Chapter 1:

Privacy Safeguard 1 —

Open and transparent management of CDR data

Version 4.0, November 2022

OAIC

Contents

Key points 3
What does Privacy Safeguard 1 say? 3
Importance of open and transparent management of CDR data and having a CDR policy 3
Who Privacy Safeguard 1 applies to 4
How Privacy Safeguard 1 interacts with the Privacy Act 5
Implementing practices, procedures and systems to ensure compliance with the CDR system 6
Circumstances that affect reasonable steps 7
Existing privacy governance arrangements 11
Have a CDR data management plan 11
A suggested approach to compliance with Privacy Safeguard 1 11
Having a CDR policy 15
Information that must be included in a CDR policy 16
Availability of the CDR policy 20
Consumer requests for a CDR policy 20
Interaction between an entity's privacy policy and CDR policy 20

Key points

- Privacy Safeguard 1,[1] together with consumer data rule (CDR Rule) 7.2 and the Competition and Consumer Regulations, outlines the requirements for all consumer data right (CDR) entities (accredited persons who are or who may become an accredited data recipient of CDR data, data holders, and designated gateways) to manage CDR data in an open and transparent way.
- All CDR entities must take steps as are reasonable in the circumstances to implement practices, procedures and systems that will ensure they comply with the CDR system, and deal with related inquiries and complaints from consumers.
- All CDR entities must have a clearly expressed and up-to-date policy about how they manage CDR data (CDR policy). The CDR policy must be provided free of charge and made available in accordance with the CDR Rules.
- The Australian Energy Market Operator Limited (AEMO) is not subject to Privacy Safeguard 1 in its capacity as a data holder.[2] Accordingly, unless otherwise indicated, references in this chapter to data holders and CDR entities exclude AEMO.

What does Privacy Safeguard 1 say?

1.1 Privacy Safeguard 1 requires all CDR entities to:

- take steps that are reasonable in the circumstances to establish and maintain internal practices, procedures and systems that ensure compliance with the CDR system, including the privacy safeguards and CDR Rules, and
- have a clearly expressed and up-to-date CDR policy describing how they manage CDR data. The policy must be available free of charge and in a form consistent with the CDR Rules and provided to the consumer upon request.

Importance of open and transparent management of CDR data and having a CDR policy

1.2 The objective of Privacy Safeguard 1 is to ensure CDR entities manage CDR data in an open and transparent way. It is the bedrock principle.

1.3 By complying with Privacy Safeguard 1, CDR entities will be establishing accountable and auditable practices, procedures and systems that will assist with compliance with all the other privacy safeguards. This leads to a trickle-down effect where privacy is automatically considered when handling CDR data, resulting in better overall privacy management, practice and compliance through a 'privacy-by-design' approach.

[1] Competition and Consumer Act, section 56ED.

[2] Competition and Consumer Regulations, paragraph 28RA(2)(a)(i). For information about how Privacy Safeguard 1 applies to retailers who receive CDR data from AEMO, see paragraph 1.7.

1.4 It is also important that consumers are aware of how their CDR data is handled, and can inquire or make complaints to resolve their concerns. A CDR policy achieves this transparency by outlining how the CDR entity manages CDR data, and by providing information on how a consumer can complain and how the CDR entity will deal with a complaint.

1.5 CDR policies are also a key tool for ensuring open and transparent management of CDR data which can build trust and engage consumers in the management of their data.

Who Privacy Safeguard 1 applies to

1.6 Privacy Safeguard 1 applies to data holders, designated gateways and accredited persons, who are or who may become accredited data recipients of CDR data.[3]

1.7 Privacy Safeguard 1 does not apply to AEMO in its capacity as a data holder.[4] Instead, data holders that are retailers in the energy sector (primary data holders) must comply with Privacy Safeguard 1 in relation to CDR data held by AEMO, that AEMO discloses to them under the Competition and Consumer Act.[5] This obligation applies alongside retailers' Privacy Safeguard 1 obligations in respect of their own data holdings.

Note: *There are currently no designated gateways in the banking sector or energy sector.[6] See Chapter B (Key concepts) for the meaning of designated gateway.*

1.8 As a non-accredited entity, a CDR representative is not directly bound by Privacy Safeguard 1. However, under the terms of the CDR representative arrangement with their CDR principal,[7] a CDR representative is required to adopt and comply with their CDR principal's CDR policy in relation to service data.[8] A CDR principal must ensure the CDR representative complies with the requirements of the CDR representative arrangement, and is liable if the CDR representative breaches any of the CDR representative arrangement provisions which are required by the CDR Rules (including the requirement to adopt and comply with their CDR principal's CDR policy).[9]

---

[3] An accredited person will be an 'accredited person … who may become an accredited data recipient' when they are seeking to collect CDR data. This means that an accredited person must ensure that they comply with their Privacy Safeguard 1 obligations before they seek to collect CDR data.

[4] Competition and Consumer Regulations, paragraph 28RA(2)(a)(i).

[5] Competition and Consumer Regulations, paragraph 28RA(3)(a).

[6] For the banking sector, see the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019. For the energy sector, the energy designation specifies AEMO as a gateway for certain information: subsection 6(4) of the Consumer Data Right (Energy Sector) Designation 2020. However, at the time of publication, AEMO is not a designated gateway for any CDR data because under current CDR Rules, no CDR data is (or is to be) disclosed to AEMO because of the reasons in paragraph 56AL(2)(c) of the Competition and Consumer Act.

There are also no designated gateways in the telecommunications sector, although unlike the banking and energy sectors, at the date of publication of these guidelines, there are no rules allowing for the sharing of designated telecommunications data under the CDR system: Consumer Data Right (Telecommunications Sector) Designation 2022.

[7] A CDR representative arrangement is a written contract between a CDR representative and their CDR principal that meets the minimum requirements listed in CDR Rules, subrule 1.10AA(2).

[8] CDR Rules, paragraph 1.10AA(2)(e). Note that a CDR representative will also have obligations under APP 1 (open and transparent management of personal information) if they are an APP entity.

[9] CDR Rules, rule 1.16A.

How Privacy Safeguard 1 interacts with the Privacy Act

1.9 It is important to understand how Privacy Safeguard 1 interacts with the *Privacy Act 1988* (the Privacy Act) and APP 1.[10]

1.10 APP 1 requires APP entities to manage personal information in an open and transparent way (see APP Guidelines, Chapter 1 (APP 1)).

CDR entity	Privacy protections that apply in the CDR context
Accredited person who may become an accredited data recipient	**Privacy Safeguard 1** When an accredited person is planning to handle 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 1 applies. APP 1 does not apply to the accredited person in relation to that CDR data. [11]
Accredited data recipient	**Privacy Safeguard 1** An accredited data recipient of a consumer's CDR data must comply with Privacy Safeguard 1 in relation to the management of that CDR data. APP 1 does not apply to the accredited data recipient in relation to that CDR data.[12]
Designated gateway	**APP 1 and Privacy Safeguard 1** A designated gateway must comply with: • Privacy Safeguard 1 in relation to the handling of CDR data, and • APP 1 in relation to the handing of personal information (if they are an APP entity). As the obligations in Privacy Safeguard 1 apply generally to an entity's handling of data, a designated gateway must have systems, practices and procedures to comply with both the privacy safeguards and the APPs (including having both a CDR policy and a privacy policy in place).

[10] The Privacy Act includes 13 APPs that regulate the handling of personal information by APP entities. See APP Guidelines, Chapter B (Key concepts) for further information.

[11] See Competition and Consumer Act, subsections 56EC(4) and 56ED(1).

Note: If Privacy Safeguard 1 does not apply, APP 1 may continue to apply to other open and transparent management of the individual's personal information where the accredited person is an APP entity (see Competition and Consumer Act, subsection 56EC(4) and paragraph 56EC(5)(aa)). 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 Privacy Act, subsection 6E(1D).

[12] The APPs do not apply to an accredited data recipient of the CDR data in relation to the CDR data (Competition and Consumer Act, paragraph 56EC(4)(a)). However, this does not affect how the APPs apply to accredited persons in relation to the open and transparent management of the individual's other personal information outside the CDR system. It also does not affect how the APPs apply to CDR data where the accredited person does not become an accredited data recipient of the CDR data (see Competition and Consumer Act, subsection 56EC(4) and paragraph 56EC(5)(aa)). Note: 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 Privacy Act, subsection 6E(1D).

CDR entity	Privacy protections that apply in the CDR context
Data holder (other than AEMO)	**APP 1 and Privacy Safeguard 1** A data holder must comply with: • Privacy Safeguard 1 in relation to the handling of CDR data, and • APP 1 in relation to the handing of personal information (if they are an APP entity). This means that a data holder must have systems, practices and procedures to comply with both the privacy safeguards and the APPs (including having both a CDR policy and a privacy policy in place).[13]
Data holder (AEMO)	**APP 1** Privacy Safeguard 1 does not apply to AEMO as a data holder.[14] AEMO must comply with APP 1 in relation to the handling of personal information. This means that AEMO must have systems, practices and procedures to comply with the APPs (including having a privacy policy in place).

Implementing practices, procedures and systems to ensure compliance with the CDR system

1.11 Privacy Safeguard 1 requires all CDR entities to take steps that are reasonable in the circumstances to establish and maintain internal practices, procedures and systems that:

- ensure compliance with the CDR system, including the privacy safeguards and the CDR Rules, and
- enable the entity to deal with inquiries or complaints from consumers about the entity's compliance with the CDR system, including the privacy safeguards and CDR Rules.[15]

1.12 This is a distinct and separate obligation upon a CDR entity, in addition to being a general statement of its obligation to comply with the CDR system.

1.13 The CDR Rules contain several governance mechanisms, policies and procedures that will assist entities to take steps that are reasonable in the circumstances to comply with the CDR system.[16] Compliance with the mandatory CDR Rules will assist entities to take steps that are reasonable but does not, of itself, demonstrate compliance with Privacy Safeguard 1.

---

[13] See section 56AJ of the Competition and Consumer Act for the meaning of data holder.

[14] Competition and Consumer Regulations, paragraph 28RA(2)(a)(i).

[15] A CDR principal is responsible for dispute resolution in relation to its CDR representatives. Consumers may however complain directly to the CDR representative about that CDR representative's provision of goods or services. Such complaints will trigger the CDR principal's internal dispute resolution obligations in the CDR Rules, paragraph 5.12(1)(b).

[16] For example, accredited persons/accredited data recipients are required to establish a formal governance framework for managing information security risks. See Privacy Safeguard 12, CDR Rules, rules 5.12 and 7.11 and Schedule 2 to the CDR Rules. For further information see Chapter 12 (Privacy Safeguard 12) and the ACCC's Supplementary Accreditation Guidelines on Information Security available on the ACCC's Accreditation Guidelines page.

1.14 To comply with Privacy Safeguard 1, CDR entities need to proactively consider, plan and address how to implement any practices, procedures and systems under the privacy safeguards and the CDR Rules (including how these interact with other obligations). This will assist CDR entities to manage CDR data in an open and transparent way, in accordance with the object of Privacy Safeguard 1.[17]

1.15 Compliance with Privacy Safeguard 1 should therefore be understood as a matter of good governance.

Risk point: Entities who implement the requirements of the privacy safeguards and the CDR Rules in isolation or at a late stage risk incurring unnecessary costs, and/or implementing inadequate solutions that fail to address the full compliance picture.

Privacy tip: Entities should take a 'privacy-by-design' approach in relation to handling CDR data across and within their organisation.[18] This ensures CDR requirements are considered holistically. A tool that may assist an entity in this regard is the CDR data management plan, as outlined in paragraphs 1.32 to 1.35. The OAIC's suggested approach to compliance with Privacy Safeguard 1 in paragraphs 1.36 to 1.45 may also be of assistance.

Circumstances that affect reasonable steps

1.16 The requirement under Privacy Safeguard 1 to implement practices, procedures and systems is qualified by a 'reasonable steps' test.

1.17 This requires an objective assessment of what is considered reasonable in the specific circumstances, which could include:

- the CDR Rules and other legislative obligations that apply to the CDR entity
- the nature of the CDR entity
- whether the CDR entity is handling, or will soon handle, CDR data
- the amount of CDR data handled by the CDR entity
- the possible adverse consequences for a consumer in the case of a breach, and
- the practicability, including time and cost involved.

The CDR system obligations that apply to the CDR entity

1.18 The CDR system obligations (such as the privacy safeguards and the CDR Rules) that apply to the entity will be relevant to determining what steps will be reasonable for compliance with Privacy Safeguard 1.

1.19 For example, the obligations that apply to accredited persons/accredited data recipients are often different to those that apply to data holders and will therefore require the development and implementation of different practices, procedures and systems to achieve compliance.

[17] Competition and Consumer Act, subsection 56ED(1).

[18] For further information on 'privacy by design', see OAIC Privacy by Design Guidance, https://www.oaic.gov.au/privacy/privacy-for-organisations/privacy-by-design.

1.20 Further, where an entity participates in the CDR system in more than one capacity (e.g. as a data holder and an accredited person), this will also affect what constitutes reasonable steps, and the entity will need to put in place mechanisms to ensure it complies with the CDR system in all its different CDR entity capacities.

Examples of key CDR system privacy obligations

The CDR system imposes a range of privacy obligations upon CDR entities. Some of these privacy obligations apply to all CDR entities, while other privacy obligations apply only to a particular entity type. Entities will need to ensure that all of the relevant obligations that apply to them are considered when deciding on the steps to be taken in relation to Privacy Safeguard 1.

For example, an accredited data recipient of CDR data must comply with the privacy safeguards in relation to the CDR data.

However, a data holder needs to comply with the APPs in relation to CDR data that is also personal information with the exception of APPs 10 and 13, which are replaced by Privacy Safeguards 11 and 13 once the data holder is required or authorised to disclose the CDR data under the CDR Rules. Data holders must also comply with both Privacy Safeguard 1 and APP 1, as well as Privacy Safeguard 10.[19] Information regarding compliance with each of the privacy safeguards is available in the relevant chapters of these Guidelines.

In addition to obligations under the privacy safeguards, accredited persons/accredited data recipients and data holders must also consider their obligations in the CDR Rules for the purposes of compliance with Privacy Safeguard 1. These obligations will need to be reflected in the steps taken under Privacy Safeguard 1. For example:

- Accredited persons/accredited data recipients have obligations to report regularly regarding their ongoing information security obligations,[20] including privacy and security training to staff.[21]
- Data holders have obligations relating to consumer data request services. [22]
- Both accredited data recipients and data holders have obligations to provide CDR consumers with access to copies of records upon request.[23]
- Accredited persons who are CDR principals have an obligation to ensure their CDR representative complies with the requirements of the CDR representative arrangement.[24]

[19] Privacy Safeguard 10 does not have an APP equivalent.

[20] CDR Rules, Part 2 of Schedule 1. For further information, see the ACCC's Supplementary Accreditation Guidelines on Information Security available on the ACCC's Accreditation Guidelines page.

[21] Accredited persons/accredited data recipients must ensure all users undergo mandatory security and privacy training prior to interacting with the CDR data environment, with 'refresher courses' provided at least annually: see Privacy Safeguard 12, CDR Rules, rule 5.12 and Part 2 of Schedule 2. For further information, see the ACCC's Supplementary Accreditation Guidelines on Information Security available on the ACCC's Accreditation Guidelines page.

[22] For further information on consumer data request services, authorisation, disclosure of CDR data and a data holder's privacy obligations more generally, see the Guide to privacy for data holders.

[23] CDR Rules, rule 9.5. Accredited data recipients and data holders are required to keep and maintain certain records as outlined in CDR Rules, rule 9.3. They are also required to comply with the reporting requirements in CDR Rules, rule 9.4.

[24] CDR Rules, rule 1.16A.

- Primary data holders have obligations to only use or disclose SR (shared responsibility) data received from a secondary data holder for the purpose of responding to the relevant SR data request.[25]
- Primary data holders have obligations to destroy unsolicited SR data received from a secondary data holder as soon as practicable, unless the primary data holder is required to retain that SR data by or under an Australian law or a court/tribunal order.[26]
- In the banking sector, both accredited persons and data holders must have internal dispute resolution processes that meet the requirements under the Australian Securities and Investments Commission's Regulatory Guide 271 on internal dispute resolution.[27]
- In the energy sector:
    - accredited persons (other than an accredited person who is also a retailer) must have internal dispute resolution processes that meet the requirements under the Australian Securities and Investments Commission's Regulatory Guide 271 on internal dispute resolution,[28] and
    - retailers (including retailers that are also an accredited person) must have internal dispute resolution processes that satisfy the applicable requirements for the retailer's standard complaints and dispute resolution procedures under the National Energy Retail Law or the Energy Retail Code (Victoria).

Privacy tip: A CDR principal is required by subrule 1.16A(1) in the CDR Rules to ensure that their CDR representative complies with the requirements of the written contract.[29] As part of discharging this obligation, a CDR principal could consider:

- undertaking review and assurance activities at least annually
- requiring the CDR representative to provide regular reports against its compliance with the written contract, and/or
- providing the CDR representative with any appropriate assistance or training in technical and compliance matters.

Prior to entering the written contract, it would be appropriate for the CDR principal to make enquiries of the proposed CDR representative, with a focus on their personal information handling capabilities, procedures and practices.

Taking these steps may assist the CDR principal in avoiding a breach of CDR Rule 1.16A, and in doing so, may also assist the CDR principal in avoiding a breach of other privacy-related

[25] CDR Rules, rule 1.24. See Chapter B (Key concepts) for additional information about primary data holders and SR data. See definition of 'primary data holder' and 'SR data' in CDR Rules, subrule 1.7(1).

[26] CDR Rules, rule 1.25. See Chapter B (Key concepts) for additional information about primary data holders and SR data.

[27] See CDR Rules, subrule 5.12(1) (for accredited persons) and Part 5 of Schedule 3 of the CDR Rules (for data holders).

[28] See CDR Rules, subrule 5.12(1) (for accredited persons) and Part 5 of Schedule 4 of the CDR Rules (for data holders).

[29] CDR Rules, subrule 1.16A(1) requires a CDR principal to ensure the CDR representative complies with all requirements under the CDR representative arrangement. Under CDR Rules, subrule 1.16A(2), a CDR principal is in breach if the CDR representative fails to comply with a provision of the CDR representative arrangement which is required by r 1.10AA to be part of that arrangement.

CDR Rules (given the CDR principal is liable for the actions of the CDR representative).

Nature of the entity

1.21 The size of the CDR entity, its resources, the complexity of its operations and the business model are all relevant to determining what steps would be reasonable when putting in place practices, procedures and systems.

1.22 For instance, where a CDR entity uses outsourced service providers, the reasonable steps it should take may be different to those it would take if it did not operate in this manner.

Handling of CDR data

1.23 In some cases, there may be a period of time in between a CDR entity becoming accredited and actively taking steps to handle CDR data. To meet the reasonable steps requirement, a CDR entity will be expected to be more advanced in its preparations under Privacy Safeguard 1 as it approaches the milestone of handling CDR data.

The amount of CDR data handled by the CDR entity

1.24 More rigorous steps may be required as the amount of CDR data handled by a CDR entity increases. Generally, as the amount of CDR data that is held increases, so too will the steps required to satisfy the reasonable steps test.

Adverse consequences for a consumer

1.25 Entities should consider the possible adverse consequences for CDR consumers if CDR data is not managed in accordance with the CDR system. For example, the nature of the CDR data or amount of data held could result in material harm from identity theft or fraud, discrimination, or humiliation or embarrassment. The likelihood of harm occurring will be relevant in considering whether it is reasonable to take a particular step.

Practicability of implementation

1.26 The practicability of implementing a particular step, including the time and cost involved, will influence the reasonableness. A 'reasonable steps' test recognises that privacy protection should be viewed in the context of the practical options available to a CDR entity.

1.27 However, a CDR entity is not excused from implementing particular practices, procedures or systems 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 a particular step will depend on whether the burden is excessive in all the circumstances.

1.28 CDR entities are also not excused from compliance with any specific processes, procedures or systems that are required by the CDR system, regardless of whether that requirement would be in excess of a reasonable step for the purposes of Privacy Safeguard 1.

Existing privacy governance arrangements

1.29 Where an entity has existing privacy practices and procedures for personal information it manages under the Privacy Act, it may be appropriate to extend these to its CDR data.[30]

1.30 However, the mere extension of current practices and procedures does not, of itself, mean that an entity has taken *reasonable steps* to implement practices, procedures and systems.

1.31 Where an entity extends existing practices and procedures to its CDR data handling activities, it will need to consider to what extent it may need to modify those practices, procedures and systems to ensure compliance with the particularities of the CDR system, including the Privacy Safeguards and CDR Rules.[31]

Have a CDR data management plan

1.32 A useful tool that can help CDR entities to plan and document the steps they will take to implement practices, procedures and systems under Privacy Safeguard 1 is a CDR data management plan.

1.33 A CDR data management plan is a document that identifies specific, measurable goals and targets, and sets out how an entity will meet its ongoing compliance obligations under Privacy Safeguard 1. As part of this, the CDR data management plan could set out the tasks an entity will undertake to ensure compliance with Privacy Safeguard 1.

1.34 The CDR data management plan could also set out the processes that will be used to measure and document the CDR entity's performance against their CDR data management plan.

1.35 Where entities have an existing privacy management plan, they may wish to update it with CDR activities so that it is integrated into the entity's privacy management processes. Alternatively, they may choose to have a separate CDR data management plan.

A suggested approach to compliance with Privacy Safeguard 1

1.36 The ongoing compliance requirement in Privacy Safeguard 1 can be addressed in a range of different ways, but should be tailored to the circumstances of the particular entity.

1.37 The following sections outline a suggested method for how steps could be taken to implement practices, procedures and systems under Privacy Safeguard 1.

1.38 The suggested method consists of 4 overarching steps:

- **Embed** a culture that respects and protects CDR data.
- **Establish** robust and effective privacy practices, procedures and systems.
- **Review** and evaluate privacy processes.
- **Enhance** response to privacy issues.

[30] CDR data protected by the privacy safeguards will also be 'personal information' under the Privacy Act. For further information, see Chapter A (Introductory matters).

[31] For information about the interaction between an entity's privacy policy and CDR policy, see paragraphs 1.63 to 1.65.

Privacy tip: Where a CDR entity has a CDR data management plan, they may choose to structure that plan around the 4 overarching steps outlined in paragraph 1.38.

Embed a culture that respects and protects CDR data

1.39 Good CDR data management stems from good data and information governance that creates a culture of privacy that respects and protects CDR data.

1.40 To embed a culture of privacy, entities could:

- Appoint a member of senior management to be responsible for the strategic leadership and overall management of CDR data.
- Appoint an officer (or officers) to be responsible for the day to day managing, advising and reporting on privacy safeguard issues.
- Record and report on how datasets containing CDR data are treated, managed and protected.
- Implement reporting mechanisms that ensure senior management are routinely informed about privacy and data management issues.

Establish robust and effective privacy practices, procedures and systems

1.41 Good privacy management requires the development and implementation of robust and effective practices, procedures and systems.

1.42 For example, an entity should:

- Implement risk management processes that allow identification, assessment and management of privacy risks, including CDR security risks. As part of this, accredited persons/accredited data recipients should consider their obligations to implement strong minimum information security controls under Schedule 2 to the CDR Rules.[32]
- Establish clear processes for reviewing and responding to CDR data complaints. CDR entities should consider their obligations to have internal dispute resolution processes under the CDR Rules.[33]
- Integrate privacy safeguards training into induction processes and provide regular training to those staff who deal with CDR data. This regular training should occur at least once per year. Note that accredited persons/accredited data recipients already have obligations to ensure all users undergo mandatory security and privacy training prior to interacting with the CDR data environment, with 'refresher courses' provided at least annually.[34]

[32] See Privacy Safeguard 12, CDR Rules, rule 5.12 and Schedule 2. For further information see Chapter 12 (Privacy Safeguard 12) and the ACCC's Supplementary Accreditation Guidelines on Information Security available on the ACCC's Accreditation Guidelines page.

[33] See CDR Rules, rule 5.12(1) (for accredited persons) and Part 6 of the CDR Rules (for data holders). For the banking sector, see CDR Rules, Part 5 of Schedule 3; for the energy sector, see CDR Rules, Part 5 of Schedule 4.

[34] See Privacy Safeguard 12, CDR Rules, subrule 5.12(1), rule 7.11 and Schedule 2.

- Establish processes that allow CDR consumers to promptly and easily access and correct their CDR data, in accordance with the privacy safeguards and CDR Rules. As part of this, and in relation to access, data holders should consider their obligations to provide consumer data request services.[35] In relation to correction, CDR entities should consider their obligations under Privacy Safeguard 13 to respond to correction requests from consumers.[36]
- If the entity is a primary data holder:
  - establish processes to ensure the entity only uses the secondary data holder's online service to request SR data it needs to respond to a SR data request[37]
  - establish processes to ensure the entity only uses and discloses the SR data received from a secondary data holder for the purpose of responding to the SR data request, and after responding to the request, deletes any of the SR data it holds in accordance with the CDR data deletion process,[38] and
  - establish processes to ensure that any unsolicited SR data is identified and destroyed as soon as practicable, unless the data is required to be retained by or under an Australian law or a court/tribunal order.[39]

Note: *In the energy sector, the primary data holder will be the relevant retailer.[40] There are no primary data holders in the banking sector.*

Privacy tip: As a starting point for deciding what practices, procedures and systems should be established, a CDR entity should consider their privacy obligations under the privacy safeguards and CDR Rules.

See paragraphs 1.18 to 1.20 for examples of the CDR system privacy obligations that apply to a CDR entity.

Regularly reviewing and evaluating privacy processes

1.43 To evaluate privacy practices, procedures and systems, entities should make a commitment to:

- Monitor and review CDR privacy processes regularly. This could include assessing the adequacy and currency of practices, procedures and systems, to ensure they are up to date and being adhered to.

[35] See CDR Rules, rule 1.13. For further information regarding consumer data request services, see the Guide to privacy for data holders.

[36] See Chapter 13 (Privacy Safeguard 13) for further information.

[37] See CDR Rules, subrule 1.24(1). See CDR Rules, subrule 1.20(2) for secondary data holders' obligations in relation to the provision of an online service that can be used by primary data holders. See Chapter B (Key concepts) for additional information about primary data holders and SR data.

[38] See CDR Rules, subrule 1.24(2). See CDR Rules, rule 1.18 for the definition of 'CDR data deletion process'. See Chapter B (Key concepts) for additional information about primary data holders and SR data.

[39] See CDR Rules, rule 1.25. See Chapter B (Key concepts) for additional information about primary data holders and SR data.

[40] CDR Rules, subclause 4.3(b) of Schedule 4.

- Create feedback channels for both staff and consumers to continue to learn lessons from complaints and breaches, as well as customer feedback more generally.

1.44 Notably, accredited persons are required to provide regular assurance reports (an audit report) and attestation statements concerning compliance with certain information security requirements.[41]

Risk point: Changes to a CDR entity's role in the CDR system and/or information handling practices may mean that existing practices, procedures and systems are no longer fit for purpose.

Privacy tip: When reviewing and evaluating privacy processes, a CDR entity should consider a range of factors including:

- Role in the CDR system – has the entity taken on a new role, for example by becoming an accredited person in addition to being a data holder, or becoming a principal in a CDR representative arrangement? [42]
- Method of service delivery — has the entity changed the way in which it provides goods or services to CDR consumers, for example, by using outsourced service providers to perform any of its functions?[43]
- Online platforms – has the entity changed the online platforms used to communicate with consumers, for example by creating a new mobile application?[44]

The answers to these questions will assist a CDR entity to make the necessary and appropriate changes to practices, procedures and systems (as recommended in the following 'Enhance response to privacy issues' section).

Privacy tip: Where a CDR entity has a CDR data management plan, it should set out the processes that will be used to measure and document the CDR entity's performance against its CDR data management plan, and measure performance against this plan as part of reviewing and evaluating privacy processes.

[41] These obligations are contained in CDR Rules, rule 5.9 and clause 2.1 of Part 2 of Schedule 1 regarding default conditions on accreditation. For further information, see the ACCC's Supplementary Accreditation Guidelines on Information Security available on the ACCC's Accreditation Guidelines page.

[42] Different CDR regime obligations apply depending on what capacity an entity is acting in. See paragraphs 1.18 to 1.20 for further information.

[43] An outsourced service provider is a person who does one or both of the following:

- collects CDR data from a CDR participant on behalf of a principal under a CDR outsourcing arrangement in accordance with the CDR Rules
- provides goods or services to the principal using CDR data that it collected on behalf of the principal or that has been disclosed to them by the principal.

Accredited persons must ensure they comply with the CDR Rules relating to outsourced service providers. For further information, see Chapter B (Key concepts).

[44] By way of example, a CDR entity would need to ensure its CDR policy was available on these new online platforms: see CDR Rules, subrule 7.2(8), which requires accredited data recipients and data holders to make their CDR policy readily available through the online service that they ordinarily use to deal with consumers, such as their website or mobile applications.

Enhance response to privacy issues

1.45 Good privacy management requires entities to be proactive, forward thinking and to anticipate future challenges. To enhance response to privacy issues, entities should make a commitment to:

- Use the results of the evaluations to make necessary and appropriate changes to an organisation's practices, procedures and systems.
- Consider having practices, procedures and systems externally assessed to identify areas where privacy processes may be improved.[45]
- Continuously monitor and address new privacy risks.

Privacy tip: Where a CDR entity has a CDR data management plan, it should ensure this plan is updated to reflect any changes to the entity's role, practices, procedures and systems and accommodate new privacy risks.

Having a CDR policy

1.46 Privacy Safeguard 1 requires all CDR entities to have and maintain a clearly expressed and up-to-date CDR policy.

1.47 The CDR policy must be in the form of a document that is distinct from any of the CDR entity's privacy policies.[46] The Information Commissioner may, but has not, approved a form for the CDR policy.[47]

1.48 Privacy Safeguard 1 and CDR Rule 7.2 set out the requirements for what information must be included in a CDR policy and how it must be made available.[48]

1.49 There are different requirements depending on whether the CDR entity is an accredited person/accredited data recipient, a data holder, or a designated gateway, as set out below. There are also some additional requirements for accredited persons who are also sponsors, affiliates or CDR principals under a CDR representative arrangement.

1.50 Where an entity occupies more than one role in the CDR system (for example is both a data holder and an accredited person), the entity can either have a single CDR policy that outlines how CDR data is managed in both capacities, or a separate CDR policy for each role.

[45] Accredited persons have obligations to provide regular assurance reports (an audit report) and attestation statements concerning compliance with certain Privacy Safeguard 12 CDR Rules. See the ACCC's Supplementary Accreditation Guidelines on Information Security available on the ACCC's Accreditation Guidelines page.

[46] CDR Rules, subrule 7.2(2).

[47] Competition and Consumer Act, paragraph 56ED(3)(b) and CDR Rules, subrule 7.2(1).

[48] The Information Commissioner may, but has not, approved a form for the CDR policy: Competition and Consumer Act, paragraph 56ED(3)(b) and CDR Rules, subrule 7.2(1).

Privacy tip: The OAIC has prepared a Guide to developing a CDR policy to assist CDR entities to prepare and maintain a CDR policy. It provides detailed guidance about what must be included in a CDR policy, as well as a suggested CDR policy development process, and a checklist to help ensure all requirements have been met.

Information that must be included in a CDR policy

1.51 The following sections outline the minimum requirements for information that must be included in a CDR policy.

1.52 For further information and discussion about the requirements for a CDR policy, see the OAIC's Guide to developing a CDR policy.

Accredited persons/Accredited data recipients

1.53 Privacy Safeguard 1 requires that accredited persons who are or may become accredited data recipients must include the following in their CDR policy:

- the classes of CDR data that are (or may be) held by (or on behalf of) the entity as an accredited data recipient. The classes of CDR data for each sector will be set out in the relevant designation instrument.[49] The banking sector designation instrument sets out 3 classes of information: customer information,[50] product use information,[51] and information about a product.[52] The energy sector designation instrument sets out 4 classes of information: information about a customer or associate,[53] information about the sale or supply of electricity,[54] information about retail arrangements,[55] and information about retail arrangements (natural gas)[56]
- how the CDR data is (or is to be) held by or on behalf of the entity as an accredited data recipient
- purposes for which the entity may do each of the following (with the consent of a consumer for the CDR data): collect, hold, use or disclose[57] CDR data
- how a CDR consumer may both access CDR data and seek correction of CDR data
- how a CDR consumer can complain and how the entity will deal with a complaint

[49] The designation instrument for the banking sector is the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019 and for the energy sector is the Consumer Data Right (Energy Sector) Designation 2020. See Chapter B (Key concepts) for further information on designation instruments.

[50] Specified in Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019, section 6.

[51] Specified in Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019, section 7.

[52] Specified in Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019, section 8.

[53] Specified in Consumer Data Right (Energy Sector) Designation 2020, section 7.

[54] Specified in Consumer Data Right (Energy Sector) Designation 2020, section 8.

[55] Specified in Consumer Data Right (Energy Sector) Designation 2020, section 9.

[56] Specified in Consumer Data Right (Energy Sector) Designation 2020, section 10.

[57] Where an accredited data recipient receives a consumer data request under CDR Rules, rule 4.7A from another accredited person, the accredited data recipient may ask the CDR consumer for an AP disclosure consent to disclose the data.

- whether overseas disclosure to accredited persons is likely, and the countries those persons are likely to be based in, if practicable to specify this
- circumstances in which the entity may disclose CDR data to a person who is not an accredited person[58]
- events about which the entity will notify the consumers of such CDR data,[59] and
- when the entity must delete or de-identify CDR data in accordance with a request by a consumer.

1.54 In addition, subrules 7.2(4)-(7) in the CDR Rules provides other matters that an accredited data recipient (or accredited person who may become an accredited data recipient) must include in the CDR policy, including:

- a statement indicating the consequences to the CDR consumer if they withdraw a consent to collect or to use CDR data. This could include information about any early cancellation fees or loss of access to goods or services based on CDR data
- where the entity is a sponsor, a list of affiliates with whom they have a sponsorship arrangement, and the nature of the services one party provides to the other under each arrangement
- where the entity is an affiliate, a list of sponsors with whom they have a sponsorship arrangement, and the nature of the services one party provides to the other under each arrangement
- where the entity is a CDR principal under a CDR representative arrangement:
  - a list of their CDR representatives
  - for each CDR representative, the nature of the goods and services that the CDR representative provides to customers using CDR data
- a list of outsourced service providers (whether based in Australia or based overseas, and whether or not any is an accredited person)
- for each such service provider, the nature of the services it provides and the CDR data or classes of CDR data that may be disclosed to it or collected by it[60]

---

[58] An accredited data recipient can only disclose CDR data to a non-accredited person in accordance with CDR Rules, subrule 7.5(1). Examples of permitted disclosures include disclosures to the consumer or to an outsourced service provider, or to a CDR representative or trusted adviser with the consumer's consent.

[59] The events about which an accredited person will notify a consumer will include:

- when a consumer gives consent to the person collecting, using and/or disclosing their CDR data or amends or withdraws such a consent (for further information, see Chapter C (Consent))
- the collection of a consumer's CDR data (see Chapter 5 (Privacy Safeguard 5))
- the disclosure of a consumer's CDR data to an accredited person (see Chapter 10 (Privacy Safeguard 10))
- any ongoing notification requirements concerning a consumer's consent (see Chapter C (Consent))
- any notification requirements concerning or in relation to the expiry of a consumer's consent (see Chapter C (Consent))
- any response to a consumer's correction request under Privacy Safeguard 13 (see Chapter 13 (Privacy Safeguard 13)), and
- any eligible data breach affecting a consumer under the Notifiable Data Breach scheme (see Chapter 12 (Privacy Safeguard 12)) and the OAIC's Data breach preparation and response guide).

[60] Paragraph 1.53 outlines where to find the classes of data for the banking and energy sectors.

- where the entity wishes to undertake general research using de-identified CDR data, a description of the research to be conducted and any benefits to be provided to the consumer for consenting to the use[61]
- where the entity is likely to disclose CDR data to an overseas, non-accredited outsourced service provider, the countries in which such persons are likely to be based, if practicable to specify this[62]
- if applicable, the following information about de-identification of CDR data that is not redundant data:
    - how the entity uses CDR data that has been de-identified in accordance with the CDR data de-identification process to provide goods or services to consumers
    - how the entity de-identifies CDR data, including a description of techniques that it uses to de-identify CDR data, and
    - if the entity ordinarily discloses (by sale or otherwise) de-identified CDR data to one or more persons: the fact of this disclosure; the classes of persons such data is ordinarily disclosed to; and the purposes for which the entity discloses de-identified CDR data
- the following information about deletion of redundant CDR data:
    - when it deletes redundant data
    - how a CDR consumer may elect for this to happen, and
    - how it deletes redundant data[63]
- if applicable, the following information about de-identification of redundant CDR data:
    - if the de-identified CDR data is used by the accredited data recipient—examples of how the accredited data recipient ordinarily uses de-identified CDR data
    - how the entity de-identifies CDR data, including a description of techniques that it uses to de-identify CDR data, and
    - if the entity ordinarily discloses (by sale or otherwise) de-identified CDR data to one or more persons: the fact of this disclosure; the classes of persons such data is ordinarily disclosed to; and the purposes for which the entity discloses de-identified CDR data
- the following information about the CDR consumer's election to delete their CDR data:
    - how the election operates and its effect, and
    - how consumers can exercise the election

[61] CDR Rules, paragraph 7.5(1)(aa) permits the use or disclosure of CDR data for general research, where it has been de-identified in accordance with the CDR data de-identification processes.

[62] See Competition and Consumer Act, paragraphs 56ED(5)(e)-(f) and CDR Rules, paragraph 7.2(4)(d).

[63] This could include whether it is irretrievably destroyed, reference to any applicable standards, how the accredited data recipient manages hard copy information, how it confirms third party deletion and whether back-ups are secured. Part B of the OAIC's Guide to securing personal information outlines questions entities should consider when destroying personal information, as well as Chapter 12 – Security of CDR data and destruction or de-identification of redundant CDR data for information on the CDR deletion process.

- further information regarding how a CDR consumer can complain and how the entity will deal with the complaint, specifically:
    - where, how and when a complaint can be lodged
    - when a consumer should expect an acknowledgement of their complaint
    - what information is required from the complainant
    - the complaint handling process, including time periods associated with the various stages
    - options for redress,[64] and
    - options for review, both internal and external[65]
- if an entity proposes to store CDR data other than in Australia or an external territory, any country in which the entity proposes to store CDR data.

Data holder

1.55 Privacy Safeguard 1 requires that data holders must include in their CDR policy how a CDR consumer can access and seek correction of their CDR data, how they may complain, and how the entity will deal with a complaint.

1.56 In addition, the CDR Rules provide the following other matters that a data holder must include in their CDR policy:

- whether the data holder accepts consumer data requests for voluntary product data or voluntary consumer data, and, if so whether the data holder charges fees for disclosure of such data and what those fees are,[66] and
- how a CDR consumer can complain and how the entity will deal with a complaint, specifically:
    - where, how and when a complaint can be lodged
    - when a consumer should expect an acknowledgement of their complaint
    - information required from the complainant
    - complaint handling process, including time periods associated with the various stages
    - options for redress,[67] and

[64] 'Redress' in this context means options for remedy rather than options for review. This could include resolution options such as correction, apology, etc.

[65] This would include the relevant external dispute resolution scheme and the Office of the Australian Information Commissioner.

[66] Voluntary product data means CDR data for which there are no consumers that is not required product data: for the banking sector see CDR Rules, clause 3.1 of Schedule 3 and for the energy sector CDR Rules, clause 3.1 of Schedule 4. Voluntary consumer data means CDR data for which there are consumers that is not required consumer data: CDR Rules, clause 3.2 of Schedule 3 and clause 3.2 of Schedule 4.

[67] 'Redress' in this context means options for remedy rather than options for review. This could include resolution options such as correction, apology, etc.

- options for review, both internal and external.[68]

1.57 Finally, the Competition and Consumer Regulations provide that data holders that are energy retailers must ensure that their CDR policy also explains how a CDR consumer can access and correct their AEMO data.[69]

Designated gateway

1.58 Privacy Safeguard 1 requires that designated gateways must include the following in their CDR policy:

- an explanation of how the entity will act between persons to facilitate the disclosure of the CDR data, the accuracy of the CDR data, or any other matters required under the CDR Rules, and
- how a CDR consumer may complain about a failure of the CDR entity to comply with the privacy safeguards or the CDR Rules, and how the CDR entity will deal with such a complaint.

Availability of the CDR policy

1.59 A CDR entity's CDR policy must be publicly and freely available in accordance with the CDR Rules.[70] This furthers the objective of Privacy Safeguard 1 of ensuring that CDR data is managed in an open and transparent way.

1.60 The CDR Rules provide that the CDR entity must make its CDR policy readily available on each online service where the CDR entity, or a CDR representative of the CDR entity, ordinarily deals with CDR consumers.[71] This includes making the CDR policy available through the consumer dashboard.[72]

Consumer requests for a CDR policy

1.61 If a copy of the CDR entity's policy is requested by a CDR consumer, the CDR entity must give the consumer a copy in accordance with CDR Rule 7.2.

1.62 CDR Rule 7.2 provides that, if requested by CDR consumer, the CDR entity must give the consumer a copy of the policy electronically or hard copy as requested by the consumer.

Interaction between an entity's privacy policy and CDR policy

1.63 An entity should be aware that its privacy policy and CDR policy obligations may overlap or relate to each other.

---

[68] This would include the relevant external dispute resolution scheme and the Office of the Australian Information Commissioner.

[69] Competition and Consumer Regulations, paragraph 28RA(3)(a).

[70] Competition and Consumer Act, subsection 56ED(7).

[71] CDR Rules, subrule 7.2(8).

[72] CDR entities ordinarily deal with CDR consumers through the consumer dashboard, and under CDR Rules, subrules 1.14(1) and 1.15(1), the consumer dashboard is an online service. See Chapter B for more information about consumer dashboards.

1.64 While the privacy policy and CDR policy need to be separate,[73] the entity's CDR policy and privacy policy may reference and link to each other where appropriate or required.

1.65 For example, Privacy Safeguard 1 requires a data holder's CDR policy to explain how a CDR consumer may access their CDR data and seek its correction.[74] As a consumer who is an individual may also access their data through APP 12 or seek correction of their data under APP 13 (where the data holder has not been authorised or required to disclose that data), the CDR policy must explain these alternative processes to those under the CDR system.

[73] CDR Rules, subrule 7.2(2).

[74] Competition and Consumer Act, paragraph 56ED(4)(a).