean a contract, to which a State or Territory or State or Territory authority is or was a party, under which services are to be, or were to be, provided to a State or Territory authority.

9.15 Some government related identifiers are regulated by other laws that restrict the way that entities can collect, use or disclose the particular identifier and related personal information. Examples include tax file numbers and individual healthcare identifiers.<sup>10</sup>

## Adopting, using or disclosing a government related identifier

9.16 An accredited data recipient must not adopt a CDR consumer government related identifier as its own identifier of the CDR consumer, or otherwise use a government related identifier, unless an exception applies.<sup>11</sup> In addition, an accredited data recipient must not include the government related identifier when it discloses CDR data unless an exception applies.

### ‘Adopt’

9.17 The term ‘adopt’ is not defined in the Competition and Consumer Act and so it is appropriate to refer to its ordinary meaning.

9.18 An accredited data recipient ‘adopts’ a CDR consumer government related identifier if it collects CDR data that includes a government related identifier of the CDR consumer and organises the CDR data that it holds about that individual with reference to that identifier.

#### Example

Saul, an accountant and accredited data recipient, receives a CDR consumer’s driver licence number when it is disclosed to Saul in response to a consumer data request. Saul then uses the identifier to refer to that consumer in his own identification system.

Saul has adopted a CDR consumer government related identifier in breach of Privacy Safeguard 9.

### ‘Use’

9.19 The term ‘use’ is discussed in Chapter B (Key Concepts).

9.20 Examples of when an accredited data recipient will ‘use’ a CDR consumer government identifier include where the entity refers to a consumer by that identifier, organises records

<sup>10</sup> For more information about the legislative regimes, visit the OAIC’s Tax File Numbers page and Healthcare Identifiers page <<https://www.oaic.gov.au>>.

<sup>11</sup> 56EL(1). Note: The principal difference between Privacy Safeguard 9 and APP 9 is that the exceptions to the prohibition on using or disclosing government related identifiers in Privacy Safeguard 9 are much narrower than in APP 9. Only the exceptions under APP 9.1 for adopting, and APP 9.2(c) and (f) for using or disclosing, a government related identifier are carried across to Privacy Safeguard 9:

- The common exceptions between Privacy Safeguard 9 and APP 9 are where the adoption, use or disclosure of the government related identifier is authorised or required by an Australian law or court/tribunal order, or where regulations under APP 9.3 prescribe the adoption, use or disclosure.
- The exceptions in APP 9.2 for using or disclosing government related identifiers for verification purposes, fulfilling obligations to agencies or State or Territory authorities, for ‘permitted general situations’ or for enforcement related activities of enforcement bodies do not apply to Privacy Safeguard 9.

and documents pertaining to that consumer by reference to that identifier, or otherwise attributes that identifier to the CDR data of the consumer for reference purposes.

## ‘Disclose’

- 9.21 The term ‘disclose’ is discussed in Chapter B (Key Concepts)
- 9.22 An accredited data recipient or designated gateway ‘discloses’ CDR data where it makes it accessible to others outside the entity and releases the subsequent handling of the information from its effective control.

## Exceptions

### Required or authorised by or under an Australian law or court/tribunal order

- 9.23 An accredited data recipient may use a CDR consumer government related identifier, adopt it as its own identifier or include it when disclosing CDR data if this is required or authorised by or under an Australian law or a court/tribunal order.<sup>12</sup>
- 9.24 The meaning of ‘required or authorised by or under an Australian law or a court/tribunal order’ is discussed in Chapter B (Key concepts).
- 9.25 The Australian law or court/tribunal order should specify:
- a particular government related identifier
  - the entities or classes of entities permitted to adopt, use or disclose it,
  - the particular circumstances in which they may adopt, use or disclose it.

### Prescribed by regulations

- 9.26 An accredited data recipient may use a CDR consumer government related identifier, adopt it as its own identifier of the consumer, or include it when disclosing CDR data if:
- the identifier is prescribed by regulations,
  - the entity is an organisation, or belongs to a class of organisations, prescribed by regulations, and
  - the adoption or use occurs in the circumstances prescribed by the regulations.<sup>13</sup>
- 9.27 Regulations may be made under the Privacy Act to prescribe these matters.<sup>14</sup>

#### Example

Accredited data recipient, Data Dump Pty Ltd, uses a third party service provider, Bale. Ian, a CDR consumer, authorises a data holder of his CDR data to disclose his CDR data to Data Dump. The data holder discloses Ian’s passport number with the data.

<sup>12</sup> 56EL(1)(c).

<sup>13</sup> 56EL(1)(d) and APP 9.3.

<sup>14</sup> See the Federal Register of Legislation <<https://www.legislation.gov.au>> for up-to-date versions of regulations made under the Privacy Act.

Data Dump discloses CDR data collected from the data holder of Ian's CDR data to Bale pursuant to Consumer Data Rule 7.5(1)(d). Bale then uses the CDR data to provide data analytics services. Data Dump's systems are set up so that all CDR data collected is sent over a secure link to Bale, where the data is then within Bale's control.

When Ian's passport number is sent to Bale along with Ian's other CDR data, Data Dump has included the government related identifier in a disclosure in breach of Privacy Safeguard 9.

**Risk point:** An accredited data recipient may unknowingly use a CDR consumer government related identifier if there are not processes in place to prevent this.

**Privacy tip:** Accredited data recipient may frame consumer data requests made to data holders to specifically exclude any government related identifiers to reduce the risk that such identifiers will be included in the disclosure.

## Interaction with other Privacy Safeguards

### Privacy Safeguard 4

- 9.28 Privacy Safeguard 9 does not specifically address the collection of government related identifiers. However, if an accredited data recipient collects a government related identifier that is considered to be CDR data, the accredited data recipient must comply with other Privacy Safeguards, including Privacy Safeguard 3 and Privacy Safeguard 4. These Privacy Safeguards are discussed in Chapters 3 and 4 respectively.