

Chapter 12:

# Privacy Safeguard 12 —

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

Version 5.0, November 2023

# Contents

<b>Key points</b>	<b>3</b>
<b>What does Privacy Safeguard 12 say?</b>	<b>3</b>
<b>Why is it important?</b>	<b>4</b>
<b>Who does Privacy Safeguard 12 apply to?</b>	<b>4</b>
<b>Accreditation guidelines on information security</b>	<b>5</b>
<b>How Privacy Safeguard 12 interacts with the Privacy Act</b>	<b>6</b>
<b>PART A: Security of CDR data</b>	<b>7</b>
What do security measures need to protect against?	7
What steps does an entity need to take to secure CDR data?	8
Additional conditions on sponsors to ensure CDR data is secure	18
Notifiable Data Breach (NDB) scheme	19
<b>PART B: Treatment of redundant data (destruction and de-identification)</b>	<b>20</b>
Overview of the process for treating redundant data	20
What is 'redundant data'?	22
Deciding how to deal with redundant data	23
Steps to destroy redundant data	26
Steps to de-identify redundant data	28
<b>Other relevant security obligations</b>	<b>29</b>
Privacy safeguards	29
<b>Other CDR de-identification processes</b>	<b>30</b>

## Key points

- Securing CDR data is an integral element of the consumer data right (CDR) system.
- Privacy Safeguard 12<sup>1</sup> places requirements on accredited data recipients of CDR data 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 of CDR data or a designated gateway no longer needs the CDR data for purposes permitted by the 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 system.

## What does Privacy Safeguard 12 say?

- 12.1 Accredited data recipients of CDR data 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 of CDR data 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.<sup>2</sup> Accredited data recipients of CDR data 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 an Australian 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.

---

<sup>1</sup> Competition and Consumer Act, section 56EO.

<sup>2</sup> CDR Rules, rule 4.16.

## 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 OAI’s long-running [Australian 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 system 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 Deleting or de-identifying 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 of CDR data and designated gateways for CDR data. 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 APPs, including APP 11, in relation to the security of personal information.
- 12.10 As a non-accredited entity, a CDR representative is not directly bound by Privacy Safeguard 12. However, under the terms of the CDR representative arrangement with their CDR representative principal,<sup>3</sup> a CDR representative is required to comply with Privacy Safeguard 12 in its handling of service data as if it were the CDR representative principal.<sup>4,5</sup> A CDR representative is also required to take the steps in Schedule 2 of the CDR Rules to protect the service data as if it were the CDR representative principal.<sup>6</sup> A failure by the CDR

---

<sup>3</sup> A CDR representative arrangement is a written contract between a person with unrestricted accreditation (the CDR representative principal) and a person without accreditation (the CDR representative). The requirements for this arrangement are outlined in CDR Rules, rule 1.10AA.

<sup>4</sup> CDR Rules, paragraph 1.10AA(4)(a)(iv).

<sup>5</sup> See [Chapter B \(Key concepts\)](#) for more information on ‘CDR representative principal’, ‘CDR representative’, ‘CDR representative arrangement’ and ‘service data’.

<sup>6</sup> CDR Rules, paragraph 1.10AA(4)(b).

representative to comply with Privacy Safeguard 12 or Schedule 2 is taken to be a failure by the CDR representative principal.<sup>7</sup>

12.11 Where they are a non-accredited entity, an outsourced service provider (OSP) is not directly bound by Privacy Safeguard 12. However, under the terms of the CDR outsourcing arrangement with their OSP principal,<sup>8</sup> an OSP is required to take the steps in Schedule 2 of the CDR Rules to protect the service data as if it were an accredited data recipient.<sup>9</sup> An OSP is also required to comply with the OSP principal's CDR policy as it relates to deletion and de-identification of CDR data and the treatment of redundant or de-identified CDR data as if it were the OSP principal.<sup>10</sup> For an accredited OSP chain principal, a failure to comply with Schedule 2 in relation to service data by their direct or indirect OSP is taken to be a failure by the OSP chain principal.<sup>11</sup>

**Note:** *There are no designated gateways in the banking sector or energy sector.<sup>12</sup> See Chapter B (Key concepts) for the meaning of designated gateway.*

## Accreditation guidelines on information security

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

12.13 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 system.

12.14 Accredited persons should refer to the Supplementary accreditation guidelines: information security by the Australian Competition and Consumer Commission (ACCC)<sup>13</sup> for specific guidance on the:

---

<sup>7</sup> CDR Rules, subrules 7.11(3) and 7.12(3). A failure by any direct or indirect OSP of the CDR representative to comply with Schedule 2 is also taken to be a failure by the CDR representative principal. See also rule 1.16A in relation to a CDR representative principal's obligations and liability.

<sup>8</sup> A CDR outsourcing arrangement is a written contract between an OSP principal and their provider that meets the minimum requirements listed in CDR Rules, subrule 1.10(3).

<sup>9</sup> CDR Rules, subrule 1.10(3)(b)(ii).

<sup>10</sup> CDR Rules, paragraph 1.10(3)(b)(i)(A).

<sup>11</sup> CDR Rules, subrule 7.11(2). See also rule 1.16 in relation to an OSP principal's obligations and liability.

<sup>12</sup> For the banking sector, see the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019. For the energy sector, the energy designation specifies AEMO as a gateway for certain information: Consumer Data Right (Energy Sector) Designation 2020, subsection 6(4). However, at the time of publication, AEMO is not a designated gateway for any CDR data because under current CDR Rules, no CDR data is (or is to be) disclosed to AEMO because of the reasons in subsection 56AL(2)(c) of the Competition and Consumer Act.

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

<sup>13</sup> <https://www.cdr.gov.au/resources/guides/accreditation-guidelines>.

- information security obligations under Privacy Safeguard 12 that applicants must satisfy for accreditation under the CDR system, 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

12.15 It is important to understand how Privacy Safeguard 12 interacts with the Privacy Act and the APPs.<sup>14</sup>

12.16 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 APP Guidelines, [Chapter 11 \(APP 11\)](#)).

CDR entity	Privacy protections that apply in the CDR context
<b>Accredited data recipient</b>	<p><b>Privacy Safeguard 12</b></p> <p>For accredited data recipients of a consumer's CDR data, Privacy Safeguard 12 applies to the security of that CDR data.<sup>15</sup></p> <p>APP 11 does not apply in relation to that CDR data.<sup>16</sup></p> <p><b>Note:</b> Accredited persons must also demonstrate compliance with the information security requirements in Privacy Safeguard 12 to maintain accreditation.<sup>17</sup></p>
<b>Designated gateways</b>	<b>Privacy Safeguard 12</b>

<sup>14</sup> The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies (APP entities). See also APP Guidelines, [Chapter B \(Key concepts\)](#).

<sup>15</sup> Privacy Safeguard 12 applies from the point when the accredited person becomes an accredited data recipient of the CDR data. An accredited person becomes an accredited data recipient for CDR data when:

- CDR data is held by (or on behalf of) the person
- the CDR data, or any other CDR data from which it was directly or indirectly derived, was disclosed to the person under the consumer data rules, and
- the person is neither a data holder, nor a designated gateway, for the first mentioned CDR data. See Competition and Consumer Act, section 56AK.

<sup>16</sup> The APPs do not apply to an accredited data recipient of CDR data, in relation to that CDR data: Competition and Consumer Act, paragraph 56EC(4)(a). However, subsection 56EC(4) does not affect how the APPs apply to accredited persons and accredited data recipients who are APP entities, in relation to the handling of personal information outside the CDR system. (Note: Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See Privacy Act, subsection 6E(1D).) Subsection 56EC(4) also does not affect how the APPs apply to an accredited person who does not become an accredited data recipient of the CDR data (other than for Privacy Safeguards 1 – 4). See Competition and Consumer Act, paragraph 56EC(5)(aa).

<sup>17</sup> See the ACCC's Supplementary accreditation guidelines: information security for more information.

---

For designated gateways for CDR data, Privacy Safeguard 12 applies to the security of the CDR data.<sup>18</sup>

APP 11 does not apply in relation to that CDR data.<sup>19</sup>

---

**Data holders<sup>20</sup>**

**APP 11**

Privacy Safeguard 12 does not apply to data holders.

---

## PART A: Security of CDR data

### What do security measures need to protect against?

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

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

12.19 The terms ‘misuse’, ‘interference’, ‘loss’, ‘unauthorised access’, ‘unauthorised modification’ and ‘unauthorised disclosure’ are not defined in the *Competition and Consumer Act 2010* (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 as an exhaustive list of examples.

- **Misuse:** occurs where CDR data is used for a purpose not permitted by the CDR Rules. For example, misuse would occur if an employee of a CDR entity browses consumer statements to discover information about someone they know.<sup>21</sup>
- **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

---

<sup>18</sup> Competition and Consumer Act, subsection 56EO(1).

<sup>19</sup> The APPs do not apply to designated gateways for CDR data in relation to that CDR data: Competition and Consumer Act, paragraph 56EC(4)(d). However, subsection 56EC(4) does not affect how the APPs apply to designated gateways who are APP entities, in relation to the handling of personal information outside the CDR system. See Competition and Consumer Act, paragraph 56EC(5)(b).

<sup>20</sup> In this chapter, references to data holders include AEMO. See [Chapter B \(Key concepts\)](#) for further information about how the privacy safeguards apply to AEMO.

<sup>21</sup> Privacy Safeguard 6 sets out when an accredited data recipient of CDR data or a designated gateway for 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 \(Privacy Safeguard 9\)](#)).

leaving data in a public place, failing to keep adequate backups in the event of systems failure or as a result of natural disasters.<sup>22</sup>

- **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 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.

12.20 Information security not only covers cybersecurity (the protection of 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?

12.21 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.

12.22 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.<sup>23</sup> Additional conditions also apply to an accredited person who proposes, under a sponsorship arrangement, to become the sponsor of a person who has sponsored accreditation (the affiliate).<sup>24</sup> These conditions relate to the affiliate's information security capabilities, and are outlined below at paragraph 12.76. For more information on the sponsorship model, see Chapter B key concepts.

12.23 Broadly, the steps accredited data recipients must take to manage the information security of CDR data are:

- **Step 1:** define and implement security governance in relation to CDR data.

---

<sup>22</sup> Loss does not apply to intentional destruction or de-identification of CDR data undertaken in accordance with the CDR Rules.

<sup>23</sup> The CDR Rules currently do not detail steps for how designated gateways must comply with Privacy Safeguard 12.

<sup>24</sup> CDR Rules, clause 2.2 of Schedule 1.



- **Step 2:** define the boundaries of the CDR data environment.<sup>25</sup>
- **Step 3:** have and maintain an information security capability (including the 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.

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

12.25 The 5 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

12.26 The CDR Rules require an accredited data recipient to establish and maintain a formal governance framework<sup>26</sup> for managing information security risks relating to CDR data.

12.27 An accredited data recipient may leverage their existing information security governance structure and extend it to their CDR data environment.<sup>27</sup> An accredited data recipient may also utilise existing frameworks, requirements and models in developing their information security governance framework and defining security areas.<sup>28</sup>

12.28 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.

12.29 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.

---

<sup>25</sup> 'CDR data environment' means the information technology systems used for, and processes that relate to, the management of CDR data: CDR Rules, subclause 1.2 of Schedule 2.

<sup>26</sup> A formal governance framework refers to policies, processes, roles and responsibilities required to facilitate the oversight and management of information security.

<sup>27</sup> For further information, see the ACCC's Supplementary accreditation guidelines: information security.

<sup>28</sup> The ACCC's Supplementary accreditation guidelines: 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.

12.30 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: 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.

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

- 12.31 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.<sup>29</sup>
- 12.32 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 12.36–12.40) or as a separate document.
- 12.33 Senior management will have ultimate responsibility for the management of information security.<sup>30</sup> 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.<sup>31</sup>
- 12.34 An accredited data recipient should establish formal information security governance structures, such as committees and forums, to oversee the security of CDR data.<sup>32</sup> These committees or forums should include membership from across key business areas, particularly where the entity's CDR data environment is large or complex, 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.
- 12.35 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.

<sup>29</sup> CDR Rules, subclause 1.3(2) of Schedule 2.

<sup>30</sup> 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: CDR Rules, clause 1.2 of Schedule 2.

<sup>31</sup> The ACCC's Supplementary accreditation guidelines: information security.

<sup>32</sup> The ACCC's Supplementary accreditation guidelines: information security.

**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
- 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

12.36 An accredited data recipient must have and maintain an information security policy that governs information security across their organisation.<sup>33</sup>

12.37 The information security policy must include information about:<sup>34</sup>

- 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.

12.38 The information security policy should be internally and externally enforceable. Compliance with the policy should also be monitored.<sup>35</sup>

12.39 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.

---

<sup>33</sup> CDR Rules, subclause 1.3(3) of Schedule 2.

<sup>34</sup> CDR Rules, subclause 1.3(3) of Schedule 2.

<sup>35</sup> The term 'enforceable' is defined in the ACCC's Supplementary accreditation guidelines: information security as both internally and externally enforceable, and as 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.

12.40 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.

### Review of appropriateness

12.41 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.<sup>36</sup>

#### 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 OSP or CDR representative, or a change to the terms and conditions of the services provided by an existing OSP.<sup>37</sup>

## Step 2: Define the boundaries of the CDR data environment

12.42 An accredited data recipient must assess, define and document its CDR data environment.<sup>38</sup> 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 OSP or third-party.<sup>39</sup>

12.43 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 practices, procedures and systems are up to date.

<sup>36</sup> CDR Rules, subclause 1.3(4) of Schedule 2.

<sup>37</sup> See the ACCC's Supplementary accreditation guidelines: information security.

<sup>38</sup> See the footnote to paragraph 12.23 for the definition of 'CDR data environment'.

<sup>39</sup> See the ACCC's Supplementary accreditation guidelines: information security.

**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 collected by or disclosed to OSPs or CDR representatives. 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.

**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.

12.44 This can either be documented through a data flow diagram or a written statement.<sup>40</sup>

12.45 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

12.46 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 CDR data were to be misused, interfered with, or accessed, modified or disclosed without authorisation.

---

<sup>40</sup> For further information see the ACCC’s Supplementary accreditation guidelines: information security.

12.47 The accredited data recipient must review and adjust its information security capability as required by the CDR Rules (see paragraphs 12.62– 12.63 following).

### Information security controls

12.48 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.

12.49 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
- 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.

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

12.51 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.

12.52 Further information regarding the minimum information security controls is contained in the ACCC's Supplementary accreditation guidelines: information security.

### Additional security controls required to respond to risks to information security

12.53 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.

12.54 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.

## OSP information security capability

12.55 Where an accredited data recipient uses an OSP to:

- collect CDR data on the accredited data recipient's behalf, and/or
- provide the accredited data recipient with goods or services, using CDR data provided by the accredited data recipient,

the accredited data recipient must ensure their contract with the OSP requires them to take the steps outlined in Schedule 2 as if the OSP were an accredited data recipient.<sup>41</sup>

12.56 To comply with this requirement, accredited data recipients may consider the following when engaging an OSP:

- assessing whether the information security capabilities of the OSP, having regard to the nature of the goods or services provided in relation to CDR data, comply with the information security capabilities set out in Part 1 of Schedule 2 to the CDR Rules and the security controls set out in Part 2 of Schedule 2 to the CDR Rules
- requesting and reviewing information from the OSP 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.<sup>42</sup>

12.57 Where an accredited data recipient is an OSP chain principal, a failure by a direct or indirect OSP to comply with Schedule 2 in relation to service data is taken to be a failure by that accredited data recipient.<sup>43</sup>

12.58 Where an accredited data recipient is a CDR representative principal, and they are considering permitting their CDR representative to engage an OSP under CDR representative arrangement,<sup>44</sup> they should also consider additional terms in the arrangement to ensure their CDR representative considers the above information security capability matters when engaging an OSP.

## CDR representative information security capability

12.59 Where an accredited data recipient has a CDR representative, the accredited data recipient (CDR representative principal) must ensure their written contract with the CDR representative (CDR representative arrangement) requires the CDR representative to comply with Privacy Safeguard 12 as if it were the CDR representative principal, and take the steps outlined in Schedule 2 to protect the data as if the CDR representative were the CDR representative principal.<sup>45</sup>

---

<sup>41</sup> CDR Rules, paragraph 1.10(3)(b)(ii).

<sup>42</sup> CDR Rules, subrule 1.10(3).

<sup>43</sup> CDR Rules, subrule 7.11(2). In this circumstance, the accredited data recipient would also breach subrule 1.16(2) in relation to direct or indirect OSP's failure.

<sup>44</sup> CDR Rules, paragraph 1.10AA(3)(b).

<sup>45</sup> CDR Rules, paragraphs 1.10AA(4)(a)(iv) and 1.10AA(4)(b).

12.60 To comply with this requirement, CDR representative principals may consider the following when entering a CDR representative arrangement:

- assessing whether the information security capabilities of the CDR representative, having regard to the nature of the goods or services provided in relation to CDR data, comply with the information security capabilities set out in Part 1 of Schedule 2 to the CDR Rules and the security controls set out in Part 2 of Schedule 2 to the CDR Rules, and
- requesting and reviewing information from the CDR representative such as vulnerability and penetration testing reports, internal audit reports, and other information security assessments and questionnaires.

12.61 A failure by a CDR representative or a direct or indirect OSP of the CDR representative to comply with Schedule 2 in relation to service data is taken to be a failure by the CDR representative principal.<sup>46</sup>

### Reviewing security capability

12.62 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.<sup>47</sup>

12.63 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

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

12.65 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

---

<sup>46</sup> CDR Rules, subrule 7.11(3). In this circumstance, a CDR representative principal would also breach subrule 1.16A(2) in relation to a CDR representative's failure, and subrule 1.16(4) in relation to failure of a direct or indirect OSP of a CDR representative.

<sup>47</sup> CDR Rules, subclause 1.5(2) of Schedule 2.



- 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.<sup>48</sup>

12.66 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.<sup>49</sup>

12.67 In order to maintain accreditation under the CDR framework, accredited persons who do not have streamlined accreditation must also provide regular attestation statements and assurance reports to the Data Recipient Accreditor.<sup>50</sup> More information can be found in the ACCC's Supplementary accreditation guidelines: information security.

12.68 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 system obligations and the control requirements in Part 2 of Schedule 2 to the CDR Rules.<sup>51</sup>

12.69 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.<sup>52</sup>

12.70 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.<sup>53</sup>

12.71 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 the boundaries of its CDR data environment, as soon as practicable, or
- b. where no such material changes occur, at least annually.<sup>54</sup>

## Step 5: Manage and report security incidents

12.72 An accredited data recipient must have procedures and practices in place to detect, record, and respond to information security incidents as soon as practicable.<sup>55</sup> More detail about

---

<sup>48</sup> CDR Rules, paragraph 1.6(1)(a) of Schedule 2.

<sup>49</sup> CDR Rules, paragraph 1.6(1)(b) of Schedule 2.

<sup>50</sup> CDR Rules, subclauses 2.1(2) and (3) of Schedule 1. Accredited persons who have streamlined accreditation under rule 5.5 are not required to follow clause 2.1 of Schedule 1 to the CDR Rules: CDR Rules, subclause 2.1(1A) of Schedule 1. In the banking sector, streamlined accreditation is available where the accreditation applicant is an ADI that is not a restricted ADI: CDR Rules, subrule 5.5(b) and rule 1.7, Clause 7.3 of Schedule 3.

<sup>51</sup> CDR Rules, subclause 1.6(2) of Schedule 2.

<sup>52</sup> CDR Rules, subclause 1.6(3) of Schedule 2.

<sup>53</sup> CDR Rules, subclause 1.6(4) of Schedule 2.

<sup>54</sup> CDR Rules, subclause 1.6(5) of Schedule 2.

<sup>55</sup> CDR Rules, subclause 1.7(1) of Schedule 2.

maintaining these practices can be found in the ACCC's Supplementary accreditation guidelines: information security.

12.73 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.<sup>56</sup>

12.74 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,<sup>57</sup> and
- 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.<sup>58</sup>

12.75 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.<sup>59</sup>

## Additional conditions on sponsors to ensure CDR data is secure

12.76 Where an accredited person proposes to become the sponsor of a person that has applied, or proposes to apply, for sponsored accreditation (the affiliate), they must have a third-party management framework in place to ensure the affiliate maintains appropriate information security capabilities.<sup>60</sup>

12.77 This management framework must include requirements and activities relating to information security, including:

- due diligence prior to establishing new relationships or contracts
- annual review and assurance activities, and
- reporting requirements.

---

<sup>56</sup> CDR Rules, subclause 1.7(2) of Schedule 2.

<sup>57</sup> See the 'Notifiable Data Breach (NDB) scheme' section further below in this Chapter.

<sup>58</sup> CDR Rules, subclause 1.7(3) of Schedule 2.

<sup>59</sup> CDR Rules, subclause 1.7(4) of Schedule 2.

<sup>60</sup> CDR Rules, clause 2.2 of Schedule 1.

12.78 A sponsor must also provide the affiliate with appropriate assistance or training in relation to the steps and obligations outlined in Schedule 2 of the CDR Rules to protect the CDR data.

12.79 The sponsor of the affiliate must:

- maintain the management framework and manage its relationship with the affiliate in accordance with this framework
- provide ongoing assistance and training on technical and compliance matters, and
- take reasonable steps to ensure the affiliate complies with its obligations under Schedule 2 of the CDR Rules.

## Notifiable Data Breach (NDB) scheme

12.80 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’.<sup>61</sup>

12.81 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.<sup>62</sup>

12.82 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.

12.83 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.<sup>63</sup>

<sup>61</sup> Competition and Consumer Act, section 56ES.

<sup>62</sup> See Part IIIC, Division 3 of the Privacy Act. See generally the OAIC’s [Notifiable Data Breaches scheme webpage](#) for further information.

<sup>63</sup> The notifiable data breaches provisions of the Privacy Act apply in the CDR system as if personal information was ‘CDR data’ (see Competition and Consumer Act, section 56ES).

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

### Overview of the process for treating redundant data

- 12.84 An accredited data recipient or a designated gateway must destroy or de-identify CDR data that has become ‘redundant’ unless an exception applies.<sup>64</sup> 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 12.87.
- 12.85 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 12.94.
- 12.86 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.<sup>65</sup>
- 12.87 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.

---

<sup>64</sup> See Competition and Consumer Act, subsection 56EO(2)(a).

<sup>65</sup> Designated gateways must also take the steps specified in the CDR Rules to destroy or de-identify the redundant data: subsection 56EO(2). However, there are no designated gateways in the banking sector or energy sector. See [Chapter B \(Key concepts\)](#) for the meaning of designated gateway.

## 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’?

12.88 ‘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.<sup>66</sup>

12.89 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.<sup>67</sup>

12.90 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).

12.91 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:<sup>68</sup>

- the entity is required to retain the data by or under an Australian law or a court/tribunal order, or
- the data relates to any current or anticipated legal proceedings or dispute resolution proceedings to which the entity or the consumer is a party.<sup>69</sup>

12.92 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.<sup>70</sup>

12.93 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.

12.94 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 particular 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.

<sup>66</sup> See Competition and Consumer Act, subsection 56EO(2)(a).

<sup>67</sup> CDR Rules, subrule 5.23(4).

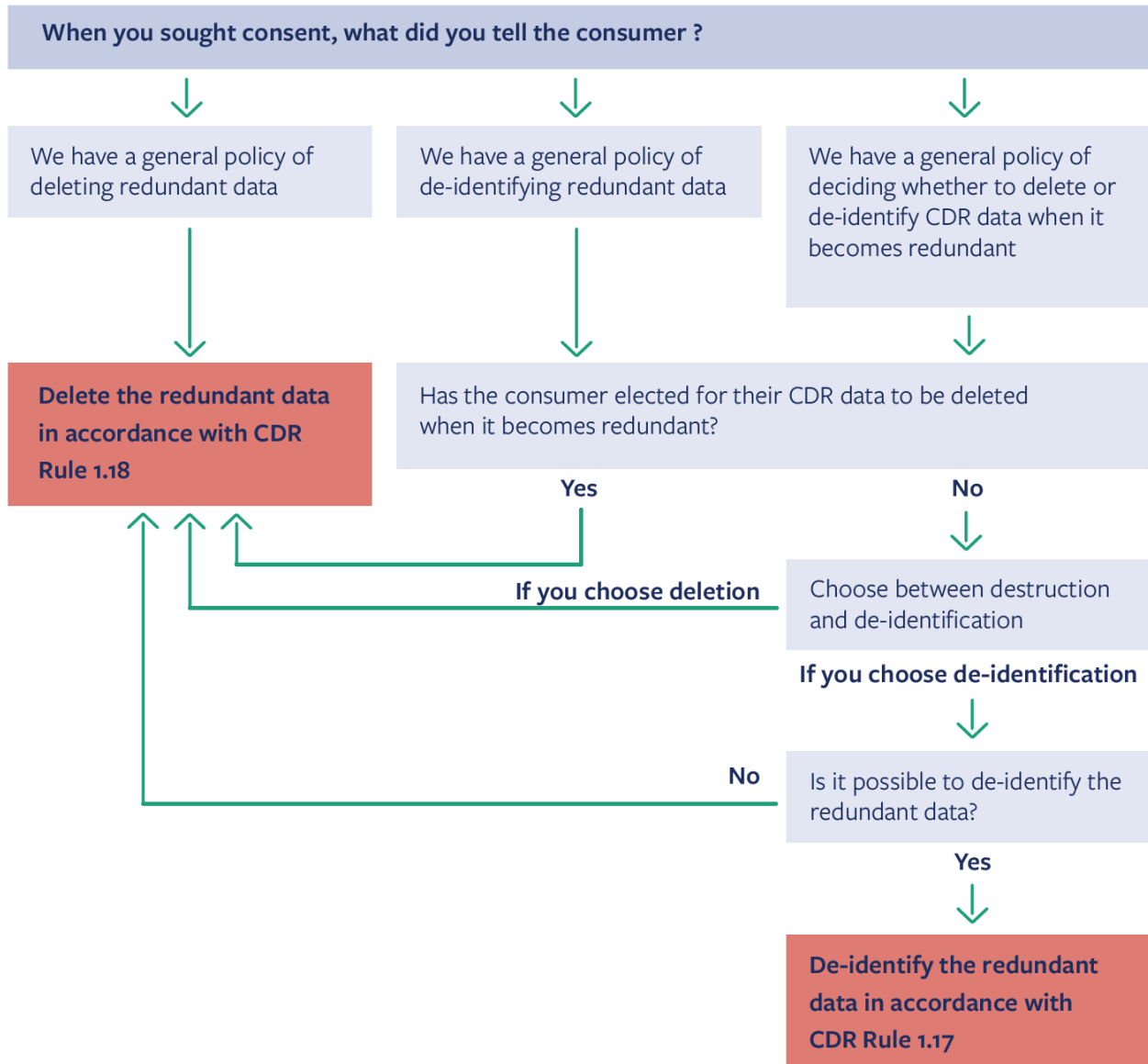
<sup>68</sup> See Competition and Consumer Act, subsection 56EO(2).

<sup>69</sup> See Competition and Consumer Act, 56BAA and CDR Rules, rule 1.17A.

<sup>70</sup> CDR Rules, paragraphs 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

12.95 When seeking consent from a consumer in relation to the handling of their CDR data,<sup>71</sup> 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.<sup>72</sup>

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

12.96 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.

12.97 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).<sup>73</sup>

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

## Step 2: Consider whether the redundant data must be destroyed

12.99 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.

12.100 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.<sup>74</sup>

12.101 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).

---

<sup>71</sup> CDR Rules, paragraph 4.11(3)(h)(i).

<sup>72</sup> CDR Rules, subrule 4.17(1).

<sup>73</sup> CDR Rules, rule 4.16. See also 'reasonably identifiable' in [Chapter B \(Key concepts\)](#).

<sup>74</sup> CDR Rules, subrule 1.17A(2).



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

12.102 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

12.103 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.<sup>75</sup> 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

12.104 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.

12.105 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.<sup>76</sup>

12.106 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').

12.107 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

---

<sup>75</sup> CDR Rules, rule 1.18

<sup>76</sup> CDR Rules, subrule 1.17(1).

released into an open environment, or what controls and safeguards apply to the data access environment).<sup>77</sup>

12.108 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.

12.109 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 persons are reasonably identifiable.

12.110 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)**

12.111 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<sup>78</sup>, they can then proceed to de-identify the data in accordance with the ‘CDR data de-identification process’ set out in the CDR Rules.<sup>79</sup> This process is explained further below under ‘Steps to de-identify redundant data’.

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

12.112 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’.<sup>80</sup>

## **Steps to destroy redundant data**

12.113 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.<sup>81</sup> The CDR data deletion process is set out in rule 1.18 in the CDR Rules.

12.114 Rule 1.18 in the CDR Rules provides that CDR data is to be deleted using the following steps:

- delete, to the extent reasonably practicable, CDR data and any copies of that data
- make a record to evidence the deletion, and

---

<sup>77</sup> CDR Rules, paragraph 1.17(2)(f).

<sup>78</sup> See paragraphs 12.102 to 12.110.

<sup>79</sup> CDR Rules, rule 1.17.

<sup>80</sup> CDR Rules, subrule 1.17(4).

<sup>81</sup> CDR Rules, rule 7.13.

- where another person holds the CDR data on behalf of an accredited data recipient and will perform the steps above (for example, an OSP), that accredited data recipient must direct that person to notify it when the steps are complete.

12.115 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
- 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'

12.116 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.<sup>82</sup>

12.117 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 OSPs) — 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?

12.118 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,<sup>83</sup> and it may not be possible to achieve this immediately (for example, archived data that could be re-installed).

---

<sup>82</sup> CDR Rules, subrule 1.18(a).

<sup>83</sup> See the CDR data deletion process in subrule 1.18(a) of the CDR Rules, which requires entities to delete CDR data and any copies 'to the extent reasonably practicable'.

12.119 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<sup>84</sup>
- commits to take reasonable steps to irretrievably destroy the data if, or when, this becomes possible.

12.120 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.

**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 Australian 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

12.121 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).<sup>85</sup>

12.122 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.<sup>86</sup>

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

- 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

---

<sup>84</sup> This should go beyond the minimum access controls specified in the CDR Rules.

<sup>85</sup> CDR Rules, subrule 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.

<sup>86</sup> CDR Rules, subrule 1.17(3).

- any persons to whom the de-identified data is disclosed.<sup>87</sup>

12.124 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.

## De-identifying data that has been provided to an OSP or CDR representative

12.125 Where an accredited data recipient has provided an OSP or CDR representative with CDR data that then becomes redundant, the accredited data recipient cannot rely on that OSP or CDR representative to undertake the de-identification process on their behalf.<sup>88</sup>

12.126 In this situation, an accredited data recipient must direct any of its direct OSPs or CDR representatives that have been provided with a copy of the redundant data to delete the redundant data, as well as any data directly or indirectly derived from it and notify the accredited data recipient of the deletion.<sup>89</sup>

12.127 If the direct OSP or CDR representative has provided the redundant data to its own direct OSP (the further recipient), the accredited data recipient must also direct its direct OSP or CDR representative to direct the further recipient to both delete the redundant data (as well as any data directly or indirectly derived from it)<sup>90</sup> and notify the accredited data recipient of the deletion.

12.128 The accredited data recipient is responsible for ensuring these directions are made, and for ensuring the data is deleted.<sup>91</sup>

12.129 Where an accredited data recipient is a CDR representative principal, a failure by the CDR representative to handle redundant data in accordance with Privacy Safeguard 12<sup>92</sup> is taken to be a failure by the CDR representative principal.<sup>93</sup>

## Other relevant security obligations

### Privacy safeguards

12.130 Compliance with the privacy safeguards as a whole will promote security and reduce the risk of CDR data being accidentally or deliberately compromised. This is because the privacy

---

<sup>87</sup> CDR Rules, paragraph 1.17(3)(d).

<sup>88</sup> For information about the meaning of OSP and CDR representative principal, see Chapter B (Key concepts).

<sup>89</sup> CDR Rules, paragraph 7.12(2)(b)(i). <sup>90</sup> CDR Rules, paragraph 7.12(2)(b)(ii).

<sup>90</sup> CDR Rules, paragraph 7.12(2)(b)(ii).

<sup>91</sup> The OSP or CDR representative is required to comply with this direction – see CDR Rules, rules 1.10 and 1.16, and 1.10AA and 1.16A.<sup>92</sup> Subsection 56EO(2) of the Act (applied as if the CDR representative were an accredited data recipient and references in subrule 7.12(1) to Division 4.3 were to Division 4.3A).

<sup>92</sup> Subsection 56EO(2) of the Act (applied as if the CDR representative were an accredited data recipient and references in subrule 7.12(1) to Division 4.3 were to Division 4.3A).

<sup>93</sup> CDR Rules, subrule 7.12(3).

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.

- 12.131 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. Privacy Safeguard 1 also requires that certain information about the deletion and de-identification of redundant data must be provided in an accredited data recipient's CDR Policy (see [Chapter 1 \(Privacy Safeguard 1\)](#)).
- 12.132 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 \(Privacy Safeguard 3\)](#)).
- 12.133 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.

## Other CDR de-identification processes

- 12.134 There are separate requirements under the CDR Rules to follow when de-identifying CDR data that is not 'redundant data'.<sup>94</sup>
- 12.135 For example, an accredited person must seek a consent from the consumer to:
- use the de-identified data for general research,<sup>95</sup> and/or
  - disclose (including by selling) the de-identified data.
- 12.136 For further information on seeking consent to use de-identified CDR data that is not redundant data, see [Chapter C \(Consent\)](#).

---

<sup>94</sup> CDR Rules, paragraph 7.5(1)(b).

<sup>95</sup> 'General research' is defined in rule 1.7 in the CDR Rules to mean research undertaken by an accredited data recipient with CDR data de-identified in accordance with the CDR Rules that does not relate to the provision of goods or services to any particular CDR consumer.