Australian Government

Consumer Data Right

Guidance for CDR representative principals on ensuring compliance of their CDR representatives

December 2023

Version Control		
December 2023	1	First version of Guide

Table of Contents

1. Introduction

1.1. Consumer Data Right

Consumer Data Right (**CDR**) gives consumers the right to require a service provider that holds their data (the **data holder**) to share that data with another service provider (the **accredited data recipient**). With the consumer's consent, the accredited data recipient may use the data to provide goods or services to the consumer or may disclose the data to another person so they can do this.

CDR aims to give consumers greater control over their data. Being able to share data easily, efficiently and securely between service providers will make it easier for consumers to compare and switch between products and services, as well as derive new benefits and efficiencies from their data. This will encourage competition between service providers, drive the development of innovative products and services, and create the potential for lower prices.

CDR is being implemented sector by sector and has commenced in the banking and energy sectors.

CDR operates under Part IVD of the *Competition and Consumer Act 2010* (Cth) (**the CCA**). The CCA sets out the CDR framework, including the privacy safeguards and the subject matter that the *Competition and Consumer (Consumer Data Right) Rules 2020* (**CDR Rules**) may cover. The CDR Rules set out the obligations that data holders, accredited data recipients and other participating entities must meet.

A glossary of common terms is published on the CDR website.

1.2. CDR representative model

The CDR representative model enables a person without accreditation (**CDR representative**) to offer goods and services to consumers using the consumer's CDR data, under a 'CDR representative arrangement' with a person with unrestricted accreditation (**CDR representative principal**).[1]

Where a CDR representative has obtained the consent of a CDR consumer to collect, use and disclose CDR data, the CDR representative principal will request the relevant data from the data holder or accredited data recipient and disclose the CDR data it obtains to the CDR representative.[2]

The requirements for a CDR representative arrangement are set out in rule 1.10AA and are outlined below in section 2. These requirements impose contractual obligations on CDR representatives which mirror provisions of the CDR Rules and Part IVD of the CCA.

Entering a CDR representative arrangement is a significant commitment for a CDR representative principal. A CDR representative principal is responsible for the conduct of its CDR representatives in the CDR ecosystem.

[1] CDR Rules, rule 1.10AA(1).

[2] CDR Rules, rule 1.10AA(1)(b).

A CDR representative principal must ensure that its CDR representatives comply with their obligations under the CDR representative arrangement and Division 4.3A of the CDR Rules.[3]

A CDR representative principal will breach the CDR Rules where its CDR representative:

- fails to comply with a 'required provision' of the CDR representative arrangement
- seeks consents for the use or disclosure of CDR data in a way not permitted by the specific CDR representative arrangement, or uses or discloses CDR data in a way that is not permitted by the specific CDR representative arrangement,[4] and
- fails to comply with requirements for giving and amending consents in Division 4.3A of the CDR Rules.[5]

This breach occurs regardless of whether the CDR representative principal knew or was aware of the CDR representative's conduct.[6]

A CDR representative principal may be subject to a range of compliance and enforcement action for such a breach including civil penalties. The substantial maximum penalty which applies in respect of such a breach reflects the importance of ensuring CDR representative principals do not enter CDR representative arrangements that would jeopardise the security, privacy and confidentiality of consumers' data, and undermine the integrity of CDR.

Where a CDR representative fails to comply with these core obligations, CDR representative principals may also be subject to the imposition of conditions on their accreditation, or revocation or suspension of their accreditation.[7] This could have serious consequences for a CDR representative principal's ability to continue to participate in CDR. There may also be a reputational risk to a CDR representative principal if consumers do not trust that the CDR representative principal can effectively manage their CDR representatives' actions to prevent harm to consumers.

For guidance on the CDR representative model more broadly, see the ACCC's CDR representatives fact sheet.

1.3. This guide

This guide has been co-produced by the Australian Competition and Consumer Commission (**ACCC**) and the Office of the Australian Information Commissioner (**OAIC**), and focuses on:

- the key requirements of a CDR representative arrangement

[3] CDR Rules, rule 1.16A.

[4] CDR Rules, rules 1.16A(2) and 1.10AA(2). Rule 1.16A(2) provides that an accredited person breaches that rule if a CDR representative fails to comply with a required provision of the CDR representative arrangement, or does one of the things in rule 1.10AA(2) in circumstances where the CDR representative arrangement does not provide for the CDR representative to do that thing.

[5] CDR Rules, rule 1.16A(4) and Division 4.3A. Rule 1.16A(4) provides that an accredited person breaches that rule if a CDR representative fails to comply with a provision of Division 4.3A.

[6] While this guidance focuses on the CDR representative principal's liability under rule 1.16A, there are other rules that impose liability on a CDR representative principal where its CDR representative fails to comply with a requirement. For example, see CDR Rules, rules 7.3(2), 7.3A, 7.6(4), 7.8A, 7.9(5), 7.10A, 7.11(2), 7.12(3) and 7.16.

[7] CDR Rules, see rules 1.16A(2), 1.16A(4), 5.10 and 5.17. Rules 1.16A(2) and 1.16A(4) are civil penalty provisions. Under section 76 of the CCA for non-body corporates the maximum civil penalty for a breach of these provisions is $500,000. For body corporates the maximum civil penalty is the greater of $10,000,000; or 3 times the value of the 'reasonably attributable' benefit obtained from the act or omission if the Court can determine this; or if the Court cannot determine the benefit, 10% of the body corporate's adjusted turnover during a specified 12-month period.

- the steps a CDR representative principal should take to ensure that its CDR representative complies with the CDR representative arrangement and the provisions in Division 4.3A of the CDR Rules.

This guide should be read together with the CDR Rules and CCA. Entities can also find more general information on CDR representative arrangements in the ACCC's CDR representatives fact sheet, the OAIC's Privacy Safeguard Guidelines and OAIC's CDR representative model guidance.

This document provides general guidance only. It does not constitute legal or other professional advice and should not be relied on as a statement of the law. It is the responsibility of each CDR participant to be fully aware of its obligations under the CDR regulatory framework. We recommend that CDR participants obtain professional advice on how the CDR framework applies to their specific circumstances. Examples in this guidance are provided for illustration only; they are not exhaustive and are not intended to impose or imply particular rules or requirements.

The ACCC and OAIC welcome feedback on this guidance via email to accc-cdr@accc.gov.au.

2. CDR representative arrangements

Rules 1.10AA(1), (3) and (4) of the CDR Rules set out the *minimum* requirements of a CDR representative arrangement.

Key requirements include that a CDR representative must, in relation to any service data:

- comply with the following privacy safeguards as if it were the CDR representative principal in holding, using or disclosing the service data:
    - privacy safeguard 2 (giving the CDR consumer the option of using a pseudonym, or not identifying themselves)
    - privacy safeguard 4 (destroying unsolicited CDR data)
    - privacy safeguard 6 (use or disclosure of CDR data)
    - privacy safeguard 7 (use or disclosure of CDR data for direct marketing)
    - privacy safeguard 8 (overseas disclosure of CDR data)
    - privacy safeguard 9 (adoption or disclosure of government-related identifiers)
    - privacy safeguard 11 (ensuring the quality of CDR data)
    - privacy safeguard 12 (security of CDR data) and
    - privacy safeguard 13 (correction of CDR data)
- take the steps in Schedule 2 to the CDR Rules to protect the service data for the purposes of complying with privacy safeguard 12 as if it were the CDR representative principal
- adopt and comply with the CDR representative principal's CDR policy in relation to the service data
- not use or disclose the service data other than in accordance with the contract with the CDR representative principal, and

- delete service data when directed to by the CDR representative principal and provide records of the deletion.[8]

Definition of service data

'Service data' in relation to a CDR representative, is CDR data that was disclosed to the CDR representative by its CDR representative principal under the CDR representative arrangement, including any data directly or indirectly derived from such CDR data.[9]

It is important for the CDR representative principal to ensure that their contract with the CDR representative meets the requirements of a CDR representative arrangement in rule 1.10AA.

3. Ensuring CDR representative compliance

3.1. Introduction – Compliance Steps

A CDR representative principal must ensure its CDR representative complies with the requirements of its CDR representative arrangement and the requirements for giving and amending consents in Division 4.3A of the CDR Rules.[10] As set out above, a CDR representative principal will breach the CDR Rules where its CDR representative fails to comply with certain provisions of the CDR representative arrangement or Division 4.3A.

3.1.1. Putting steps in place

This guide sets out steps that CDR representative principals should consider taking to manage their CDR representatives and reduce the risk of non-compliance by CDR representatives (see section 3.2).

We use the expression 'steps' in this guide to refer to the CDR representative principal's processes, procedures or arrangements for ensuring the compliance of its CDR representatives. The steps set out in this guide are intended to be general and may not be suitable for every CDR representative principal. A CDR representative principal should consider a wide range of matters when deciding which steps will be appropriate and effective to ensure compliance. For example, the specific steps which a CDR representative principal chooses to implement may be informed by the risk of non-compliance by the CDR representative. Relevant considerations might include:

- nature, scale and complexity of the CDR representative's businesses (e.g., whether the CDR representative uses outsourced service providers, whether the CDR representative has established personal information handling capabilities, practices and procedures)
- the use case of each CDR representative and the inherent risks associated with each use case, such as the possible adverse consequences for a consumer if there is a breach
- the volume and/or sensitivity of the CDR data that will be managed by each CDR representative.

[8] This is not an exhaustive list of the requirements in rule 1.10AA.

[9] CDR Rules, rule 1.10AA(5).

[10] CDR Rules, rules 1.16A(1) and 1.16A(3).

Example of good practice

Monsoon Industries has two CDR representatives:

1. Alaska Ltd is a start-up. It has new governance processes and data handling practices, and is currently building up its cyber security capability. Alaska Ltd plans to use and interact with moderate volumes of customer, account and transaction data for CDR consumers.

2. Aquaria Brokers Ltd is an established company. Aquaria Brokers Ltd is experienced with managing consumer data and has a policy of prompt deletion of this data after that data has been disclosed to the consumer. This limits the amount of CDR data held at any one time.

Monsoon Industries tailors the steps that they take to ensure and monitor compliance for the different entities based on the differences in their CDR representatives' businesses and how they are going to use and store CDR data. For example, Monsoon Industries conducts more frequent audits of Alaska Ltd's data handling practices, requires more comprehensive and frequent reports from Alaska Ltd, and provides additional training to help Alaska Ltd understand its obligations under the CDR representative arrangement.

In addition, Monsoon Industries conducts more detailed and frequent due diligence checks on Alaska Ltd such as checks with the Australian Securities and Investments Commission's banned and disqualified register and the OAIC's register of privacy determinations to identify if there are any privacy determinations. Monsoon Industries conducts these checks prior to entering into the CDR representative arrangement and periodically throughout the life of the CDR representative arrangement. See section 3.2.1 for more information.

In addition to the obligation in rule 1.16A to ensure the compliance of their CDR representatives with certain requirements, CDR representative principals must comply with Privacy Safeguard 1 which requires them to take reasonable steps to establish and maintain practices, procedures and systems to ensure compliance with Part IVD of the CCA and the CDR Rules. This includes taking reasonable steps to ensure compliance with rule 1.16A. See Chapter 1 of the OAIC's Privacy Safeguard Guidelines (open and transparent management of CDR data) for further information.

3.1.2. Recording steps

The CDR Rules require CDR representative principals to keep and maintain records that record and explain the steps they have taken to ensure that their CDR representatives comply with their requirements under the CDR representative arrangement.[11]

Records must include the date and time when the record was made and, if applicable, the date and time when the event described by the record occurred.[12]

In addition, the CDR Rules list other records that CDR representative principals must keep in relation to CDR representatives. This includes, for example, records explaining CDR

[11] CDR Rules, rule 9.3(2A)(c). This is a civil penalty provision and failure to comply may result in a civil penalty of up to $50,000 for individuals and up to $250,000 for body corporates.

[12] CDR Rules, rule 9.3(3).

consumer complaints and records explaining the management of CDR data under outsourcing service provider arrangements.

See rule 9.3(2A) for the full list of records that the CDR representative principal must keep.

Records must be kept for 6 years beginning on the day the record was created.[13]

For more guidance on the record-keeping and reporting obligations of CDR representative principals, see the ACCC's CDR representatives fact sheet.

3.1.3. Reviewing steps

A CDR representative principal should regularly review the steps in place to ensure its CDR representatives are compliant with the CDR representative arrangement. Regular reviews will help ensure the steps remain relevant and effective. In some cases, it may be appropriate to consider external review of steps in place. In particular, where compliance issues have arisen (such as major breaches or repeated compliance failures), an external compliance review may be appropriate.

A CDR representative principal should review its steps if it takes on a new CDR representative for reasons which include the following:

- the oversight that is needed for different types of CDR representatives will be different
- the risk of non-compliance, and therefore the risk to a CDR representative principal, will grow as the number of CDR representatives that it has increases
- managing a larger number of CDR representatives will increase complexity and may require additional compliance resources.

It may be necessary for a CDR representative principal to modify the steps that it takes or add additional steps to ensure that they remain relevant and effective.

A CDR representative principal should also review its steps when there are material changes to its business or its CDR representatives' businesses.[14] For example, this may be where a CDR representative plans to offer new services or change their method of service delivery or change their online platforms (e.g., a user application).

We expect that CDR representative principals will have a process for identifying changes that may impact on the effectiveness of the steps they have in place.

Example of good practice

FinTech Innovators Pty Ltd is a CDR representative principal. Some of its CDR representatives wish to introduce new use cases which would require the collection and use of more voluminous and/or sensitive CDR data.

[13] CDR Rules, rule 9.3(5). This is a civil penalty provision and failure to comply may result in a civil penalty of up to $50,000 for individuals and up to $250,000 for body corporates.

[14] Rule 5.14(1) also imposes notification obligations on an accredited person which includes notifying the ACCC within 5 business days if any material change in its circumstances occurs that might affect its ability to comply with its obligations under subdivision 5.2.3 of the CDR Rules.

FinTech Innovators' CDR representative arrangements have clauses which require the CDR representatives to:

- notify FinTech Innovators of any change in use case, and
- obtain approval from FinTech Innovators in writing before engaging any customers with that new use case.

When a CDR representative notifies it of a proposed change in use case, FinTech Innovators liaises closely with the CDR representative to make sure it has sufficient information security controls in place to safely manage the expanded dataset before it provides approval.

3.2. What the steps should cover

This section sets out steps a CDR representative principal could take before entering into a CDR representative arrangement as well as throughout the duration of a CDR representative arrangement in order to assist with compliance with its own obligations under rule 1.16A of the CDR Rules.[15]

3.2.1. Due diligence on CDR representatives

A CDR representative principal should conduct due diligence on its prospective CDR representatives. This includes checking their fitness and propriety to provide goods or services to consumers using CDR data, and keeping records of such checks.

A CDR representative principal should not rely solely on a CDR representative's self-assessment that it can participate in CDR and comply with the requirements of its CDR representative arrangement. A CDR representative principal should undertake its own risk assessment and design and implement steps to ensure the CDR representative's compliance with the CDR representative arrangement and Division 4.3A, and to assist with compliance with its own obligations under rules 1.16A(1) and (3).

While the CDR Rules do not require CDR representatives to satisfy the fit and proper criteria in rule 1.9 to participate in CDR, we expect CDR representative principals will assess their CDR representatives against similar criteria and meet with their CDR representatives to get an understanding of the business and key individuals involved in the business. Conducting such checks will help a CDR representative principal to ensure that the CDR representatives it chooses to engage:

- understand the obligations that will be placed on them under a CDR representative arrangement and can comply with these obligations
- have appropriate governance and structures to manage CDR data in accordance with the CDR representative arrangement, and
- are capable of managing and handling CDR data in accordance with the CDR representative arrangement.

[15] To avoid repetition in section 3.2, "CDR representative principals" and "CDR representatives" include *current* and *prospective* CDR representative principals and CDR representatives (e.g., where an accredited person is assessing an unaccredited entity *before* entering into a valid CDR representative arrangement with that unaccredited entity).

This will assist a CDR representative principal manage its own risk of breaching the CDR Rules due to its CDR representative breaching its obligations under the CDR representative arrangement.

Examples of fitness and propriety checks a CDR representative principal may consider undertaking include:

- searching the internet to see if there are any red flags, such as contraventions of laws or privacy concerns that suggest further investigations may be required
- checking the Australian Securities and Investments Commission's banned and disqualified register in relation to the entity's owners, directors or other key individuals associated with the entity
- checking the OAIC's register of privacy determinations to identify if there are any privacy determinations made against the entity or any key individuals associated with the entity
- checking the Australian Financial Complaints Authority's membership database to identify if there are any adverse determinations made against an entity with membership to the Australian Financial Complaints Authority, or one of its predecessors
- requesting referee reports or police checks in relation to the entity's owners, directors or other key individuals associated with the entity.

Other forms of due diligence may include:

- confirming that the CDR representative is not already in a CDR representative arrangement with another accredited person (see the CDR website's find a provider page)[16]
- considering the maturity of the CDR representative's IT systems and security, as well as the qualifications and work experience of key individuals. This may involve considering the CDR representative's history in relation to cyber and IT security. A history of breaches and unsecure practices may indicate that they are not able to safely use and disclose CDR data (unless there have been demonstrated improvements to their practices)
- considering the CDR representative's personal information handling capabilities, procedures and practices
- ensuring the CDR representative has adequate insurance in place to cover the risks associated with its use of CDR data (e.g., this may involve some combination of professional indemnity and cyber coverage)[17]
- seeking and considering information about the CDR representative's experience, capacity, and processes to handle consumer complaints (if the parties have agreed that the CDR representative will handle complaints in the first instance).

[16] A CDR representative must not enter into another CDR representative arrangement – see CDR Rules, rule 1.10AA(3).

[17] See the Supplementary accreditation guidelines on insurance. While not developed for the CDR representative model, these guidelines point towards some of the factors a CDR representative principal should consider when assessing the adequacy of a CDR representative's insurance.

Licensing or certification under different regulatory regime

A CDR representative principal should not rely solely on a potential CDR representative being certified or licenced under a different regime (such as holding an Australian Financial Services Licence). Being certified or licenced under a different regime with different requirements does not necessarily indicate that someone will hold, use and disclose CDR data securely and act in a manner to prevent consumer harm. While it may be a relevant consideration in designing appropriate steps to ensure compliance, it is unlikely to be sufficient of itself to discharge the CDR representative principal's obligations to ensure the compliance of the CDR representative.

3.2.2. Consider including additional terms in the CDR representative arrangement

To manage the risk of a CDR representative breaching key privacy obligations, and to support the CDR representative principal's compliance with its own privacy obligations, a CDR representative principal could consider including additional terms in the CDR representative arrangement (in addition to the minimum required provisions).[18]

For example:

- a term which makes clear that the CDR representative principal will not share CDR data with a CDR representative if the CDR representative principal is not satisfied the CDR representative will use and disclose it in accordance with the CDR representative arrangement.
- a term requiring the CDR representative to notify the CDR representative principal of any change in use case and to seek written approval from the CDR representative principal before engaging any customers with a new use case.
- a term requiring the CDR representative to provide the CDR representative principal with evidence that it has obtained the consents required for a 'valid request' under rule 4.3A. This will ensure that a CDR representative principal does not collect CDR data in breach of Privacy Safeguard 3 and the CDR Rules.
- if applicable (e.g., where the CDR representative principal chooses for their CDR representative to provide the dashboard), a term requiring the CDR representative to notify the CDR representative principal as soon as possible upon becoming aware that a consumer has withdrawn their collection consent or that the collection consent has otherwise expired. This will ensure that a CDR representative principal does not collect CDR data in breach of Privacy Safeguard 3 and the CDR Rules.
- a term making clear the CDR representative is prohibited from seeking and/or attempting to seek a business consumer disclosure consent.[19]
- a term requiring the CDR representative to take reasonable steps to implement practices, procedures and systems that will ensure the CDR representative complies with the terms of the CDR representative arrangement. This will assist in considering privacy when handling CDR data, resulting in better overall privacy management, practice and compliance by encouraging a 'privacy-by-design'

[18] The required provisions of a CDR representative arrangement are those set out in rules 1.10AA(1), (3) and (4).

[19] CDR Rules, rule 1.10A(1)(c)(v).

approach.[20]

- for abundance of clarity, a term prohibiting the CDR representative from collecting CDR data from any person, other than the CDR representative principal.
- a term requiring CDR representatives to seek written approval before entering into a CDR outsourcing arrangement.
- a term which prohibits the CDR representative from having any indirect outsourced service providers.
- terms providing for the consequences of non-compliance with the CDR Rules and the CDR representative agreement (e.g., termination of the arrangement).
- a term requiring the CDR representative to keep appropriate records to enable the CDR representative principal to comply with its own record-keeping requirements under the CDR Rules.[21]

For more information, see the OAIC's guidance on the privacy obligations of a CDR representative principal under the heading 'Additional terms in the written contract'.

3.2.3. Helping CDR representatives to understand and comply with their CDR representative arrangements

Given that a CDR representative principal is legally responsible for ensuring compliance by its CDR representatives and is also legally responsible for its CDR representatives' non-compliance with the CDR Rules and the CDR representative arrangement, it is in a CDR representative principal's interest to ensure its CDR representatives understand their obligations. This could include providing the CDR representative with appropriate assistance or training in relation to:

- the CDR legislative framework, including how to interpret the CDR Rules, particularly provisions that relate to CDR representatives
- the CDR representative's obligations under the CDR representative arrangement
- the CDR representative principal's compliance program and how it applies to CDR representatives
- records the CDR representative principal will require the CDR representative to keep to show that it is compliant with the CDR representative arrangement
- technical and compliance matters relating to Schedule 2 to the CDR Rules (security of CDR data).

3.2.4. Establishing a compliance program

CDR representative principals should establish a compliance program for managing their CDR representatives and their compliance with their CDR representative arrangement.

This compliance program may include:

[20] For example, the CDR representative arrangement could require the CDR representative to have a CDR data management plan. For more information, see the Privacy Tip in the OAIC's guidance for CDR representatives.

[21] For example, see rule 9.3(2A)(ka) which requires among other things, a CDR representative principal to keep records which explain any CDR outsourcing arrangement to which the CDR representative, or a direct or indirect OSP of the CDR representative, is a party.

- mechanisms (such as a systematic or documented audit process) for identifying concerns about a CDR representative
- when concerns are identified (for example, via an audit or receipt of a CDR consumer complaint), immediately taking positive steps to confirm the CDR representative's compliance position and realistically assessing the options available to deal with any potential breach and the need to report it to a government agency
- periodic reporting requirements requiring CDR representatives to report on their activities to their CDR representative principal, supported by periodic audits to verify these reports
- ongoing testing of the CDR representative's compliance with the CDR representative principal's CDR policy, and each relevant Privacy Safeguard applying under the CDR representative arrangement
- ensuring the CDR representative principal has sufficient human resources to ensure compliance (e.g., having a compliance team with staffing levels commensurate with the number of CDR representatives)
- having a framework which sets out which sections/staff are responsible for ensuring compliance
- appointing a compliance officer and ensuring the compliance officer is trained by a suitably qualified compliance professional or legal practitioner with expertise in CDR[22]
- oversight arrangements to ensure the CDR representative principal's directors or relevant boards/committees are regularly informed about the effectiveness of their compliance processes
- a mechanism to enable matters to be escalated to the CDR representative principal's directors or relevant boards/committees, when required
- obtaining appropriate external advice where required and considering and acting appropriately on such advice. This may include engaging external consultants to review and advise on the compliance program, or to advise on specific risks or issues (such as whether a particular CDR representative has sufficiently met the terms of the CDR representative arrangement).

A compliance program that only, or predominantly, relies on a CDR representative self-assessing its compliance with the CDR representative arrangement is unlikely to:

- assist a CDR representative principal to ensure the compliance of its CDR representative with the requirements of the CDR representative arrangement and Division 4.3A of the CDR Rules, and
- meet a CDR representative principal's Privacy Safeguard 1 obligations.

A CDR representative principal should consider a wide range of matters including those listed above in designing and implementing any program to help ensure the compliance of its CDR representatives.

[22] The ACCC has published guidance on implementing a business compliance program which includes four templates depending on the size of the business. While these templates were not developed specifically for CDR, CDR representative principals may wish to consider aspects of the templates depending on their business size and needs - https://www.accc.gov.au/business/compliance-and-enforcement/implementing-a-business-compliance-program

Example of good practice

Smart Solutions Ltd is a CDR representative principal.

For the first few months of being a CDR representative principal, Smart Solutions had one CDR representative and one compliance officer. In recent weeks, a significant number of companies have expressed interest in becoming CDR representatives of Smart Solutions.

In anticipation of the significant increase in CDR representatives, Smart Solutions takes steps to manage potential risks, including:

- recruiting additional and qualified compliance staff commensurate to the expected number of total CDR representatives
- preparing and maintaining training and induction material to ensure new staff can quickly implement Smart Solutions' compliance procedures and processes, and to minimise "key person" risks
- staggering the commencement of new CDR representative arrangements, if necessary, to align with the speed of recruiting additional staff (e.g., if only one additional person has been employed, it may be more appropriate to limit the number of new CDR representatives until pending recruitment activities have been finalised).

For processes and procedures to work effectively in practice, the CDR representative principal's staff, contractors and agents (particularly those involved in the management of CDR data) need to understand them and be committed to their success. Incorporating the processes and procedures into the culture of the CDR representative principal's business helps ensure they are effective on an ongoing basis.

Example of good practice

To ensure awareness of policies and procedures, and to incorporate these into the culture of the business, a CDR representative principal should:

- ensure new staff are aware of policies and procedures by including training on, or information about, these as part of their induction
- ensure existing staff are required to attend regular refresher training every 6 – 12 months
- ensure each policy or procedure has a responsible manager/staff champion who other staff can seek guidance from or provide feedback to
- invite feedback from staff on the efficacy of policies and procedures and be open to making changes in response to this feedback
- have clear success measures to enable reporting and monitoring against policies

and procedures

- conduct regular reviews of policies and procedures to ensure they are up to date, particularly when significant developments occur (e.g., the CDR Rules or CCA are amended).

3.2.4.1. Considerations relevant to service data protection

A CDR representative is required to take the steps in Schedule 2 to the CDR Rules to protect service data as if it were the CDR representative principal.[23] Schedule 2 is comprised of two parts. Part 1 concerns governance requirements for information security and Part 2 concerns the minimum information security controls to be maintained (see below table for an overview of the requirements of these Parts).

Application to CDR Data Environment	
Part 1 (governance)	**Part 2 (control requirements)**
Step 1: Define and implement security governance in relation to CDR data	Limit the risk of inappropriate or unauthorised access to the CDR data environment.
Step 2: Define the boundaries of the CDR data environment	Secure network and systems within the CDR data environment.
Step 3: Have and maintain an information security capability	Securely manage information assets within the CDR data environment over their lifecycle.
Step 4: Implement a formal controls assessment program	Implement a formal vulnerability management program to identify, track and remediate vulnerabilities within the CDR data environment in a timely manner.
Step 5: Manage and support security incidents	Limit, prevent, detect, and remove malware in regard to the CDR data environment. Implement a formal security training and awareness program for all personnel interacting with CDR data.

Additional appropriate steps may include:

- 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
- ad hoc checks and audits on the operating effectiveness of particular information security controls in Part 2 of Schedule 2

[23] 'Service data' in relation to a CDR representative is defined under rule 1.10AA(5) and refers to CDR data disclosed to a CDR representative by its CDR representative principal for the purposes of the CDR representative arrangement, including any data directly or indirectly derived from such CDR data.

- considering how the ACCC's resources on information security could be applied to assess or monitor a CDR representative's compliance with Schedule 2. More information about key resources and how they may assist is set out below.

ACCC Resource	Description
Supplementary guidelines on information security	These guidelines are intended to assist applicants for accreditation and accredited persons to meet the CDR Rules information security obligation. We do not expect a CDR representative principal's assessment of its CDR representative's compliance with Schedule 2 to be as stringent or the same as the ACCC's assessment of accreditation applicants. However, these guidelines can be used by a CDR representative principal to help inform the steps it takes when assessing a CDR representative's compliance with Schedule 2, and the issues to consider (which may prompt further investigation) during its assessment process. These guidelines also identify where meeting other common frameworks (such as PCI-DSS and ISO 27001) would be sufficient evidence of compliance with Schedule 2 obligations and where there are gaps that would need to be addressed by other evidence. For example: • does the CDR representative understand what they are required to do under Parts 1 and 2 of Schedule 2? • if a CDR representative has ISO 27001 certification, has the CDR representative principal considered the need to seek other evidence from the CDR representative to address gaps between that certification and the Schedule 2 requirements?[24]
Accreditation controls guidance	This guidance includes a mapping of controls from Part 2 of Schedule 2 against three broadly used standards/frameworks (ISO 27001, PCI DSS and Trust Services Criteria). This may assist in assessing alignment with Schedule 2 where a CDR representative is already certified against one of those standards/frameworks. This guidance also provides additional information on the controls in Part 2 of Schedule 2, and can be used by:

[24] See section 3.2 of the Supplementary accreditation guidelines on information security.

ACCC Resource	Description
	• CDR representative principals to assist when assessing a CDR representative's compliance; and • CDR representatives to ensure they have implemented these controls, and to assist with the completion of any self-assessment of their compliance.
Sponsored accreditation self-assessment and attestation form	Applicants seeking accreditation at the sponsored level and persons accredited at the sponsored level must complete and provide a self-assessment and attestation form to the ACCC to demonstrate their compliance with Schedule 2 requirements. Accredited persons may consider adopting a similar approach for their CDR representatives (e.g., requiring CDR representatives to complete a self-assessment form addressing the requirements in Schedule 2). It is important that CDR representative principals also critically assess the responses provided in the form and seek further information where necessary. This approach may be more appropriate for smaller or newer organisations who may not have existing information security certifications to demonstrate compliance with Schedule 2. The form includes test procedures which entities can conduct to test the design and implementation of their information security controls (see sheet C3A), as well as the operating effectiveness of those controls (see sheet C3B). As noted above, the form is used by applicants seeking accreditation at the sponsored level and persons accredited at the sponsored level. Accordingly, not all aspects of the form will be relevant, and CDR representative principals should adjust the wording, questions and structure of the form to suit their assessment process for their CDR representatives.

A CDR representative principal may also want to consider using the Australian Cyber Security Centre's resources to supplement its processes and procedures for assessing its CDR representatives' compliance.[25] Chapter 12 of the OAIC's Privacy Safeguard Guidelines also includes steps that an accredited data recipient must take to protect CDR data from

[25] https://www.cyber.gov.au/resources-business-and-government

misuse, interference and loss, as well as unauthorised access, modification and disclosure.[26]

These resources could be used by a CDR representative principal to help its CDR representatives to understand the information security requirements. For example, the Australian Cyber Security Centre's Information Security Manual includes a chapter titled Cyber Security Terminology which provides a glossary of information security terminology.[27]

Example of poor practice

Tech Trends Inc. is a CDR representative principal. Money Matters Pty Ltd wishes to become Tech Trends' CDR representative.

Money Matters has an Australian Credit Licence and indicates to Tech Trends that this is sufficient evidence of its ability to comply with the information security requirements in Schedule 2 to the CDR Rules.

Tech Trends agrees to enter into a CDR representative arrangement with Money Matters on the condition that Money Matters must provide evidence of its current Australian Credit Licence upon request.

Tech Trends considers this step to be sufficient to ensure Money Matters' compliance with its obligations under the CDR representative arrangement. This is despite not having considered whether there are any information security requirements associated with an Australian Credit Licence and, if so, whether they align with the requirements in the CDR Rules.

3.2.4.2. Considerations relevant to the use of outsourced service providers

CDR representatives can engage outsourced service providers (OSP), where this is allowed under the CDR representative arrangement.[28]

A CDR representative's OSP may use or disclose CDR data to provide specified goods or services to the CDR representative.[29] However, CDR representatives are precluded from conducting data collection activities or engaging an OSP to do so.[30]

To engage an OSP, the CDR representative must enter into a 'CDR outsourcing arrangement' which is a written contract between the CDR representative (who becomes the 'OSP principal' in this arrangement) and another person (the 'provider' in this arrangement).[31]

If an OSP provider (the first provider, or 'direct OSP') engages another OSP provider (the second provider, or 'indirect OSP') in a further CDR outsourcing arrangement, the first

[26] https://www.oaic.gov.au/consumer-data-right/consumer-data-right-guidance-for-business/consumer-data-right-privacy-safeguard-guidelines/chapter-12-privacy-safeguard-12-security-of-cdr-data-and-destruction-or-de-identification-of-redundant-cdr-data

[27] https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-terminology

[28] CDR Rules, rules 1.10 and 1.10AA(3)(b).

[29] CDR Rules, rules 1.10(3)(a)(ii) and (4).

[30] CDR Rules, rule 1.10AA(1)(b) and note to rule 1.10AA(3)(b).

[31] CDR Rules, rule 1.10(3).

provider would become the 'OSP principal' of the further CDR outsourcing arrangement. The CDR representative would become the 'OSP chain principal' in these arrangements. These CDR outsourcing arrangements can apply repeatedly.[32]

Any use or disclosure of service data by a direct or indirect OSP of an accredited person's CDR representative is taken to have been by the accredited person (i.e., the CDR representative principal).[33] This means that if the use or disclosure of the service data is non-compliant with the CDR outsourcing arrangement, the CDR representative principal is liable and may be subject to a range of compliance and enforcement action.[34]

As such, a CDR representative principal should take steps to:

- ensure its CDR representatives' CDR outsourcing arrangements comply with the CDR Rules (e.g., providing information on the 'required provisions' of a CDR outsourcing arrangement and conducting regular audits of CDR outsourcing arrangements to ensure compliance)[35]
- clearly state in the CDR representative arrangement any terms that the CDR representative must adhere to when engaging a direct OSP and any indirect OSPs – this could include for example, terms which limit the number of direct OSPs and/or indirect OSPs[36]
- ensure the CDR representative arrangement expressly prohibits the CDR representative from engaging an OSP, if the CDR representative principal does not intend for this to happen[37]
- ensure its CDR representatives are actively monitoring compliance of their direct and indirect OSPs with these CDR outsourcing arrangements, and are informing the CDR representative principal of any new direct OSPs they engage, as well as any indirect OSPs that are engaged further down the chain
- ensure CDR representatives are providing adequate support and training to direct and indirect OSPs to ensure they understand and are able to comply with their obligations under the relevant CDR outsourcing arrangement
- ensure it keeps its CDR policy up to date by listing all direct and indirect OSPs of the CDR representative.[38]

A CDR representative principal must keep records which explain the steps it and its CDR representatives have taken to ensure that each CDR representative's direct or indirect OSP complies with the requirements of the relevant CDR outsourcing arrangement, including how their direct OSPs ensure compliance by indirect OSPs.[39]

---

[32] CDR Rules, see note to rule 1.10(1)(c).

[33] CDR Rules, rule 7.6(2).

[34] The CDR representative principal is also liable where a direct or indirect OSP of their CDR representative fails to comply with privacy safeguards 4 (destruction of unsolicited data), 8 (overseas disclosure) and 9 (government related identifiers) as if it were an accredited person. See CDR Rules, rules 7.3B and 7.8B.

[35] CDR Rules, see rules 1.16(6) and 1.10(3) for the meaning of 'required provision' for CDR outsourcing arrangements.

[36] CDR Rules, rule 1.10AA(3)(b). Under this rule, the CDR representative arrangement must require the CDR representative not to engage a person as the provider in a CDR outsourcing arrangement except as provided in the CDR representative arrangement.

[37] As above.

[38] CDR Rules, rule 7.2(4)(f).

[39] CDR Rules, rule 9.3(2A)(ka).

Example of good practice

Financial Focus Ltd is a CDR representative principal of several CDR representatives.

As a general rule, Financial Focus' CDR representative arrangements require the CDR representatives to seek written approval before entering into a CDR outsourcing arrangement.

For CDR representatives that present a higher risk (e.g., a newly established business or a business that will be managing high volumes of sensitive service data), Financial Focus decides to add a further term in the CDR representative arrangement which prohibits the CDR representative from having any indirect OSPs.

3.2.5. Ongoing monitoring of CDR representatives

A CDR representative principal should regularly monitor, review and document its CDR representative's compliance with the CDR representative arrangement (e.g., through a compliance program). This process will then feed into any future actions that are needed to improve the CDR representative's maturity and/or reduce the risk of non-compliance.

For example, a CDR representative principal should continue to screen, test and monitor its CDR representative's:

- CDR use cases
- consent flows
- compliance with the data minimisation principle
- treatment of redundant or de-identified CDR data
- consumer complaint trends
- use of OSPs.

A CDR representative principal should also continue to carry out due diligence checks for its CDR representatives throughout the life of the CDR representative arrangement.

The level and frequency of review should be proportionate to the nature, scale and complexity of the CDR representative's business and the risk of non-compliance.

For example, more detailed and frequent checks may be more appropriate where the entity is relatively small, unknown, has low levels of governance or business maturity, and/or is not already subject to similar professional or regulatory oversight. The CDR representative principal may wish to schedule in advance the frequency and level of any planned review of its CDR representatives.

The nature/number of CDR consumer complaints received about a particular CDR representative may also indicate that a CDR representative principal should:

- conduct more frequent and stringent checks
- help the CDR representative to take corrective and preventive action to address the issues raised in the complaints, and/or

- consider termination of the CDR representative arrangement if these issues are not addressed in a timely and satisfactory manner.[40]

[40] The CDR representative principal is responsible for handling CDR consumer complaints in line with its internal dispute resolution process, which must meet the 'internal dispute resolution requirements' set out in the CDR Rules (see clause 5.1, Schedule 3 for the banking sector and clause 5.1, Schedule 4 for the energy sector). For more information about CDR consumer complaints in the context of CDR representative arrangements, see the ACCC's CDR representatives fact sheet.