Chapter 1:

Privacy Safeguard 1 —

Open and transparent management of CDR data

Version 2.0, July 2020

OAIC

Contents

Key points

- Privacy Safeguard 1, together with consumer data rule (CDR Rule) 7.2, outlines the requirements for all consumer data right (CDR) entities (accredited data recipients, data holders and designated gateways) to handle 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 regime, and are able to 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. The policy must be provided free of charge and made available in accordance with the CDR Rules.

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 regime, including the Privacy Safeguards and CDR Rules, and
- have a clearly expressed and up-to-date 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 handle 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.

1.4 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.

Who Privacy Safeguard 1 applies to

1.6 Privacy Safeguard 1 applies to data holders, designated gateways and accredited data recipients.

Note: *Currently, there are no designated gateways in the CDR regime responsible for facilitating the transfer of information between data holders and accredited persons (see Chapter B (Key concepts) for the meaning of designated gateway).*

How Privacy Safeguard 1 interacts with the Privacy Act and APP 1

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

1.8 APP 1 requires APP entities to manage personal information in an open and transparent way (see Chapter 1: APP 1 — Open and transparent management of personal information of the APP Guidelines).

CDR entity	Privacy protections that apply in the CDR context
Accredited person / accredited data recipient	**Privacy Safeguard 1 and APP 1** All accredited persons must comply with APP 1 in relation to the handling of personal information.[2] Entities should be aware that when an accredited person collects *any* CDR data, the person will also become an accredited data recipient and must then comply with: • Privacy Safeguard 1 in relation to the handling of CDR data, and • APP 1 in relation to the handling of personal information that is not CDR data. As APP 1 and Privacy Safeguard 1 both apply generally to an entity's handling of data, accredited data recipients must have systems, practices and procedures in place to ensure compliance with both the privacy safeguards and the APPs (including having both a CDR policy and privacy policy in place).[3] **Note**: While Privacy Safeguard 1 does not apply to accredited persons before they have collected any CDR data, the OAIC recommends that accredited persons consider their Privacy Safeguard 1 obligations early, so that they will meet their obligations under Privacy Safeguard 1 and CDR Rule 4.11(3) as soon as they start to seek to collect CDR data.

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

[2] 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. Section 6E(1D) of the Privacy Act.

[3] CDR Rule 4.11(3) requires accredited persons to provide certain information from their CDR policy to the consumer when seeking consent to collect and use CDR data.

CDR entity	Privacy protections that apply in the CDR context
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).
Data holder	**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).[4]

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

1.9 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 regime, 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 regime, including the privacy safeguards and CDR Rules.

1.10 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 regime.

1.11 The CDR Rules contain several governance mechanisms, policies and procedures that will assist entities to take steps that are reasonable to comply with the CDR regime.[5] However, while compliance with the CDR Rules will assist entities to take steps that are reasonable, this does not of itself mean that the entity has complied with Privacy Safeguard 1.

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

[5] For example, accredited data recipients are required to establish a formal governance framework for managing information security risks under the Privacy Safeguard 12 CDR Rules.

1.12 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.[6]

1.13 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. 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 1.29 to 1.32. The OAIC's suggested approach to compliance with Privacy Safeguard 1 in paragraphs 1.33 to 1.42 may also be of assistance.

Circumstances that affect reasonable steps

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

1.15 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
- 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 regime obligations that apply to the CDR entity

1.16 The CDR regime 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 in terms of compliance with Privacy Safeguard 1.

1.17 For example, the obligations that apply to accredited data recipients are in many cases 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.

1.18 Further, where an entity participates in the CDR regime in more than one capacity (e.g. as a data holder and an accredited data recipient), 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 regime in all its different CDR entity capacities.

[6] Section 56ED(1) of the Competition and Consumer Act.

Examples of key CDR regime privacy obligations

The CDR regime 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 must comply with all 13 privacy safeguards, while a data holder needs to comply only with Privacy Safeguards 1, 10, 11 and 13. 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 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 data recipients have obligations to report regularly regarding their compliance with Privacy Safeguard 12,[7] and provide privacy and security training to staff.[8]
- Data holders have obligations relating to consumer data request services, and the authorisation and disclosure of CDR data.[9]
- Both accredited data recipients and data holders have obligations to provide consumers with access to copies of records upon request.[10]
- In the banking sector, both accredited data recipients and data holders must have internal dispute resolution processes that meet the requirements under the Australian Securities and Investments Commission's Regulatory Guide 165 on internal and external dispute resolution.[11]

Nature of the entity

1.19 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.

1.20 For instance, where a CDR entity uses outsourced service providers (such as cloud-based service providers for hosting services or data centres and backup providers), the reasonable

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

[8] 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 Part 2 of Schedule 2 to the CDR Rules, in relation to Privacy Safeguard 12.

[9] 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.

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

[11] See CDR Rule 5.12(1) (for accredited data recipients) and Part 6 of the CDR Rules (for data holders).

steps it should take may be different to those it would take if it did not operate in this manner.

The amount of CDR data handled by the CDR entity

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

Adverse consequences for a consumer

1.22 Entities should consider the possible adverse consequences for the consumers concerned if the CDR data is not handled in accordance with the CDR regime. 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

1.23 The practicality of implementing, 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.

1.24 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.

1.25 CDR entities are also not excused from any specific processes, procedures or systems that are required by the CDR regime.

Existing privacy governance arrangements

1.26 Where an entity has existing privacy practices and procedures for personal information it handles under the Privacy Act, it may be appropriate to extend these to its CDR data.[12]

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

1.28 Entities will need to take further action to modify practices, procedures and systems to meet obligations under Privacy Safeguard 1 to ensure compliance with the particularities of the CDR regime.

Have a CDR data management plan

1.29 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.

---

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

1.30 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.

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

1.32 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

1.33 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.

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

1.35 The suggested method consists of four 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.

Privacy tip: Where a CDR entity has a CDR data management plan, they may choose to structure that plan around the four overarching steps outlined in paragraph 1.35.

Embed a culture that respects and protects CDR data

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

1.37 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

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

1.39 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 data recipients should consider their obligations to implement strong minimum information security controls under Privacy Safeguard 12.[13]
- Establish clear processes for reviewing and responding to CDR data complaints. For the banking sector, CDR entities should consider their obligations to have internal dispute resolution processes that meet the relevant ASIC requirements.[14]
- Integrate privacy safeguards training into induction processes and provide regular staff training to those who deal with CDR data. This regular training should occur at a minimum of once per year. Note that accredited data recipients already have obligations under Privacy Safeguard 12 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.[15]
- Establish processes that allow 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.[16] In relation to correction, CDR entities should consider their obligations under Privacy Safeguard 13 to respond to correction requests from consumers.[17]

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 1.16 to 1.18 for examples of the CDR regime privacy obligations that apply to a CDR entity.

[13] See Schedule 2 to the CDR Rules, Chapter 12 (Privacy Safeguard 12) and the ACCC's Supplementary Accreditation Guidelines on Information Security available on the ACCC's Accreditation Guidelines page.

[14] The obligation is to have internal dispute resolution processes that meet the requirements under the Australian Securities and Investments Commission's Regulatory Guide 165 on internal and external dispute resolution. See CDR Rule 5.12(1) (for accredited data recipients) and Part 6 of the CDR Rules (for data holders).

[15] See Part 2 of Schedule 2 to the CDR Rules.

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

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

Regularly reviewing and evaluating privacy processes

1.40 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.
- Create feedback channels for both staff and consumers to continue to learn lessons from complaints and breaches, as well as customer feedback more generally.

1.41 Notably, accredited data recipients are required to provide regular assurance reports (an audit report) and attestation statements concerning compliance with certain information security requirements under Privacy Safeguard 12.[18]

Risk point: Changes to a CDR entity's role in the CDR regime 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 regime — has the entity taken on a new role, for example by becoming an accredited data recipient in addition to being a data holder?[19]
- 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?[20]
- Online platforms — has the entity changed the online platforms used to communicate with CDR consumers, for example by creating a new mobile application?[21]

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).

[18] These obligations are contained in Part 2 of Schedule 1 to the CDR Rules. For further information, see the ACCC's Supplementary Accreditation Guidelines on Information Security available on the ACCC's Accreditation Guidelines page.

[19] Different CDR regime obligations apply depending on what capacity an entity is acting in. See paragraphs 1.16 to 1.18 for further information.

[20] An outsourced service provider is a person to whom an accredited person discloses CDR data under a CDR outsourcing arrangement. Accredited persons must ensure they comply with the CDR Rules relating to outsourced service providers. For further information, see Chapter B (Key concepts) of the CDR Privacy Safeguard Guidelines.

[21] By way of example, a CDR entity would need to ensure their CDR policy was available on these new online platforms: see CDR Rule 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.

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

Enhance response to privacy issues

1.42 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.[22]
- Continuously monitor and address new privacy risks.

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

Having a CDR policy

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

1.44 The CDR policy must be in the form of a document that is distinct from any of the CDR entity's privacy policies.[23] The Information Commissioner may, but has not, approved a form for the CDR policy.[24]

1.45 Privacy Safeguard 1 and CDR Rule 7.2 set out the requirements for what information must be included in a CDR policy, how it must be made available and what form it should be in.[25]

1.46 There are different requirements depending on whether the CDR entity is an accredited data recipient, a data holder, or a designated gateway, as set out below.

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

---

[22] 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.

[23] CDR Rule 7.2(2).

[24] Section 56ED(3)(b) of the Competition and Consumer Act and CDR Rule 7.2(1).

[25] The Information Commissioner may, but has not, approved a form for the CDR policy: section 56ED(3)(b) of the Competition and Consumer Act and CDR Rule 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 process, and a checklist to help ensure all requirements have been met.

Information that must be included in a CDR policy

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

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

Accredited data recipients

1.50 Privacy Safeguard 1 requires that accredited data recipients must include the following in their CDR policy:

- the classes[26] of CDR data held. The designation instrument sets out three classes of information for the banking sector: customer information,[27] product use information,[28] and information about a product[29]
- how the CDR data is held
- purposes for which the entity may collect, hold, use or disclose CDR data
- how a consumer may access or correct CDR data
- how a consumer can complain and how the entity will deal with a complaint
- 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[30]
- events about which the entity will notify the consumers of such CDR data,[31] and
- when the entity must delete or de-identify CDR data in accordance with a request by a consumer.

1.51 In addition, the CDR Rules provide other matters that must be included in the CDR policy, including:

---

[26] The classes of information are set out in the designation instrument for the relevant sector.

[27] Specified in section 6 of the designation instrument.

[28] Specified in section 7 of the designation instrument.

[29] Specified in section 8 of the designation instrument.

[30] An accredited data recipient is not authorised under the CDR Rules to disclose to any person except directly to the consumer or to an outsourced service provider.

[31] The events about which an accredited person will notify a consumer will include when a consumer gives consent to the person collecting and using their CDR data or withdraws such a consent, the collection of a consumer's CDR data, any ongoing notification requirements concerning a consumer's consent, any response to a consumer's correction request under Privacy Safeguard 13 and any eligible data breach affecting a consumer under the Notifiable Data Breach scheme.

- A statement indicating the consequences to the consumer if they withdraw a consent to collect or to use CDR data. This could include information about any early cancellation fees.
- A list of outsourced service providers, the nature of their services, the CDR data and classes of CDR data that may be disclosed.
- Where the entity is likely to disclose CDR data overseas to a service provider who is not accredited, a list of countries in which the overseas persons are likely to be based (if it is practicable to specify those countries in the policy).
- Where the entity proposes to store CDR data other than in Australia or an external territory, the countries in which the entity proposes to store CDR data.
- Where the entity seeks or intends that it will seek consent from consumers to de-identify their CDR data in accordance with CDR Rule 4.11(3)(e):
    - why the entity asks for consents to de-identify 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 accredited data recipient discloses de-identified CDR data.
- When and how the entity destroys 'redundant data', and how a consumer may ask for the entity to destroy their CDR data when it becomes redundant data.
- Where the entity has a general policy of de-identifying CDR data once it becomes redundant data:
    - if the entity uses the de-identified CDR data, examples of how the entity 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 to whom such data is ordinarily disclosed, and the purposes for which the entity discloses de-identified CDR data.
- Further information regarding how a 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, and
    - options for review.

Data holder

1.52 Privacy Safeguard 1 requires that data holders must include in their CDR policy how a consumer can access and correct the CDR data, and how they may complain.

1.53 In addition, the CDR Rules provide other matters that must be included in the CDR policy, including:

- 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,[32] and
- how a 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, and
  - options for review.

Designated gateway

1.54 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 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

1.55 The CDR policy must be publicly and freely available in accordance with the CDR Rules.[33] This furthers the objective of Privacy Safeguard 1 of ensuring that CDR data is managed in an open and transparent way.

1.56 The CDR Rules provide that the CDR policy must be readily available on each online service where the CDR entity ordinarily deals with CDR consumers.[34]

---

[32] Voluntary product data means CDR data for which there are no consumers that is not required product data: clause 3.1 of Schedule 3 to the CDR Rules. Voluntary consumer data means CDR data for which there are consumers that is not required consumer data: clause 3.2 of Schedule 3 to the CDR Rules.

[33] Section 56ED(7) of the Competition and Consumer Act.

[34] CDR Rule 7.2(8).

Consumer requests for a CDR policy

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

1.58 The CDR Rules provide that, if requested by 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

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

1.60 While the privacy policy and CDR policy need to be separate,[35] the entity's CDR policy and privacy policy may reference and link to each other where appropriate or required.

1.61 For example, Privacy Safeguard 1 requires a data holder's CDR policy to explain how a consumer may access their CDR data and seek its correction.[36] 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 regime.

[35] CDR Rule 7.2(2).

[36] Section 56ED(4)(a) of the Competition and Consumer Act.