Chapter 8:

Privacy Safeguard 8 —

Overseas disclosure of CDR data by accredited data recipients

Consultation draft, October 2019

OAIC

Contents

Key points

- Privacy Safeguard 8 sets out the circumstances in which an accredited data recipient can disclose CDR data to a recipient located overseas.
- An accredited data recipient must not disclose CDR data to a recipient located overseas unless:
  - the overseas recipient is also an accredited person, or
  - the accredited data recipient takes reasonable steps to ensure the overseas recipient will not contravene the privacy safeguards (and the accredited data recipient remains liable for any contravention 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.

What does Privacy Safeguard 8 say?

8.1 An accredited data recipient must not disclose CDR data to a person located overseas unless:

a. the overseas recipient is an accredited person, or

b. the accredited data recipient takes reasonable steps to ensure the overseas recipient does not breach the Privacy Safeguards[1] and has a CDR policy in relation to the CDR data, or

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 CDR consumer will be able to enforce that law or scheme in relation to the CDR data, or

d. conditions specified in the Consumer Data Rules for overseas disclosure are met. There are currently no Consumer Data Rules in relation to Privacy Safeguard 8.

8.2 Where an accredited data recipient takes reasonable steps to ensure the overseas recipient does not breach the Privacy Safeguards (as described in condition 2 above), but the overseas recipient nevertheless contravenes a relevant privacy safeguard, the accredited data recipient is accountable for that contravention, notwithstanding the fact they complied with their Privacy Safeguard 8 obligations.

8.3 For the purposes of a CDR outsourcing arrangement, an accredited data recipient must comply with Privacy Safeguard 8 and the Consumer Data Rules that relate to CDR outsourcing arrangements (Rule 1.10, Rule 7.5(1)(d) and Rule 7.6).

Why is this important?

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

[1] The relevant Privacy Safeguards are the privacy safeguard penalty provisions in defined in s56EU (Privacy Safeguards 3 – 13 inclusive, and the requirement to have a CDR policy in Privacy Safeguard 1).

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 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. However, data holders and designated gateways should ensure that they adhere to their obligations under the Privacy Act 1988 and the 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?

8.8 It is important to understand how Privacy Safeguard 8 interacts with the Privacy Act 1988 (the Privacy Act) and Australian Privacy Principles (APPs).[2]

8.9 The Privacy Safeguards are assumed to apply to an overseas recipient where the overseas recipient's act or omission in relation to the CDR data would contravene the Privacy Safeguards.

Summary of application of Privacy Safeguard 8 by CDR participant

CDR Participant	Privacy principle that applies to CDR data
Accredited person	**Australian Privacy Principle 8** Privacy Safeguard 8 does not apply to an accredited person who is not an accredited data recipient of the relevant CDR data.
Accredited data recipient	**Privacy Safeguard 8** Privacy Safeguard 8 applies instead of APP 8,[3] meaning APP 8 will not apply to CDR data that has been received by an accredited data recipient through the CDR regime, and is being disclosed to a person located overseas. APP 8 will continue to apply to any personal information handled by the accredited data recipient 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.[4]

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

[3] 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).

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

CDR Participant	Privacy principle that applies to CDR data
Designated gateway	**Australian Privacy Principle 8** Privacy Safeguard 8 does not apply to a designated gateway.
Data holder	**Australian Privacy Principle 8** Privacy Safeguard 8 does not apply to a data holder.

When does an accredited data recipient 'disclose' CDR data to an overseas recipient?

8.10 The term 'disclose' is not defined in the CDR legislation. It is discussed in Chapter B (Key Concepts).

8.11 An accredited data recipient discloses CDR data when it makes it accessible to others outside the entity and releases the subsequent handling of the information from its effective control.

8.12 The release of the information may be a release in accordance with the Consumer Data Rules, or an accidental release or an unauthorised release.

8.13 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?

8.14 Under Privacy Safeguard 8, an overseas recipient is a person,[5] who receives CDR data from an accredited data recipient, who is not:

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

8.15 Where an accredited data recipient in Australia sends CDR data to an overseas office of the same entity, Privacy Safeguard 8 will not apply.

8.16 This is to be distinguished from the case where an accredited data recipient in Australia sends CDR data to a 'related body corporate' located outside of Australia. In that case, the related body corporate is a different entity to the accredited data recipient in Australia. It may therefore be an overseas recipient (assuming it does not meet the 'located in Australia or external Territory' requirement) and Privacy Safeguard 8 will apply.

8.17 The term 'CDR consumer' is discussed in Chapter B – Key Concepts.

[5] Including a body corporate with separate legal personality.

Conditions for disclosing CDR data to an overseas recipient

Disclosing CDR data to an overseas recipient who is an accredited person

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

8.19 The term 'accredited person' is discussed in Chapter B – Key Concepts.

8.20 The Consumer Data 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.

8.21 The Consumer Data Rules and the draft ACCC's Accreditation Guidelines provide more information about the requirements and process for accreditation.

8.22 Accreditation is considered sufficient protection to ensure compliance with the privacy safeguards.[6]

Disclosing CDR data after taking 'reasonable steps' to ensure an overseas recipient does not contravene the privacy safeguards

8.23 The requirement in Privacy Safeguard 8 to ensure that an overseas recipient does not breach the Privacy Safeguards is qualified by a 'reasonable steps' test.

What are 'reasonable steps'?

8.24 It is generally expected that an accredited data recipient will enter into an enforceable contractual arrangement with the overseas recipient that requires the recipient to handle the CDR data in accordance with the Privacy Safeguards.

8.25 Consideration of whether an accredited data recipient has taken reasonable steps to ensure the overseas recipient can comply with the CDR regime may include:

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

[6] Explanatory Memorandum, Treasure Laws Amendment (Consumer Data Right) Bill 2019, section 1.348.

- the possible adverse consequences for a CDR consumer if the CDR data is mishandled by the overseas recipient. More rigorous steps may be required as the risk of adversity increases
- existing technical and operational safeguards 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 Consumer Data Rules). More rigorous steps will be required where the recipient has limited existing safeguards in place
- the practicability, 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

'on behalf of'

8.26 Privacy Safeguard 8 contemplates management or handling of CDR data undertaken on behalf of an overseas recipient. This may include employees, directors, officers, consultants, or subcontractors of an overseas recipient.

8.27 The Privacy Safeguards apply to the acts or omissions of an overseas recipient (or an individual or entity acting on behalf of the overseas recipient) as though the overseas recipient was the accredited data recipient who disclosed the CDR data for the purposes of the obligations of an accredited data recipient under Privacy Safeguard 8.

Risk point: An accredited data recipient will be liable under CDR legislation for the acts and omissions of an overseas recipient (and the acts or omissions of the subcontractors of the overseas recipient), where an accredited data recipient relies on the "reasonable steps" exception in Privacy Safeguard 8.

Privacy tip: It is advisable that an accredited person ensures 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.

Example

KTelco Ltd outsources its customer contact centre services function to HelpsHere Pty Ltd, an Australian-based entity. HelpsHere Pty Ltd uses a subcontractor located overseas to ensure HelpsHere Pty Ltd can meet a service commitment to its customers.

KTelco Ltd and HelpsHere Pty Ltd have a contract capturing their CDR outsourcing arrangement, which is compliant with the Consumer Data Rules. Under this contract, HelpsHere Pty Ltd and its subcontractors must comply with the CDR regime.

The subcontractor breaches its contract with HelpsHere Pty Ltd by accidentally disclosing CDR data to a third party. Under the Privacy Safeguards, KTelco Ltd is liable for the breach by their subcontractor.

Disclosing CDR data with a 'reasonable belief' the overseas recipient is subject to a substantially similar law (and the consumer can enforce that law)

What is 'reasonable belief'?

8.28 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 CDR consumer will be able to enforce the protections provided by that law or binding scheme.

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

What is a 'law or binding scheme'?

8.30 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 scheme, 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.

8.31 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'?

8.32 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.

8.33 Whether there is substantial similarity is a question of fact.

8.34 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
- the law or scheme includes a right to access and seek correction of consumer data

When can a CDR consumer enforce the protections?

8.35 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.

8.36 An enforcement mechanism should meet two key requirements:

- it should be accessible to the individual, and
- it should have effective powers to enforce the consumer data protections in the law or binding scheme.

8.37 A range of mechanisms may satisfy those requirements, ranging from a regulatory body similar to the OAIC, to an accredited dispute resolution scheme, an independent tribunal or a court with judicial functions and powers. Factors that may be relevant in deciding whether there is an accessible and effective enforcement mechanism 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
- has 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
- is required to operate according to principles of procedural fairness.

8.38 The mechanism may be a single mechanism or a combination of mechanisms. It may be established by the law or binding scheme that contains the consumer data protections, or by another law or binding scheme. Alternatively, the mechanism may take effect through the operation of cross-border enforcement arrangements between the OAIC and an appropriate regulatory authority in the foreign jurisdiction.

Conditions specified in the Consumer Data Rules

8.39 Privacy Safeguard 8 permits an overseas disclosure where conditions specified in the Consumer Data Rules are met.

8.40 The Consumer Data Rules do not currently provide any conditions for overseas disclosure and therefore this basis for disclosure is not available.

When is an accredited person accountable for the acts or omission of an overseas recipient?

8.41 Privacy Safeguard 8 provides that an accredited person 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, and
- the accredited person 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 conditions in the Consumer Data Laws are not met, and
- the overseas recipient contravenes the privacy safeguards[7] and/or does not have a CDR policy.[8]

8.42 In these circumstances, the act or omission is taken to have been done by the accredited data recipient. The accredited data recipient it taken to have contravened the Privacy Safeguards.

8.43 Where an accredited data recipient takes reasonable steps to ensure the overseas recipient complies with the Privacy Safeguards, but the overseas recipient nevertheless contravenes a relevant Privacy Safeguard, the accredited data recipient is liable for that contravention (notwithstanding the fact it complied with its Privacy Safeguard 8 obligations).

8.44 As noted above, the conditions in the Consumer Data Rules relate to disclosures to outsourced service providers and stipulate the requirements that must be met by the accredited data recipient in doing so.

8.45 Importantly, Consumer Data Rule 7.6(2) provides that the accredited data recipient will be liable for the acts or omissions of the outsourced service provider (or its subcontractors), whether or not they were in accordance with the arrangement or not.

8.46 Therefore, it would be prudent for an accredited data recipient to consider maintaining policies in relation to the nature of the entities it engages under a CDR outsourcing arrangement. Those entities that:

- are accredited persons, or
- are located in jurisdictions in which they are bound by a law or scheme that is substantially similar to the CDR regime.

[7] The relevant Privacy Safeguards are the privacy safeguard penalty provisions in defined in s56EU (Privacy Safeguards 3 – 13 inclusive, and the requirement to have a CDR policy in Privacy Safeguard 1).

[8] 56EK(2).