Chapter 12:

Privacy Safeguard 12 —

Security of CDR data, and destruction or de-identification of redundant data

Version 1.0, February 2020

OAIC

Contents

Key points

- Securing CDR data is an integral element of the consumer data right (CDR) regime.
- Privacy Safeguard 12 places requirements on accredited data recipients and designated gateways to ensure CDR data is protected from misuse, interference and loss, as well as from unauthorised access, modification or disclosure. The specific steps that these entities must take to protect CDR data are in the consumer data rules (CDR Rules).
- In addition, if an accredited data recipient or a designated gateway no longer needs the CDR data for purposes permitted by privacy safeguards or the CDR Rules, then the data is considered 'redundant data' and will need to be destroyed (or deleted) or de-identified unless an exception applies.
- An applicant for accreditation must demonstrate compliance with the information security requirements in Privacy Safeguard 12 in order to gain and maintain accreditation under the CDR regime.

What does Privacy Safeguard 12 say?

12.1 Accredited data recipients and designated gateways must take the steps in the CDR Rules to protect CDR data from misuse, interference and loss, as well as unauthorised access, modification and disclosure.

12.2 Accredited data recipients and designated gateways must also take the steps set out in the CDR Rules to destroy or de-identify any CDR data that is no longer needed for:

- the purposes permitted under the CDR Rules, or
- any purpose for which the information may be used or disclosed under the privacy safeguards.

12.3 Consumers can request that their CDR data be deleted once it is no longer needed. Accredited data recipients and designated gateways must delete CDR data that is subject to a deletion request unless an exception applies.

12.4 These requirements apply except where:

- the accredited data recipient or designated gateway is required by law or a court/tribunal order to keep the CDR data, or
- the CDR data relates to current or anticipated legal or dispute resolution proceedings to which the accredited data recipient, designated gateway or consumer is a party.

Why is it important?

12.5 Poor information security can leave systems and services at risk and may cause harm and distress to individuals, whether to their well-being, finances, or reputation. Some examples of harm include:

- financial fraud including unauthorised credit card transactions or credit fraud

- identity theft causing financial loss or emotional and psychological harm
- family violence, and
- physical harm or intimidation.

12.6 Poor information security practices negatively impact an entity's reputation and undermine its commercial interests. As shown in the OAIC's long-running national community attitudes to privacy survey, privacy protection contributes to an individual's trust in an entity. If an entity is perceived to be handling data contrary to community expectations, individuals may seek out alternative products and services.

12.7 In addition, accredited data recipients are entrusted with CDR data under the CDR regime to allow them to provide products and services to consumers. Privacy Safeguard 12 ensures that accredited data recipients are taking steps to ensure a consistent, high standard of security under the CDR Rules to ensure this data is protected. This helps to build public trust and confidence in the security practices of accredited data recipients.

12.8 Dealing with redundant data also minimises the risk profile of an accredited data recipient as they are not holding unnecessary CDR data.

Who does Privacy Safeguard 12 apply to?

12.9 Privacy Safeguard 12 applies to accredited data recipients and designated gateways. It does not apply to data holders. However, data holders must ensure that they are adhering to their obligations under the *Privacy Act 1988* (the Privacy Act) and the Australian Privacy Principles (APPs), including APP 11, in relation to the security of personal information.

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).*

Accreditation guidelines on information security

12.10 This chapter provides guidance on the steps for securing CDR data and managing redundant data in compliance with Privacy Safeguard 12.

12.11 An applicant for accreditation must demonstrate compliance with information security requirements in Privacy Safeguard 12 in order to gain and maintain accreditation under the CDR regime.

12.12 Accredited persons should refer to the Supplementary Accreditation Guidelines on Information Security by the Australian Competition and Consumer Commission (ACCC) for specific guidance on the:

- information security obligations under Privacy Safeguard 12 that applicants must satisfy for accreditation under the CDR regime, and
- ongoing information security and reporting obligations under Privacy Safeguard 12, including preparing attestation and assurance reports.

How Privacy Safeguard 12 interacts with the Privacy Act

12.13 It is important to understand how Privacy Safeguard 12 interacts with the Privacy Act and the APPs.[1]

12.14 APP 11 requires APP entities to take measures to ensure the security of personal information they hold and to consider whether they are permitted to retain this personal information (see Chapter 11: APP 11 – Security of personal information of the APP Guidelines).

CDR entity	Privacy protections that apply in the CDR context
Accredited person / Accredited data recipient	**Privacy Safeguard 12** Privacy Safeguard 12 applies instead of APP 11 to CDR data collected by an accredited data recipient under the CDR regime. APP 11 will continue to apply to the security of personal information held by an accredited person or accredited data recipient that is not CDR data. [2] **Note:** All accredited persons must also demonstrate compliance with Privacy Safeguard 12 to maintain accreditation under the CDR regime. [3]
Designated gateways	**Privacy Safeguard 12** Privacy Safeguard 12 applies instead of APP 11 in relation to the security of CDR data.[4] APP 11 will continue to apply to any personal information held that is not CDR data.
Data holders	**APP 11** Privacy Safeguard 12 does not apply to data holders.

[1] The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies (APP entities). See also Chapter B: Key concepts of the APP guidelines.

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

[3] See the ACCC's Supplementary Accreditation Guidelines on Information Security for more information.

[4] Section 56EC(4)(d) of the Competition and Consumer Act.

PART A: Security of CDR data

What do security measures need to protect against?

12.15 An accredited data recipient is required to put in place specific information security measures to protect the CDR data they receive from misuse, interference and loss, as well as unauthorised access, modification and disclosure.

12.16 A designated gateway of CDR data is required to put in place information security measures to protect that CDR data from misuse, interference and loss, as well as unauthorised access, modification and disclosure.

12.17 The terms 'misuse', 'interference', 'loss' and 'unauthorised access' are not defined in the Competition and Consumer Act. The following discussion represents the OAIC's interpretation of these terms based on their ordinary meaning. However, given that information security is an evolving concept, the discussion below is not intended to include an exhaustive list of examples.

- **Misuse:** occurs where CDR data is used for a purpose not permitted by the CDR. For example, misuse would occur if an employee of a CDR entity browses consumer statements to discover information about someone they know. [5]
- **Interference:** occurs when there is an attack on CDR data that interferes with the CDR data but does not necessarily modify its content. For example, interference would occur if there is a ransomware attack that leads to the data being locked down and ransomed.
- **Loss:** refers to the accidental or inadvertent loss of CDR data where the data is no longer accessible and usable for its purpose, or in circumstances where it is likely to result in authorised access or disclosure. Examples of loss include physical loss by leaving data in a public place, failing to keep adequate backups in the event of systems failure or as a result of natural disasters.[6]
- **Unauthorised access:** occurs where CDR data is accessed by someone who is not permitted to do so. This includes unauthorised access by an employee of the accredited data recipient or designated gateway, or an independent contractor, as well as unauthorised access by an external third party. For example, unauthorised access would occur if a computer network is compromised by an external attacker resulting in CDR data being accessed without authority.
- **Unauthorised modification:** occurs where CDR data is altered by someone who is not permitted to do so, or where the data is altered in a way that is not permitted. For example, unauthorised modification would occur if an employee of an accredited

[5] Privacy Safeguard 6 sets out when an accredited data recipient of CDR data or a designated gateway of CDR data is permitted to use that CDR data (see Chapter 6 (Privacy Safeguard 6)). Privacy Safeguards 7 and 9 also contain requirements relating to an entity's use of CDR data for the purpose of direct marketing and use of government related identifiers respectively (see Chapters 7 (Privacy Safeguard 7) and 9 (Privacy Safeguard 9)).

[6] Loss does not apply to intentional destruction or de-identification of CDR data undertaken in accordance with the CDR Rules.

data recipient or designated gateway altered a consumer's savings account information to offer a more favourable deal.

- **Unauthorised disclosure:** occurs where an accredited data recipient or designated gateway, whether intentionally or unintentionally, makes CDR data accessible or visible to others outside the entity. For example, unauthorised disclosure includes 'human error', such as an email sent to the wrong person. It can also include disclosure of CDR data to a scammer as a result of inadequate identity verification procedures.

12.18 Information security not only covers cybersecurity (the protection of your networks and information systems from cyber attack), but also physical and organisational security measures.

What steps does an entity need to take to secure CDR data?

12.19 Privacy Safeguard 12 requires accredited data recipients and designated gateways to take the steps in the CDR Rules to protect the CDR data from misuse, interference and loss, as well as unauthorised access, modification and disclosure. These steps are detailed in Schedule 2 of the CDR Rules.

12.20 The CDR Rules provide obligations for accredited data recipients to have governance requirements in place, understand their data environment and risk posture, and implement minimum security controls.

12.21 Broadly, the steps to manage the information security of CDR data are:

- **Step 1:** define and implement security governance in relation to CDR data.
- **Step 2:** define the boundaries of the CDR data environment.
- **Step 3:** have and maintain an information security capability (including minimum security controls set out in Part 2 of Schedule 2 to the CDR Rules).
- **Step 4:** implement a formal controls assessment program.
- **Step 5:** manage and report security incidents.

12.22 This section summarises what is required by these steps and provides guidance on how accredited data recipients may implement them.

12.23 The five steps are not sequential and do not have to be undertaken in order. They should be understood as the minimum processes, policies and procedures that must be put in place to ensure security of CDR data. As such, these steps may occur in parallel and may be repeated iteratively as required.

Step 1: Define and implement security governance in relation to CDR Data

Information security governance framework

12.24 The CDR Rules require an accredited data recipient to establish and maintain a formal governance framework[7] for managing information security risks relating to CDR data.

12.25 An accredited data recipient may leverage their existing information security governance structure and extend it to their CDR data environment.[8] An accredited data recipient may also utilise existing frameworks, requirements and models in developing their information security governance framework and defining security areas.[9]

12.26 Complying with an existing framework or model does not, of itself, mean that the entity will be compliant with all information security obligations under Privacy Safeguard 12.

12.27 When deciding whether to adopt, apply or modify a standard information security governance framework or model, an accredited data recipient should ensure that the framework or model:

- is appropriate for CDR data and the CDR sector(s) in which the accredited data recipient is operating
- is current and up to date
- takes into account what internal or external auditing is undertaken, and
- is underpinned by a risk profile comparable to the risk profile of the accredited data recipient's CDR data environment.

12.28 Accredited persons are subject to ongoing reporting and audit requirements set out in the CDR Rules (Schedule 1, Part 2). Further information regarding the reporting requirements is contained within the ACCC's Supplementary Accreditation Guidelines on Information Security. Accredited data recipients should ensure that any information security governance framework or model takes these requirements into account.

Privacy tip: An accredited data recipient should consider conducting a security risk assessment (which may be part of a broader risk assessment to identify other risks including data mismanagement and quality) before establishing and maintaining a formal governance framework. This ensures the accredited data recipient is aware of their security risk profile and vulnerabilities so that the formal governance framework matches the privacy risks and is fit for purpose.

[7] A formal governance framework refers to policies, processes, roles and responsibilities required to facilitate the oversight and management of information security.

[8] For further information, see the ACCC's Supplementary Accreditation Guidelines on Information Security.

[9] The ACCC's Supplementary Accreditation Guidelines on Information Security provide examples of frameworks, requirements and models that might be used in this regard, namely ISO 27001, NIST CSF, PCI DSS and CPS 234.

Documenting practices and procedures relating to information security and management of CDR data

12.29 Accredited data recipients must clearly document their practices and procedures relating to information security and management of CDR data, including the specific responsibilities of senior management.[10]

12.30 Accredited data recipients may choose to document these practices and procedures as part of the information security policy required by the CDR Rules, (see paragraphs 12.34–12.38) or as a separate document.

12.31 Senior management will have ultimate responsibility for the management of information security.[11] Senior management should implement the necessary practices, procedures, resources and training to allow the accredited data recipient to effectively discharge its responsibilities under the CDR Rules.[12]

12.32 An accredited data recipient should establish formal information security governance structures, such as committees and forums, to oversee the security of CDR data.[13] These committees or forums should include membership from across key business areas, particularly where the entity's CDR data environment is large or complex,[14] so information security is an integrated component of the accredited data recipient's entire business and not left to the compliance or the information and communications technology area alone.

12.33 An accredited data recipient's formal information security governance structures should have clear procedures for oversight and accountability, and clear lines of authority for decisions regarding the security of CDR data.

Risk point: Accredited data recipients that view security as a box-ticking exercise or treat it in isolation from broader organisational frameworks can expose CDR data to security risks.

Privacy tip: Accredited data recipients should foster a security-aware culture amongst staff. When establishing procedures for oversight, accountability and lines of authority for decisions regarding CDR security, it is expected that:

- privacy and personal information security steps and strategies are supported by senior management
- senior management should promote a privacy culture that values and protects CDR data and supports the integration of privacy practices, procedures and systems into broader organisational frameworks

[10] Clause 1.3(2) of Schedule 2 to the CDR Rules.

[11] Senior management, of an accredited data recipient that is a body corporate, means: (a) the accredited data recipient's directors; and (b) any person who makes or participates in making decisions that affect the management of CDR data by the accredited data recipient: clause 1.2 of Schedule 2 to the CDR Rules.

[12] The ACCC's Supplementary Accreditation Guidelines on Information Security.

[13] The ACCC's Supplementary Accreditation Guidelines on Information Security.

[14] The ACCC's Supplementary Accreditation Guidelines on Information Security.

- it is clear to staff who holds key security roles, including who is responsible for the overall operational oversight and strategic direction of secure CDR data handling, and
- if there are several areas or teams responsible for information security and privacy, or if the organisation's CDR data environment is large or complex, there should be governance arrangements in place to ensure that key business areas work together (for example, committees and forums).

Information security policy

12.34 An accredited data recipient must have and maintain an information security policy that governs information security across their organisation.[15]

12.35 The information security policy must include information about[16]:

- its information security risk posture (that is, the exposure and potential harm to the entity's information assets, including CDR data, from security threats)
- how the entity plans to address those risks
- the exposure and potential harm from security threats, and
- how its information security practices and procedures and its information security controls, are designed, implemented and operated to mitigate those risks.

12.36 The information security policy should be internally and externally enforceable. Compliance with the policy should also be monitored.[17]

12.37 An accredited data recipient may choose to address CDR data security in a single policy or across multiple policies (for example, to account for different business areas). While a specific information security policy for CDR data is preferred, it is not required.

12.38 Entities should ensure relevant staff are aware of the information security policy and are trained in their responsibilities. The information security policy should be easily accessible to all relevant staff.

Risk point: Failing to ensure that employees are aware of their information security obligations risks non-compliance with the CDR information security requirements.

Privacy tip: Relevant employees should be aware of, and have access to, the information security policy. The information security policy should include provisions to deal with breaches of the policy by employees and ongoing monitoring of compliance.

---

[15] Clause 1.3(3) of Schedule 2 to the CDR Rules.

[16] Clause 1.3(3) of Schedule 2 to the CDR Rules.

[17] The term 'enforceable' is defined in the ACCC's Supplementary Accreditation Guidelines on Information Security as both internally and externally, including provisions to deal with breaches of the policy. 'Internally' refers to the policy being enforceable against an accredited person's employees and internal departments. 'Externally' refers to the policy, or parts thereof, being enforceable against the accredited person's third-parties and vendors through mechanisms such as contractual requirements and ongoing third party monitoring processes.

Review of appropriateness

12.39 The accredited data recipient must review and update the formal governance framework for appropriateness:

- in response to material changes to both the extent and nature of threats to its CDR data environment and its operating environment, or
- where no such material changes occur — at least annually.[18]

What is a material change?

A material change is one that significantly changes the CDR data environment, such as the introduction of a new system, the migration of data onto new infrastructure, introduction of a new outsourced service provider, or a change to the terms and conditions of the services provided by an existing outsourced service provider.[19]

Step 2: Define the boundaries of the CDR data environment

12.40 An accredited data recipient must assess, define and document its CDR data environment. To define and document the CDR data environment, accredited data recipients should identify the people, processes and technology that manage, secure, store or otherwise interact with CDR data. This includes infrastructure, which may be owned and/or managed by an outsourced service provider or third-party.[20]

12.41 Mapping the CDR data environment will ensure an accredited data recipient is fully aware of the CDR data it handles, where the data is kept, who has access to it, and the risks associated with that data before applying security capability controls in Step 3. It will also help to ensure that an accredited data recipient's privacy, procedures and systems are up to date.

Factors to consider as part of the documented CDR data environment analysis

'CDR data environment' refers to the systems, technology and processes that relate to the management of CDR data, including CDR data disclosed to outsourced service providers. The documented analysis should generally include information about:

People: Who will have access to CDR data? Who will authorise access?

Technology: Such as information systems, storage systems (including whether data is stored overseas, with a cloud service provider, or other third-party), data security systems, authentication systems.

Processes: The entity's CDR information handling practices, such as how it collects, uses and stores personal information, including whether CDR data handling practices are outsourced to third parties.

[18] Clause 1.3(4) of Schedule 2 to the CDR Rules.

[19] See the ACCC's Supplementary Accreditation Guidelines on Information Security.

[20] See the ACCC's Supplementary Accreditation Guidelines on Information Security.

Other factors to consider: What other data exists in the data environment, and how does it overlap or connect with the CDR data? This is important to know in order to identify which datasets are high-risk. It is important to identify where non-CDR datasets could be linked with CDR data, increasing the risk of unauthorised disclosure or access.

12.42 This can either be documented through a data flow diagram or a written statement.[21]

12.43 Accredited data recipients need to review their CDR data environment for completeness and accuracy:

- as soon as practicable when they become aware of material changes to the extent and nature of threats to their CDR data environment, or
- where no such material changes occur, at least annually.

Step 3: Have and maintain an information security capability

12.44 The CDR Rules require an accredited data recipient to have and maintain an information security capability that:

- complies with minimum controls set out in Part 2 to Schedule 2 of the CDR Rules, and
- is appropriate and adapted to respond to risks to information security, having regard to:
  - the extent and nature of threats to CDR data that the accredited data recipient holds
  - the extent and nature of CDR data that it holds, and
  - the potential loss or damage to one or more consumers if all, or part, of the consumer's data were to be misused, interfered with, or accessed, modified or disclosed without authorisation.

12.45 The accredited data recipient must review and adjust its information security capability as required by the CDR Rules (see paragraphs 12.55 – 12.56 following).

Information security controls

12.46 The CDR Rules contain information security controls to be designed, implemented and operated by an accredited data recipient as part of its information security capability. These are detailed in Part 2 to Schedule 2 to the CDR Rules.

12.47 These controls cover:

- having processes in place to limit the risk of inappropriate or unauthorised access to its CDR data environment
- taking steps to secure the network and systems within the CDR data environment

[21] For further information see the ACCC's Supplementary Accreditation Guidelines on Information Security.

- securely managing information assets within the CDR data environment over their lifecycle
- implementing a formal vulnerability management program to identify, track and remediate vulnerabilities within the CDR data environment in a timely manner
- taking steps to limit, prevent, detect and remove malware in the CDR data environment, and
- implementing a formal information security training and awareness program for all personnel interacting with CDR data.

12.48 Compliance with Privacy Safeguard 12 requires the implementation of these controls across the CDR environment.

12.49 The information security controls in Part 2, Schedule 2 of the CDR Rules are the *minimum controls* required for an applicant to become accredited and for an accredited data recipient to ensure ongoing compliance with Privacy Safeguard 12. An accredited data recipient may choose to implement stronger protections.

12.50 Further information regarding the minimum information security controls is contained in the ACCC's Supplementary Accreditation Guidelines on Information Security.

Additional security controls required to respond to risks to information security

12.51 In addition to the information security controls set out in Part 2 Schedule 2 of the CDR Rules, an accredited data recipient must also have and maintain an information security capability that is appropriate and adapted to respond to risks to information security, having regard to:

- the extent and nature of threats to CDR data that it holds, and
- the extent and nature of CDR data that it holds, and the potential loss or damage to one or more consumers if all or part of the consumer's data were to be misused, interfered with, or accessed, modified or disclosed without authorisation.

12.52 Accredited data recipients familiar with the Privacy Act may recognise that this is a similar process to determining what constitutes 'reasonable steps' to meet obligations under APP 1.2 and APP 11.

Outsourced service provider information security capability

12.53 Where an accredited data recipient uses an outsourced service provider to provide goods or services to a consumer, the accredited data recipient must ensure their contract with the outsourced service provider requires them to take the steps outlined in Schedule 2 as if the outsourced service provider were an accredited data recipient.[22]

12.54 To comply with this requirement, accredited data recipients may consider the following when engaging an outsourced provider:

- assessing whether the information security capabilities of the outsourced service provider, having regard to the nature of the goods or services provided in relation to

[22] CDR Rule 1.10(2)(b)(i).

CDR data, comply with the information security capabilities set out in Part 1 of the CDR Rules and the security controls set out in Part 2 of the CDR Rules

- requesting and reviewing information from the outsourced service provider such as vulnerability and penetration testing reports, internal audit reports, and other information security assessments and questionnaires, and
- including contractual provisions regarding security capability reflecting the definition of a CDR outsourcing arrangement in the CDR Rules.[23]

Reviewing security capability

12.55 Under the CDR Rules, an accredited data recipient must review and adjust its information security capability:

- in response to material changes to both the nature and extent of threats and its CDR data environment, or
- where no such material changes occur, at least annually.[24]

12.56 Where changes in the operations of the accredited data recipient could lead to changes in its risk posture (for example, development of new applications, migration to new infrastructure), the accredited data recipient should review its information security capability to ensure it remains fit for purpose in managing information security risks.

Step 4: implement a formal controls assessment program

Assessing the effectiveness of controls

12.57 An accredited data recipient must establish and implement a testing program to review and assess the effectiveness of its information security capability.

12.58 This testing program must be appropriate and adapted to respond to risks to information security, having regard to:

- the extent and nature of threats to CDR data that it holds
- the extent and nature of CDR data that it holds, and
- the potential loss or damage to one or more consumers if all or part of the consumer's data were to be misused, interfered with or lost, or accessed, modified or disclosed without authorisation.[25]

12.59 The extent and frequency of this testing must be commensurate with:

- the rate at which vulnerabilities and threats change
- material changes to the accredited data recipient's CDR data environment, and
- the likelihood of failure of controls having regard to the results of previous testing.[26]

---

[23] CDR Rule 1.10(2).

[24] Clause 1.5(2) of Schedule 2 to the CDR Rules.

[25] Clause 1.6(1)(a) of Schedule 2 to the CDR Rules.

[26] Clause 1.6(1)(b) of Schedule 2 to the CDR Rules.

12.60 In order to maintain accreditation under the CDR framework, an accredited person must also provide regular attestation statements and assurance reports to the Data Recipient Accreditor.[27] More information can be found in the ACCC's Supplementary Accreditation Guidelines on Information Security.

12.61 The accredited data recipient must monitor and evaluate the design, implementation and operating effectiveness of security controls relating to the management of CDR data and have regard to its CDR regime obligations and the control requirements in Part 2 of Schedule 2 to the CDR Rules.[28]

12.62 The accredited data recipient must escalate and report the results of any testing that identifies design, implementation or operational deficiencies in information security controls relevant to its CDR data environment to senior management.[29]

12.63 The accredited data recipient must ensure that testing is conducted by appropriately skilled persons who are independent from the performance of controls over the CDR data environment.[30]

12.64 The accredited data recipient must review the sufficiency of its testing program:

a. when there is a material change to the nature and extent of threats to its CDR data environment or to its CDR data environment, as soon as practicable, or

b. where no such material changes occur, at least annually.[31]

Step 5: Manage and report security incidents

12.65 An accredited data recipient must have procedures and practices in place to detect, record, and respond to information security incidents as soon as practicable.[32] More detail about maintaining these practices can be found in ACCC's Supplementary Accreditation Guidelines on Information Security.

12.66 The accredited data recipient must create and maintain plans to respond to information security incidents that could plausibly occur. These are known as CDR data security response plans.[33]

12.67 The accredited data recipient's CDR data security response plans must include procedures for:

a. managing all relevant stages of an incident, from detection to post-incident review

b. notifying CDR data security breaches to the Information Commissioner and to consumers as required under Part IIIC of the Privacy Act,[34] and

[27] Clause 2.1(2) of Schedule 1 to the CDR Rules.

[28] Clause 1.6(2) of Schedule 2 to the CDR Rules.

[29] Clause 1.6(3) of Schedule 2 to the CDR Rules.

[30] Clause 1.6(4) of Schedule 2 to the CDR Rules.

[31] Clause 1.6(4) of Schedule 2 to the CDR Rules.

[32] Clause 1.7(1) of Schedule 2 to the CDR Rules.

[33] Clause 1.7(2) of Schedule 2 to the CDR Rules.

[34] See the 'Notifiable Data Breach (NDB) scheme' section further below in this Chapter.

c. notifying information security incidents to the Australian Cyber Security Centre as soon as practicable and no later than 30 days after the accredited data recipient becomes aware of the security incident.[35]

12.68 The accredited data recipient must review and test its CDR data security response plans to ensure they remain resilient, effective and consistent with its obligations in relation to CDR data security breaches.

- Where there is a material change to the nature and extent of threats to the accredited data recipient's CDR data environment or to the boundaries of the accredited data recipient's CDR data environment, this review and test must be undertaken as soon as practicable.
- Where no such material changes occur, this review and test must be undertaken at least annually.[36]

Notifiable Data Breach (NDB) scheme

12.69 The Notifiable Data Breaches (NDB) provisions in Part IIIC of the Privacy Act apply to accredited data recipients as if personal information was 'CDR data'.[37]

12.70 Under the NDB scheme, accredited data recipients are required to notify affected consumers and the Information Commissioner in the event of an 'eligible data breach' under the NDB scheme.[38]

12.71 A data breach is eligible if it is likely to result in serious harm to any of the consumers to whom the information relates. Entities must conduct a prompt and reasonable assessment if they suspect that they may have experienced an eligible data breach.

12.72 For more information, see the OAIC's Notifiable Data Breaches scheme webpage.

The OAIC has developed the Data breach preparation and response guide — A guide to managing data breaches in accordance with the Privacy Act to support the development and implementation of an effective data breach response, including developing a data breach response plan. The principles and concepts from this guide are useful and applicable to CDR data security breaches.[39]

[35] Clause 1.7(3) of Schedule 2 to the CDR Rules.

[36] Clause 1.7(4) of Schedule 2 to the CDR Rules.

[37] Section 56ES of the Competition and Consumer Act.

[38] See Part IIIC, Division 3 of the Privacy Act. See generally the OAIC's Notifiable Data Breaches scheme webpage for further information.

[39] The notifiable data breaches provisions of the Privacy Act apply in the CDR regime as if personal information was 'CDR data' (see section 56ES of the Competition and Consumer Act).

PART B: Treatment of redundant data (destruction and de-identification)

Overview of the process for treating redundant data

12.73 An accredited data recipient must destroy or de-identify CDR data that has become 'redundant' unless an exception applies.[40] Information regarding when CDR data becomes 'redundant', as well as the exceptions to the requirement to destroy or de-identify redundant data, are discussed below at 'What is 'redundant data'?' and outlined in the flow chart beneath paragraph 12.76.

12.74 Once CDR data is redundant, the steps an entity must take to determine whether to destroy or de-identify the CDR data are set out in the CDR Rules and explained under the heading 'Deciding how to deal with redundant data' below. What an accredited data recipient told the consumer during the consent phase (about how they treat redundant data) and whether the consumer has made an election to delete will be relevant to this decision, as demonstrated by the flow chart below at paragraph 12.83.

12.75 Once the accredited data recipient has determined whether to destroy or de-identify (and provided a consumer has not made an election to delete), it must follow the specific destruction and de-identification processes set out in the CDR Rules and outlined under the headings 'Steps to destroy redundant data' and 'Steps to de-identify redundant data' below.

12.76 Where the de-identification process does not apply or cannot result in de-identified information in accordance with the CDR Rules, the destruction process must be followed as outlined under the heading 'Steps to destroy redundant data' below.

[40] See Section 56EO(2)(a) of the Competition and Consumer Act.

Redundant data in the CDR regime

Whether CDR data is redundant

Do you need the CDR data for:

- **a purpose permitted under the CDR Rules**

or

- **a purpose for which you can use or disclose under the privacy safeguards?**

No

Does an exception apply that allows you to keep the redundant data?

- Are you required to retain the redundant data by or under a law or court or tribunal order

or

- Does the redundant data relate to any current or anticipated legal or dispute resolution proceedings to which you or the consumer are a party?

Yes

You are permitted to retain the redundant data, and must continue to handle the redundant data in accordance with the privacy safeguards (including by continuing to take the steps specified in the CDR Rules to protect the redundant data).

Yes

The CDR data is not redundant data. Continue to handle the CDR data in accordance with the privacy safeguards.

No

You must delete or de-identify the redundant data in accordance with the CDR Rules.

See the flowchart on deleting or de-identifying redundant data.

What is 'redundant data'?

12.77 'Redundant data' is CDR data that an accredited data recipient or designated gateway no longer needs for a purpose permitted under the CDR Rules, or for any purpose for which it is allowed to be used or disclosed under the privacy safeguards.[41]

12.78 While the expiry of a consent will automatically cause CDR data to become redundant, there are other situations where CDR data will become redundant. For example, when an accredited data recipient's accreditation is revoked or surrendered.[42]

12.79 The terms 'purpose' (in the context of redundant data) and 'required by or under an Australian law or court/tribunal order' are discussed in more detail in Chapter B (Key concepts).

12.80 Privacy Safeguard 12 requires an accredited data recipient or designated gateway to take the steps in the CDR Rules to destroy or de-identify redundant data unless:[43]

- the entity is not required to retain the data by or under an Australian law or a court/tribunal order, or
- the data does not relate to any current or anticipated legal proceedings or dispute resolution proceedings to which the entity or the consumer is a party.[44]

12.81 An accredited data recipient may request that the consumer state whether a legal or dispute resolution proceeding to which the consumer is a party is current or anticipated, and may rely on such a statement made by the consumer.[45]

12.82 A legal or dispute resolution proceeding is 'anticipated' if there is a real prospect of proceedings being commenced, as distinct from a mere possibility. A dispute resolution proceeding includes those undertaken through external dispute resolution schemes.

12.83 Within a dataset, some of the data may become redundant while other data does not. For instance, where a consumer has a number of banking accounts with a data holder, and data associated with one of those accounts is no longer needed by the accredited data recipient to provide the consumer with the requested services, that account data will become redundant data.

Risk point: Where an exception applies, entities risk keeping redundant data longer than they need to.

Privacy tip: Where, for example, laws prevent de-identification or destruction of redundant data, the entity should adopt other measures to limit privacy risks such as archiving and limiting access to those CDR data holdings. Entities should also clearly specify the law that authorises or requires the retention, how long the authorisation lasts, and the degree of information needed.

---

[41] See section 56EO(2)(a) of the Competition and Consumer Act.

[42] CDR Rule 5.23(4).

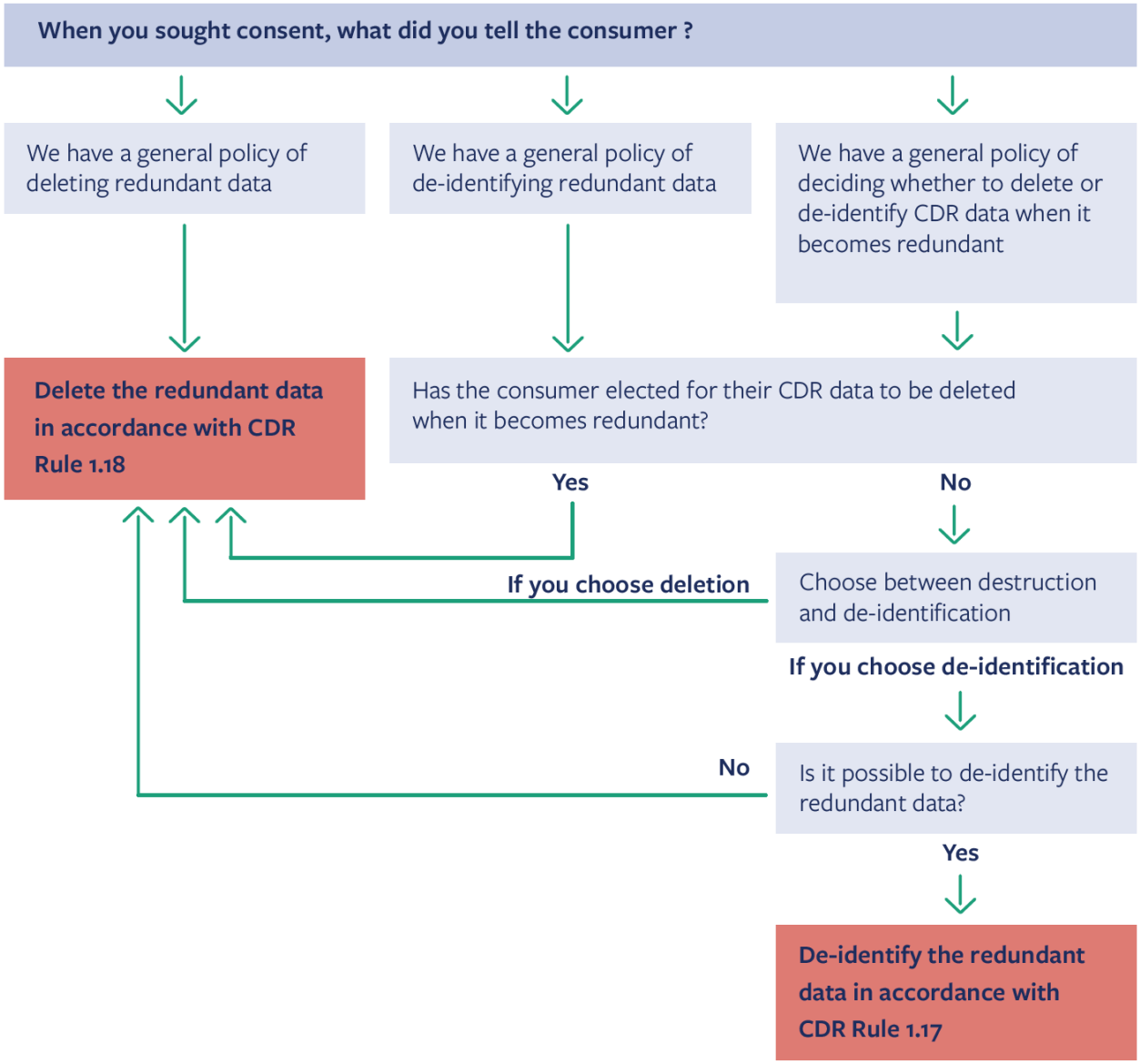
[43] See section 56EO(2) of the Competition and Consumer Act.

[44] See section 56BAA of the Competition and Consumer Act and CDR Rule 1.17A.

[45] CDR Rules 1.17(A)(2) – (3).

Deciding how to deal with redundant data

Deleting or de-identifying redundant data



Step 1: Notification to consumer of matters relating to redundant data

General policy for dealing with redundant data

12.84 When seeking consent from a consumer to collect and use their CDR data,[46] an accredited person must advise the consumer whether they have a general policy of:

- deleting the redundant data
- de-identifying the redundant data, or
- deciding whether to delete or de-identify the CDR data at the time it becomes redundant data.[47]

The consumer's right to elect for their redundant data to be deleted

12.85 If an accredited person's general policy is either de-identification or deciding between deletion and de-identification when the CDR data becomes redundant, then the accredited data recipient must allow the consumer to elect for their redundant data to be deleted.

12.86 A consumer can elect at any time for their data to be deleted when redundant. The deletion request applies to CDR data and any data derived from it (to the extent that the relevant consumer is identifiable or reasonably identifiable from the derived data). [48]

12.87 See Chapter B (Key Concepts) for further guidance about the meaning of 'derived data'.

Step 2: Consider whether the redundant data must be destroyed

12.88 In many cases, an accredited data recipient will not have the option to de-identify under the CDR Rules, and the CDR data must be destroyed.

12.89 An accredited data recipient must consider whether an exception to the requirement to destroy redundant data set out above at 'What is 'redundant data'?' applies to the redundant data. If an exception applies, the accredited data recipient must retain the CDR data while the exception applies.[49]

12.90 The CDR Rules require redundant data to be destroyed where:

- the consumer has elected for their redundant data to be deleted,
- if no election has been made, the accredited data recipient advised the consumer at the time of seeking consent that it had a general policy of deleting redundant data. Where an accredited data recipient advised the consumer of a general policy of destruction, the accredited data recipient **must destroy the redundant data**, even if their general policy has since changed, or
- it is not possible to de-identify the CDR data to the required extent (see Step 5).

---

[46] CDR Rule 4.11(3).

[47] CDR Rule 4.17(1).

[48] CDR Rule 4.16. See also 'reasonably identifiable' in Chapter B (Key concepts).

[49] CDR Rule 1.17A(2).

Step 3: If destruction isn't required, choose between destruction and de-identification

12.91 If there is 'no election to delete' in place, and the entity did not advise the consumer that it has a general approach of deleting redundant data, then the entity **can decide between destroying or de-identifying the CDR data** using the steps and processes contained in the CDR Rules and outlined below.

Step 4: Destroying redundant data

12.92 If the accredited data recipient chooses under Step 3 to destroy the redundant data, then they must proceed to destroy the data in accordance with the 'CDR data deletion process' set out in the CDR Rules.[50] This process is explained further below under the heading 'Steps to destroy redundant data'.

Step 5: De-identifying redundant data

Consider whether it is possible to de-identify the CDR data

12.93 Once an accredited data recipient has determined the de-identification process could apply, and the accredited data recipient is interested in pursuing this option, it must consider whether the CDR de-identification process will ensure that the data is de-identified in accordance with the CDR Rules.

12.94 In making this decision, an accredited data recipient must consider:

- OAIC and Data61's De-Identification Decision-Making Framework
- the techniques that are available for de-identification of data
- the extent to which it would be technically possible for **any person** to be re-identified, or be reasonably identifiable, after de-identification in accordance with such techniques, and
- the likelihood of any person becoming identifiable, or reasonably identifiable from the data after de-identification.[51]

12.95 Based on the above considerations, the accredited data recipient must determine whether it would be possible to de-identify the relevant data so that no person would any longer be identifiable, or reasonably identifiable, from:

- the relevant data after the proposed de-identification, and
- other information that would be held, following the proposed de-identification, by any person (the 'required extent').

12.96 The accredited data recipient must take into account the possibility of re-identification by using other information that may be held by **any person.** That is, whether the CDR data would be suitable for an open release environment (regardless of whether data is in fact

[50] CDR Rule 1.18

[51] CDR Rule 1.17(1).

released into an open environment, or what controls and safeguards apply to the data access environment).[52]

12.97 This is equivalent to using the De-Identification Decision-Making Framework to determine de-identification practices for open release. That is, accredited data recipients must use the De-Identification Decision-Making Framework as they would when intending to openly release de-identified information.

12.98 De-identification will be possible only where CDR data has been through an extremely robust de-identification process that ensures, with a very high degree of confidence, that no consumers are reasonably identifiable.

12.99 Accredited data recipients should be aware that there is significant complexity and risk involved with attempting to de-identify unit record data derived from CDR data to the 'required extent' as defined in the CDR Rules.

De-identifying redundant data (if de-identification is possible)

12.100 If, having taken the steps outlined in this section, the accredited data recipient determines that it is possible to de-identify the redundant data to the required extent[53], they can then proceed to de-identify the data in accordance with the 'CDR data de-identification process' set out in the CDR Rules.[54] This process is explained further below under 'Steps to de-identify redundant data'.

Destroying redundant data (if de-identification is not possible)

12.101 If, having taken the steps outlined above, the accredited data recipient determines it is not possible to de-identify the data to the required extent, the accredited data recipient must delete the CDR data and any derived data in accordance with the CDR data deletion process set out in the CDR Rules, and explained below under 'Steps to destroy redundant data'.[55]

Steps to destroy redundant data

12.102 The CDR Rules provide that the CDR data deletion process is to be applied for the purposes of destroying redundant data under Privacy Safeguard 12.[56] The CDR data deletion process is set out in CDR Rule 1.18.

12.103 This process applies:

- to the deletion of CDR data in response to a consumer's election,
- where the entity otherwise chooses to delete the redundant data in order to comply with their Privacy Safeguard 12 obligations, and

[52] CDR Rule 1.17(2)(f).

[53] See paragraphs 12.91 to 12.99.

[54] CDR Rule 1.17.

[55] CDR Rule 1.17(4).

[56] CDR Rule 7.13.

- where it is not possible to de-identify the CDR data to the required extent (see Step 5 above).

Deleting the CDR data 'to the extent reasonably practicable'

12.104 The CDR data deletion process requires the accredited data recipient to delete, 'to the extent reasonably practicable', CDR data and any copies of that CDR data.[57]

12.105 The meaning of deleting data 'to the extent reasonably practicable' depends on the circumstances, including:

- **the amount of CDR data** — more rigorous steps may be required as the quantity of data increases
- **the nature of the accredited data recipient**, and of any other entities to whom the CDR data has been disclosed (such as outsourced service providers) — relevant considerations include an accredited data recipient's size, resources and its business model
- the **possible adverse consequences for a consumer** if their CDR data is not properly deleted — more rigorous steps may be required as the risk of adversity increases
- the accredited data recipient's **information handling practices** — such as how it collects, uses and stores personal information, including whether CDR data handling practices are outsourced to third parties, and
- the **practicability, including time and cost involved** — however an accredited data recipient is not excused from deleting CDR data 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.

What if CDR data cannot practically be deleted?

12.106 The CDR Rules recognise that irretrievable destruction of CDR data such as from a back-up system or a database more generally is not always straightforward, and it may not be possible to achieve this immediately (for example, archived data that could be re-installed).

12.107 For this reason, CDR data can be put 'beyond use', if it is not actually destroyed, provided the accredited data recipient:

- is not able, and will not attempt, to use or disclose the CDR data
- cannot give any other entity access to the CDR data
- surrounds the CDR data with appropriate technical, physical and organisational security, and[58]
- commits to take reasonable steps to irretrievably destroy the data if, or when, this becomes possible.

[57] CDR Rule 1.18(a).

[58] This should go beyond the minimum access controls specified in the CDR Rules.

12.108 It is important to note that the accredited data recipient must continue to take reasonable steps to work towards a solution to eventually delete the CDR data.

Make a record to evidence the deletion

12.109 The accredited data recipient must also make a record to evidence the deletion.[59]

12.110 The accredited data recipient must also direct any other person to which it has disclosed[60] that CDR data to:

- delete, to the extent reasonably practicable, any copies of that CDR data, or any CDR data directly or indirectly derived from it, that it holds
- make a record to evidence the steps taken to delete the CDR data, and
- notify the person who gave the direction to delete.[61]

Privacy tip: If a consumer requests deletion of their redundant data but the accredited data recipient determines that it is required to retain the data under a relevant law, court/tribunal order, or because of legal or dispute resolution proceedings, the entity should notify the consumer in writing of the reasons that their request was not complied with.

Steps to de-identify redundant data

12.111 If the accredited data recipient determines that it is possible to de-identify the data to the required extent, it must determine and apply the appropriate de-identification technique (or techniques).[62]

12.112 Specifically, the accredited data recipient must:

- determine the technique/s appropriate in the circumstances
- apply that technique/s to de-identify the relevant data to the required extent, and
- delete, in accordance with the CDR data deletion process, any CDR data that must be deleted to ensure that no person is any longer identifiable or reasonably identifiable.[63]

12.113 As soon as practicable after undertaking the de-identification process, the accredited data recipient must record the process including:

---

[59] CDR Rule 1.18(b).

[60] Currently, an accredited data recipient is only authorised to disclose CDR data to an outsourced service provider or the consumer to which the CDR data relates (CDR Rule 7.5(1)).

[61] CDR Rule 1.18(c). Where the accredited data recipient has disclosed the relevant CDR data to an outsourced service provider, CDR Rule 1.18(c)(iii) requires the outsourced service provider to notify the accredited data recipient that the deletion has occurred.

[62] CDR Rule 1.17(3). This determination is a point in time assessment, i.e. with the technology available at that time rather than technology that may become available (such as quantum computing, for instance) in the future.

[63] CDR Rule 1.17(3).

- details of the assessment that it is possible to de-identify the relevant data to the required extent
- that the relevant data was de-identified to that extent
- how the relevant data was de-identified, including specifying the technique that was used, and
- any persons to whom the de-identified data is disclosed.

12.114 If the accredited data recipient determines that it is not possible to de-identify CDR data using the appropriate technique, it must delete the relevant data and any CDR data directly or indirectly derived from it.

Outsourced service providers

12.115 Accredited data recipients undertaking the de-identification process must also direct any outsourced service providers[64] to return or delete the redundant data, as well as any data directly or indirectly derived from the redundant data. [65]

12.116 Where the accredited data recipient receives redundant data from an outsourced service provider, it must de-identify the data in accordance with the CDR de-identification process, as it would with any other redundant data.

12.117 The accredited data recipient is responsible for ensuring these directions are made to any other person who has received the data. If the outsourced service provider has also disclosed the data to another person, the accredited data recipient must ensure that that person receives a direction to return or delete the data. If that person has also disclosed the data, the accredited data recipient must ensure that person receives such a direction.[66]

Other relevant security obligations

Privacy safeguards

12.118 Compliance with the privacy safeguards as a whole will promote security and reduce the risk of CDR data being accidently or deliberately compromised. This is because the privacy safeguards ensure that privacy risks are reduced or removed at each stage of CDR data handling, including collection, storage, use, disclosure, and destruction of CDR data.

12.119 Privacy Safeguard 1 requires entities to take reasonable steps to establish and maintain practices, procedures, and systems to ensure compliance with the privacy safeguards, including Privacy Safeguard 12 (see Chapter 1 (Privacy Safeguard 1)).

12.120 Privacy Safeguard 3 limits the collection of CDR data, which is an effective risk management practice reducing the scope of data that may be accessed in the case of a cyber-attack (see Chapter 3 (Privacy Safeguard 3)).

---

[64] For information on outsourced service providers, see Chapter B (Key concepts).

[65] CDR Rule 7.12(2)(b).

[66] CDR Rule 7.12(2)(b)(ii).

12.121 Privacy Safeguard 4 contains requirements to destroy information if it is unsolicited and not required to be retained by the entity (see Chapter 4 (Privacy Safeguard 4)). This minimises the amount of data held by an entity and the amount of time the entity holds that information, reducing overall risk of data breach.