Chapter 8:

Privacy Safeguard 8 —

Overseas disclosure of CDR data by accredited data recipients

Version 2.0, July 2020

OAIC

Contents

Key points

- Privacy Safeguard 8 sets out the circumstances in which an accredited data recipient can disclose consumer data right (CDR) data to a recipient located overseas.
- Under Privacy Safeguard 8, an accredited data recipient must not disclose CDR data to a recipient located overseas unless one of the following exceptions applies:
  - the overseas recipient is also an accredited person
  - the accredited data recipient takes reasonable steps to ensure the overseas recipient will not breach the privacy safeguards (noting that, for this exception, the accredited data recipient remains accountable for any breach of the privacy safeguards by the overseas recipient), or
  - the accredited data recipient reasonably believes the overseas recipient is subject to a law equivalent to the privacy safeguards and there are mechanisms available to the consumer to enforce that protection.
- These requirements are in addition to the other disclosure restrictions set out in Privacy Safeguards 6, 7 and 9 and the consumer data rules (CDR rules).

What does Privacy Safeguard 8 say?

8.1 In addition to the disclosure restrictions set out in Privacy Safeguards 6, 7 and 9, an accredited data recipient must not disclose CDR data to a person located overseas unless one of the following four exceptions applies:

a. the overseas recipient is an accredited person

b. the accredited data recipient takes reasonable steps to ensure the overseas recipient does not breach the privacy safeguards[1] and the overseas recipient has a CDR policy in place in relation to the CDR data

c. the accredited data recipient reasonably believes the overseas recipient is bound by a law or scheme that is substantially similar to the privacy safeguards and a consumer will be able to enforce that law or scheme in relation to the CDR data, or

d. conditions specified in the CDR Rules for overseas disclosure are met. As there are currently no CDR Rules made specifically in relation to Privacy Safeguard 8, an accredited data recipient cannot rely on this exception.

8.2 Where the overseas recipient is not accredited or subject to a similar law or binding scheme to the privacy safeguards, even if an accredited data recipient takes reasonable steps to ensure the overseas recipient does not breach the privacy safeguards, but the overseas recipient nevertheless breaches a relevant privacy safeguard, the accredited data recipient remains accountable for that breach.

[1] The relevant privacy safeguards are the privacy safeguard penalty provisions as defined in s 56EU of the Competition and Consumer Act (Privacy Safeguards 3–13 inclusive, and the requirement to have a CDR policy in Privacy Safeguard 1).

8.3 For the purposes of a CDR outsourcing arrangement, an accredited data recipient must also comply with the CDR Rules that relate to CDR outsourcing arrangements.[2]

Why is this important?

8.4 As an overarching objective of the CDR framework, consumers should be able to trust that an accredited data recipient will manage CDR data appropriately and in compliance with the privacy safeguards, especially when it is disclosed overseas.

8.5 It is also important that entities are aware of and understand the obligations on them to protect CDR data where they seek to make a disclosure of CDR data to an overseas recipient.

Who does Privacy Safeguard 8 apply to?

8.6 Privacy Safeguard 8 applies to accredited data recipients.

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

8.8 Data holders and designated gateways should ensure that they adhere to their obligations under the *Privacy Act 1988* (Privacy Act) and the Australian Privacy Principles (APPs), including APP 8, when disclosing personal information to an overseas recipient.

How does Privacy Safeguard 8 interact with the Privacy Act and the APPs?

8.9 It is important to understand how Privacy Safeguard 8 interacts with the Privacy Act and the APPs.[3]

8.10 APP 8 outlines when an APP entity may disclose personal information about an individual to an overseas recipient (see Chapter 8 of the APP Guidelines: APP 8 — Cross-border disclosure of personal information).

CDR entity	Privacy protections that apply in the CDR context
Accredited person / accredited data recipient	**Privacy Safeguard 8** Privacy Safeguard 8 applies instead of APP 8 to the overseas disclosure of CDR data where the CDR data has been collected by an accredited data recipient under the CDR regime. APP 8 will continue to apply to overseas disclosures of personal information by an accredited person or accredited data recipient where the data is not CDR data.[4]

[2] CDR Rules 1.10, 1.16, 7.5(1)(d) and 7.6. For more information on CDR outsourcing arrangement, please refer to Chapter B (Key concepts).

[3] The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies (APP entities).

[4] All accredited persons are subject to the Privacy Act and the APPs in relation to information that is personal information but is not CDR data. See s 6E(1D) of the Privacy Act.

CDR entity	Privacy protections that apply in the CDR context
Designated gateway	**APP 8** Privacy Safeguard 8 does not apply to a designated gateway.
Data holder	**APP 8** Privacy Safeguard 8 does not apply to a data holder.

Meaning of disclosure

8.11 The term 'disclose' is not defined in the Competition and Consumer Act. It is discussed in Chapter B (Key concepts).

8.12 An accredited data recipient discloses CDR data when it makes it accessible or visible to others outside the entity.[5]

8.13 The release of the information may be a release in accordance with the CDR Rules, an accidental release or an unauthorised release.

8.14 This focuses on the act done by the disclosing party. The state of mind or intentions of the recipient does not affect the fact of disclosure. Further, there will be a disclosure even where the information is already known to the overseas recipient.

What is an overseas recipient?

8.15 Under Privacy Safeguard 8, an overseas recipient is a person,[6] who receives CDR data from an accredited data recipient, who is not:

- in Australia or in an external Territory and
- a consumer for the CDR data.

When can CDR data be disclosed to an overseas recipient?

8.16 When making an overseas disclosure of CDR data, an accredited data recipient must comply with Privacy Safeguard 8 in addition to each of the other privacy safeguards and consumer data rules that relate to disclosure of CDR data (to the extent they are applicable to the relevant disclosure).[7]

---

[5] Any provision of CDR data to an outsourced service provider located overseas is a disclosure. This is different to the arrangements under the Privacy Act, where in limited circumstances providing personal information to an overseas contractor to perform services on behalf of an APP entity may be a use, rather than a disclosure of information. Whether an accredited data recipient retains effective control over the data does not affect whether data is 'disclosed'. See paragraph 8.14 in Chapter 8 of the APP Guidelines: APP 8 — Cross-border disclosure of personal information, for more information.

[6] Being a body corporate, body politic or individual.

[7] Privacy Safeguard 6 and the CDR Rules relating to permitted uses and disclosures (CDR Rules 7.5 and 7.6), Privacy Safeguard 7 and the CDR Rules relating to disclosure of CDR data for direct marketing (CDR Rules 7.8 and 7.5(3)), Privacy Safeguard 9 relating to disclosure of government related identifiers, and the CDR outsourcing arrangements (CDR Rules 7.5(1)(d) and 7.6).

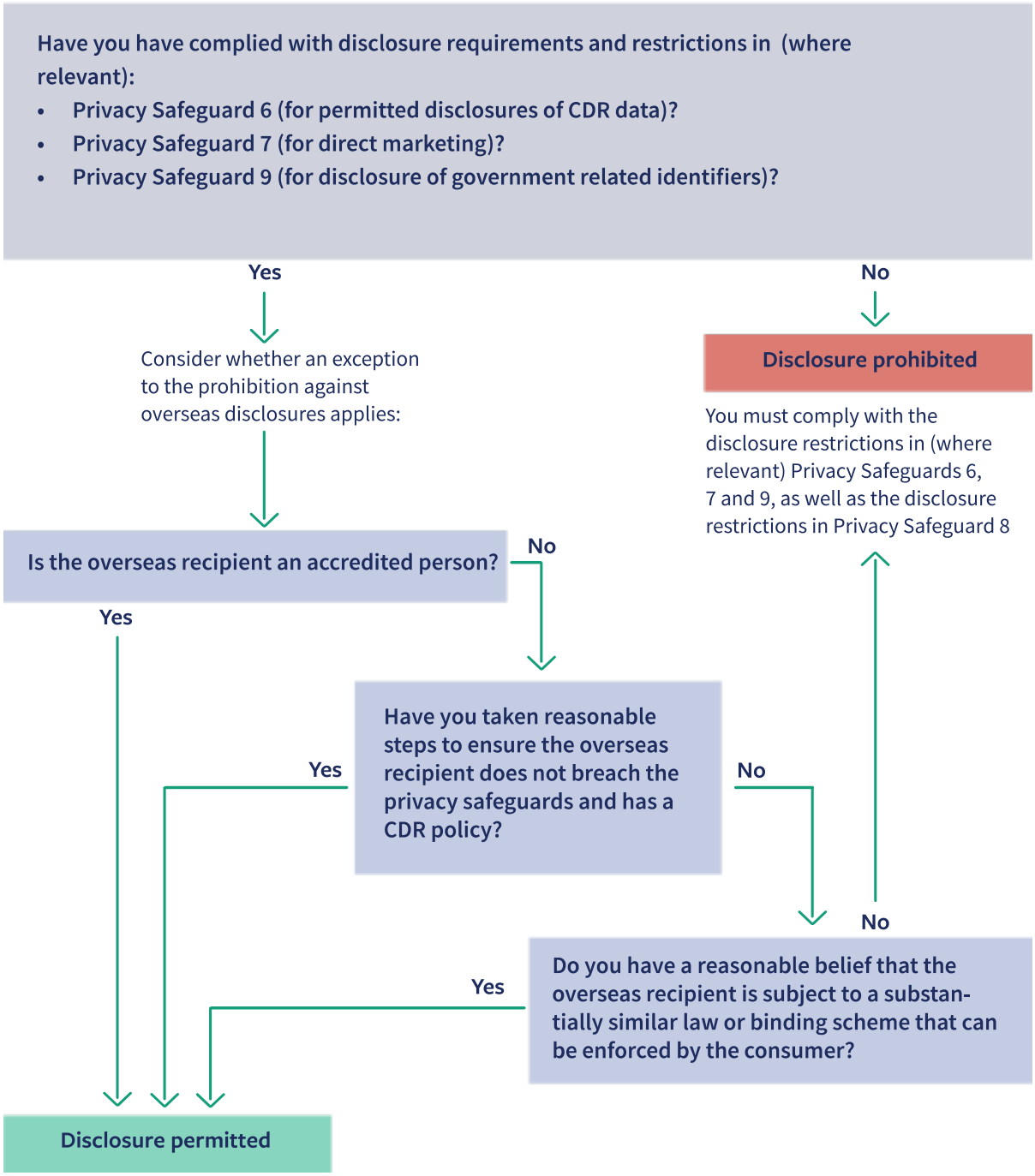
8.17 Privacy Safeguard 8 provides that an accredited data recipient must not disclose CDR data to a person located overseas unless one of the following four exceptions applies:

- the overseas recipient is an accredited person
- the accredited data recipient takes reasonable steps to ensure the overseas recipient does not breach the privacy safeguards[8] and that the overseas recipient has a CDR policy in place in relation to the CDR data
- the accredited data recipient reasonably believes the overseas recipient is bound by a law or scheme that is substantially similar to the privacy safeguards which can be enforced by the consumer, or
- conditions specified in the CDR Rules for overseas disclosure are met. As there are currently no CDR Rules made specifically in relation to Privacy Safeguard 8, an accredited data recipient cannot currently rely on this exception.

8.18 The flow chart following outlines at a high level when an accredited data recipient may disclose CDR data to an overseas recipient, including by demonstrating the point at which the entity must consider other relevant privacy safeguards and relevant exceptions under Privacy Safeguard 8.

[8] The relevant privacy safeguards are the privacy safeguard penalty provisions defined in s 56EU of the Competition and Consumer Act (Privacy Safeguards 3–13 inclusive, and the requirement to have a CDR policy in Privacy Safeguard 1).

When can an accredited data recipient disclose CDR data to an overseas recipient?



Exception 1 — Disclosing CDR data to an overseas recipient who is an accredited person

8.19 An accredited data recipient may disclose CDR data to an overseas recipient if the person is an accredited person.

8.20 The term 'accredited person' is discussed in Chapter B (Key concepts).

8.21 The CDR Rules require that an individual or company must apply to be an accredited person under the Competition and Consumer Act. Accredited persons will be added to the Register of Accredited Persons if their application is successful.

8.22 The CDR Rules and the ACCC's Accreditation Guidelines provide more information about the requirements and process for accreditation.

8.23 Accreditation is considered sufficient protection to ensure compliance with the privacy safeguards.[9]

Exception 2 — Disclosing CDR data after taking 'reasonable steps' to ensure an overseas recipient does not breach the privacy safeguards

8.24 An accredited data recipient may disclose CDR data to an overseas recipient if they take reasonable steps to ensure that any act or omission by (or on behalf of) the overseas recipient will not breach the privacy safeguards.

8.25 The privacy safeguards apply to the acts or omissions as though the overseas recipient (or those who acted on behalf of the overseas recipient) was the accredited data recipient who disclosed the CDR data.

8.26 Examples for persons acting on behalf of the overseas recipient could include employees, directors, officers, or subcontractors.

What are 'reasonable steps'?

8.27 Reasonable steps would generally involve, at a minimum, that an accredited data recipient enters into an enforceable contractual arrangement with the overseas recipient that requires the overseas recipient to handle the CDR data in accordance with:

- the privacy safeguards, and
- the CDR Rules that relate to CDR outsourcing arrangements.[10]

8.28 Whether an accredited data recipient has taken reasonable steps to ensure the overseas recipient can comply with the CDR regime may include consideration of the following factors:

- the terms of the contract between the accredited data recipient and the overseas recipient

[9] Explanatory Memorandum, *Treasury Laws Amendment (Consumer Data Right) Bill 2019*, section 1.348.

[10] CDR Rules 1.10, 1.16 7.5(1)(d) and 7.6. For more information on CDR outsourcing arrangement, please refer to Chapter B (Key concepts).

- steps taken by the accredited data recipient to monitor compliance with the contract
- the accredited data recipient's relationship with the overseas recipient. More rigorous steps may be required when an entity discloses CDR data to an overseas recipient for the first time
- the nature of the overseas recipient, including the maturity of its processes and systems, and familiarity with CDR legislation (which may be derived from previous engagements with other CDR entities)
- the possible adverse consequences for a consumer if the CDR data is mishandled by the overseas recipient. More rigorous steps may be required as the risk of adversity increases
- the nature of the CDR data being disclosed. Where CDR data is sensitive in nature (and could, for example, cause financial or physical harm to a consumer if mishandled), it should be subject to more rigorous protections in the contractual arrangements
- existing technical and operational protections implemented by the overseas recipient to protect the CDR data (where these are not equivalent to the security requirements set out in Privacy Safeguard 12 and in Schedule 2 of the CDR Rules), and
- the practicability of taking protective steps, including time and cost involved. However, a CDR entity is not excused from ensuring that an overseas recipient is compliant with CDR legislation by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take particular steps will depend on whether the burden is excessive in all the circumstances.

Example

YC Pty Ltd is an accredited person that provides banking services and products to customers. YC Pty Ltd seeks to engage a contractor located overseas, Analysed Data Services, in order to offer certain data analytics services to its customers using their payments transactions data.

YC Pty Ltd considers whether an exception under Privacy Safeguard 8 relating to overseas disclosures will apply.

Analysed Data Services is not an accredited person and is not subject to a law or scheme similar to that of the CDR regime.

Before disclosing CDR data to Analysed Data Services, YC Pty Ltd must therefore take reasonable steps to ensure Analysed Data Services complies with the privacy safeguards and has a CDR policy in place in relation to the CDR data.

YC Pty Ltd will remain accountable if Analysed Data Services mishandles the CDR data.

Exception 3 — Disclosing CDR data where overseas recipient is subject to a substantially similar law

8.29 An accredited data recipient may disclose CDR data to an overseas recipient if:

- they reasonably believe the overseas recipient is bound by a law or binding scheme that is substantially similar to the privacy safeguards, and
- this can be enforced by the consumer.

What is 'reasonable belief'?

8.30 To rely on this exception, an accredited data recipient must have a reasonable belief that an overseas recipient is subject to a law, or binding scheme that provides substantially similar protections to the privacy safeguards and that a consumer will be able to enforce the protections provided by that law or binding scheme.

8.31 An accredited data recipient must have a reasonable basis for the belief, which is an objective test and not merely a genuinely held subjective belief. It is the responsibility of the entity to be able to justify its reasonable belief.

What is a 'law or binding scheme'?

8.32 An overseas recipient may be subject to a law or binding scheme, where, for example, it is:

- bound by consumer data protection law that applies in the jurisdiction of the overseas recipient
- required to comply with another law that imposes comparable obligations to the CDR regime, or
- subject to an industry scheme or code that is enforceable, irrespective of whether the overseas recipient was obliged or volunteered to participate or subscribe to the scheme or code.

8.33 However, an overseas recipient may not be subject to a law or binding scheme where, for example:

- the overseas recipient is exempt from complying, or is authorised not to comply, with part, or all, of the consumer data protection law in the jurisdiction, or
- the overseas recipient can opt out of the binding scheme without notice and without returning or destroying the data.

What is meant by 'substantially similar'?

8.34 A substantially similar law or binding scheme would provide a comparable, or a higher level of privacy protection to that provided by the privacy safeguards. Each provision of the law or scheme is not required to correspond directly to an equivalent privacy safeguard. Rather, the overall effect of the law or scheme is of central importance.

8.35 Whether there is substantial similarity is a question of fact. Factors that may indicate that the overall effect is substantially similar, include:

- the law or scheme regulates the collection of consumer data in a comparable way
- the law or scheme requires the recipient to notify individuals about the collection of their consumer data
- the law or scheme requires the recipient to only use or disclose the consumer data for authorised purposes
- the law or scheme includes comparable data quality and data security standards, and
- the law or scheme includes a right to access and seek correction of consumer data

When can a consumer enforce the protections?

8.36 A consumer will be able to enforce the protections when it has access to a mechanism to allow for the enforcement of a law or binding scheme that is substantially similar to the CDR regime.

8.37 A range of mechanisms may satisfy those requirements, ranging from a regulatory body similar to the Office of the Australian Information Commissioner (the OAIC), to an accredited dispute resolution scheme, an independent tribunal, or a court with judicial functions and powers.

8.38 Factors that may be relevant in deciding whether the enforcement mechanism is an accessible and effective include whether the mechanism:

- is independent of the overseas recipient that is required by the law or binding scheme to comply with the consumer data protections
- is a body with authority to consider a breach of any of the consumer data protections in the law or binding scheme
- is accessible to an individual, for example, the existence of the scheme is publicly known, and can be accessed by individuals directly and without payment of any unreasonable charge
- has the power to make a finding that the overseas recipient is in breach of the law or binding scheme and to provide a remedy to the individual, and
- is required to operate according to principles of procedural fairness.

When is an accredited data recipient accountable for the breaches by an overseas recipient?

8.39 Privacy Safeguard 8 provides that an accredited data recipient is accountable for the acts or omissions of an overseas recipient where it discloses CDR data to an overseas recipient and:

- the overseas recipient is not an accredited person
- the accredited data recipient does not reasonably believe that the overseas recipient is bound by a law or scheme that is similar to the CDR regime and that a consumer will be able to enforce protections provided by that law or scheme, or
- the overseas recipient (or a person acting on behalf of the overseas recipient) breaches the privacy safeguards[11] and/or does not have a CDR policy.[12]

8.40 In these circumstances, for the purposes of Privacy Safeguard 8, the act or omission is taken to have been done by the accredited data recipient. The accredited data recipient is taken to have breached the privacy safeguards.

[11] The relevant privacy safeguards are those privacy safeguard penalty provisions in defined in s 56EU (privacy safeguards 3–13 inclusive, and the requirement to have a CDR policy in Privacy Safeguard 1).

[12] Section 56EK(2) of the Competition and Consumer Act.

8.41 Where an accredited data recipient takes reasonable steps to ensure the overseas recipient complies with the privacy safeguards, but the overseas recipient nevertheless breaches a relevant privacy safeguard, the accredited data recipient is accountable for that breach.[13]

Risk point: An accredited data recipient will be accountable under the CDR regime for the acts and omissions of an overseas recipient under Privacy Safeguard 8 in the circumstances set out above at 8.39 - 8.41.

Privacy tip: Accredited data recipients should maintain strong governance mechanisms, policies and procedures in relation to overseas disclosures of CDR data, including outsourcing arrangements. An accredited person should ensure that all contracts that aim to ensure compliance with the 'reasonable steps' exception in Privacy Safeguard 8 contain enforceable provisions that extend to the acts or omissions of subcontractors. Disclosing CDR data to overseas participants who are either accredited persons or a bound by a similar law to the CDR regime will reduce the risk profile for an accredited data recipient.

8.42 There are also other conditions in the CDR Rules that affect when an accredited data recipient is liable when making an overseas disclosure. Importantly, CDR Rule 7.6(2) provides that the accredited data recipient will be liable for the acts or omissions of an outsourced service provider (or its subcontractors).

How does Privacy Safeguard 8 interact with the other privacy safeguards?

Privacy Safeguard 6

8.43 In addition to Privacy Safeguard 8, an accredited data recipient should consider Privacy Safeguard 6 when determining whether to disclose CDR data to an overseas recipient.

8.44 This includes whether the disclosure is a permitted disclosure for the purposes of Privacy Safeguard 6 and also whether the accredited data recipient will need to comply with CDR outsourcing arrangements relating to outsourced service providers. See Chapter 6 (Privacy Safeguard 6).

Privacy Safeguard 7

8.45 In addition to Privacy Safeguard 8, an accredited data recipient should consider Privacy Safeguard 7 where they are seeking to disclose CDR data to engage in permitted direct marketing activities. See Chapter 7 (Privacy Safeguard 7).

Privacy Safeguard 9

8.46 In addition to Privacy Safeguard 8, an accredited data recipient should also consider Privacy Safeguard 9 where CDR data it is seeking to disclose to an overseas recipient contains government identifiers. See Chapter 9 (Privacy Safeguard 9).

[13] Please note the similar liability position under CDR Rule 7.6 relating to outsource service providers where the use or disclosure of CDR data by the outsource service provider (or by one of its subcontractors) is taken to be use or disclosure of the accredited data recipient whether or not in accordance with the CDR outsourcing arrangement between the parties.