USING THE OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER (OAIC) CDR PRIVACY SAFEGUARD GUIDELINES AS A FAQ

There is a lot of reading to do if you want to receive and use Consumer Data Right (CDR) data for Open Banking or Open Energy. Regardless of whether you are an ADI or non-ADI, unrestricted Accredited Data Recipient (ADR), sponsor, affiliate, representative agent or an outsourced service provider (OSP) you must demonstrate compliance with information security requirements in Privacy Safeguard 12 (Schedule 2 Part 1 and Part 2).

Some examples of readings are:

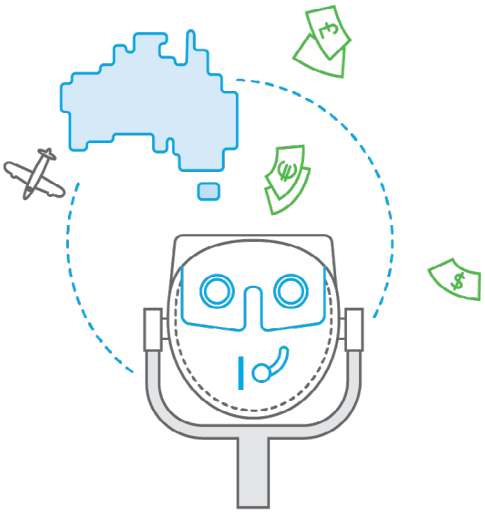
- **The Treasury Laws Amendment – Consumer Data Right Act 2019 (110 pages)**
- **The Competition and Consumer – Consumer Data Right Rules 2020 (160 pages)**
- **The OAIC Consumer Data Right (CDR) Privacy Safeguard Guidelines (234 pages)**
- **The ACCC Supplementary Accreditation Guidelines – Information Security (26 pages)**

That is over 500 pages of regulatory content (never mind the additional supporting information at:

- **http://cdr.gov.au**
- **http://cdr-support.zendesk.com**
- **http://treasury.gov.au/consumer-data-right**
- **https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0**
- **http://oaic.gov.au/consumer-data-right**
- **http://consumerdatastandards.gov.au**

Content on the websites could be consolidated by the various agencies to reduce duplication and make it easier for an ADR applicant to understand their obligations. There is lots of complementary, duplicated and unfortunately some contradictory information in the various CDR documents.

This article will only focus on the recently updated **OAIC Consumer Data Right (CDR) Privacy Safeguard Guidelines** (v3.0 June 2021). It focuses on information that is useful for an ADR applicant to comply with the information security requirements (Privacy Safeguard 12 and Schedule 2 of the Rules), whilst also repositioning the guidelines as an easier to digest FAQ.



As you can imagine, due to the vast volume of information, it is critical for anyone seeking to become an Accredited Data Recipient to engage with the right subject matter experts.

The key points highlighted below are based on the common questions that applicants have raised with RSM over the past year of CDR being live (based on the current version of the CDR Rules, v2). This is, however, no substitute for talking through your own use case, data flows, system architecture and information security controls with an experienced CDR assurance provider.

RSM

References below to sections in the OAIC Consumer Data Right (CDR) Privacy Safeguard Guidelines are denoted by a letter.number e.g., A.01 or letter.letter e.g., 10.11. Many of the references are copied verbatim from the guidelines.

1. What CDR data can an ADR collect and use?

B.105 The data minimisation principle (CDR Rule 1.8) limits the scope and amount of CDR data an accredited person may collect and use.

4.5 Privacy Safeguard 4 requires accredited persons to destroy (or de-identify) CDR data they have collected but not requested, unless an exception applies.

2. When do the information security requirements apply?

A.12 The privacy safeguards only apply to CDR data for which there are one or more 'CDR consumers'. A CDR consumer can be an individual or a business enterprise (this is different to the Privacy Act, where a consumer would only be an individual).

A.14 The privacy safeguards do not apply where there is no CDR consumer because, for example, there is no person that is identifiable or reasonably identifiable from the data. Product data is an example of CDR data for which there is no CDR consumer.

B.16 'CDR data' is information that is within a class of information specified in the designation instrument for each sector, derived from the above information ('derived CDR data').

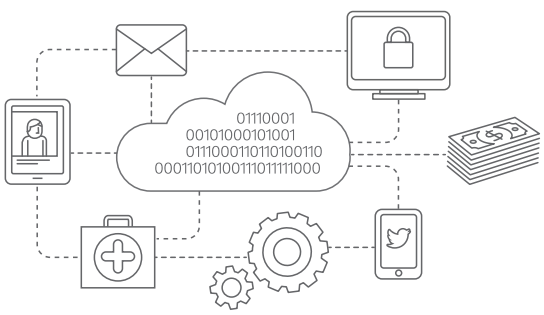
B.17 'Derived CDR data' is data that has been wholly or partly derived from CDR data, or data derived from previously derived data. This means data derived from 'derived CDR data' is also 'derived CDR data'.

B.57 By using the broad phrase 'relates to', the CDR regime captures meta-data. This includes meta-data of the type found not to be 'about' an individual for the purpose of the Privacy Act.

3. What is the threshold for de-identification?

Rule 1.17(2)(f) states:

> *"...the accredited data recipient must consider whether... it would be possible to de-identify the relevant data to the extent (the required extent) that no person would any longer be identifiable, or reasonably identifiable, from...other information that would be held, following the completion of the de-identification process, by* **any** *person."*, whereas **Act 56AI(3)(c)(ii)** refers to the relevant entity.



The difference between being able to be re-identified by any person compared to the relevant entity is a small but very important difference for potentially sharing de-identified CDR data with unaccredited parties e.g. ADR customers or outsourced service providers. Unfortunately, the OAIC CDR Privacy Safeguard Guidelines do not help to clarify this and instead ends up making things even more confusing for an ADR, as it uses in different sections any person and the relevant entity as the threshold for de-identification.

Per A.30, B.43 and B.47, for a person to be a 'CDR consumer' that person must be identifiable, or 'reasonably identifiable', from the CDR data or other information held by the relevant entity (i.e. the data holder, accredited data recipient, or person holding data on their behalf). This seems to imply that each relevant entity is mutually exclusive, but is a different definition to that used in the Rules in 1.17(2)(f) and per 12.96, where the threshold for re-identification is other information that may be held by any person.

A.30 ...for there to be a CDR consumer, at least one person must be identifiable or reasonably identifiable from the CDR data or other information held by the relevant entity.

B.40 A de-identification consent is a consent given by a consumer for an accredited data recipient of particular CDR data to de-identify some or all of that CDR data in accordance with the CDR data de-identification process and use the de-identified data for 'general research', and/or disclose (including by selling) the de-identified data.

B.43 A person is a 'CDR consumer' for CDR data if each of the following four conditions are met:

- The CDR data 'relates to' the person because of the supply of a good or service to the person or an associate of the person.
- The CDR data is held by another person who is: a data holder of the CDR data, an accredited data recipient of the CDR data, or holding the data on behalf of a data holder or accredited data recipient of the CDR data.
- The person is identifiable, or reasonably identifiable, from the CDR data or other information held by the other person (the data holder, accredited data recipient, or person holding data on their behalf), and
- None of the conditions (if any) prescribed by the regulations apply to the person in relation to the CDR data.

B.47 As outlined in paragraph B.43, for a person to be a 'CDR consumer' that person must be identifiable, or 'reasonably identifiable', from the CDR data or other information held by the relevant entity (i.e. the data holder, accredited data recipient, or person holding data on their behalf).

12.96 The accredited data recipient must take into account the possibility of re-identification by using other information that may be held by any person.

RSM

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

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

4. Does CDR data need to be deidentified or deleted from back-ups?

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

12.108 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.
- Commits to take reasonable steps to irretrievably destroy the data if, or when, this becomes possible.

5. Can I only give the consumer the option for de-identification?

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

12.86 A consumer can elect at any time for their data to be deleted when redundant. The deletion request applies to CDR data and any data derived from it.

6. What is the difference between a third party provider and an outsourced service provider (OSP)? Is a managed service provider (MSP) and X-As-A-Service classified as a third-party provider or an OSP?

6.14 Examples of 'disclosure' include where an accredited data recipient:

- Shares the CDR data with another entity or individual, including a related party of the entity (subject to some exceptions).
- Publishes the CDR data on the internet, whether intentionally or not.
- Accidentally provides CDR data to an unintended recipient.
- Reveals the CDR data in the course of a conversation with a person outside the entity, and
- Displays data on a computer screen so that the CDR data can be read by another entity or individual.

B.121 An entity discloses CDR data when it makes the data accessible or visible to others outside the entity. Information will be 'disclosed' under the CDR regime regardless of whether an entity retains effective control over the data.

B.129 The CDR Rules provide that an 'outsourced service provider' is a person who is accredited and collects CDR data from a CDR participant on behalf of an accredited person under a CDR outsourcing arrangement, and/or to whom an accredited person discloses CDR data under a CDR outsourcing arrangement for the purpose of the provider providing goods or services to the accredited person.

B.133 The CDR outsourcing arrangement must require the provider to take the steps in Schedule 2 to the CDR Rules to protect service data, as if it were an accredited data recipient.

Per B.172 and B.173, in limited circumstances, providing CDR data to a third party (such as a cloud service provider) for limited purposes may be a use of data, rather than a disclosure of data. Whether the provision of CDR data constitutes a use or a disclosure needs to be considered carefully on a case-by-case basis, and depends on the specific technical arrangements in place with the third party. A use of data would result in the provider being classified as a third party provider, whereas a disclosure of data means that the provider is classified as an outsourced service provider. Examples of a disclosure are included in 6.14. An outsourced service provider must take the steps to comply with Schedule 2 on information security as if it were an ADR.

However, such a provision of data will constitute a 'use' only if the data remains encrypted at all times, and the third party does not hold or have access to the decryption keys (on the basis that the third party would be technically unable to view or access the data at all times, and there would therefore be no disclosure).

This guidance related to encryption again contradicts Rule 1.17(2)(f). If the third party could access or view unencrypted data, for example, to maintain or provide its service, then the provision of data to that third party would constitute a disclosure, and a CDR outsourcing arrangement would be required.

B.172 In limited circumstances, providing CDR data to a third party (such as a cloud service provider) for limited purposes may be a use of data, rather than a disclosure. However, such a provision of data will constitute a 'use' only if the data remains encrypted at all times, and the third party does not hold or have access to the decryption keys (on the basis that the third party would be technically unable to view or access the data at all times, and there would therefore be no disclosure).

B.173 Whether the provision of CDR data constitutes a use or a disclosure needs to be considered carefully on a case-by-case basis, and depends on the specific technical arrangements in place with the third party. If the third party could access or view unencrypted data, for example, to maintain or provide its service, then the provision of data to that third party would constitute a disclosure, and a CDR outsourcing arrangement would be required.

7. What does the ADR need to do when the consumer withdraws consent or when consent expires?

C.84 Where a consumer withdraws each of their collection, use and disclosure consents, the CDR data is likely to become redundant data that the accredited person is required to delete or de-identify in accordance with Privacy Safeguard 12 (unless an exception applies due to a requirement to retain the data for our regulatory compliance e.g. evidence of responsible lending).

8. Why can't an ADR just get consent from the consumer to share the CDR data with an unaccredited party?

6.23 CDR Rule 4.12(3) prohibits an accredited data recipient from asking a consumer to give consent to the use or disclosure of their CDR data for prohibited uses or disclosures.

9. The consumer isn't accredited, can CDR data be shared with them?

6.39 An accredited data recipient is permitted to disclose to a consumer any of their CDR data for the purpose of providing the existing goods or services.

10. How do you develop a CDR Policy?

B.21 The CDR policy must be a separate document to an entity's privacy policy. For further information on the suggested process for developing a CDR policy and the minimum requirements for what must be included, please visit **here**.

11. What does the ADR need to do if they use an outsourced service provider to collect CDR data (an intermediary)?

C.54 Where the accredited person uses an outsourced service provider to collect CDR data, or may disclose the consumer's CDR data to an outsourced service provider (including one that is based overseas), the accredited person must tell the consumer that the accredited person will use an outsourced service provider to collect CDR data and/or disclose the consumer's CDR data to an outsourced service provider, and provide the consumer with a link to the accredited person's CDR policy, noting that further information about outsourced service providers can be found in that policy.

12. What Privacy Safeguards does an outsourced service provider need to comply with?

6.46 An accredited data recipient who discloses CDR data to an outsourced service provider under a CDR outsourcing arrangement must ensure that the provider complies with its requirements under the arrangement.

6.48 The accredited data recipient should ensure that the relevant CDR outsourcing arrangement requires the outsourced service provider to adhere to the accredited data recipient's Privacy Safeguard obligations.

6.49 The contract should also provide the accredited data recipient with the appropriate level of transparency to allow them to monitor and audit the CDR outsourcing arrangement.

13. Can CDR Data be sent and stored overseas?

8.1 An accredited data recipient of a consumer's CDR data must not disclose that data to a person located overseas unless one of the following four exceptions applies:

- The overseas recipient is an accredited person.
- The accredited data recipient takes reasonable steps to ensure the overseas recipient does not breach the privacy safeguards and the overseas recipient has a CDR policy in place in relation to the CDR data.
- The accredited data recipient reasonably believes the overseas recipient is bound by a law or scheme that is substantially similar to the privacy safeguards and a consumer will be able to enforce that law or scheme in relation to the CDR data, or
- Conditions specified in the CDR Rules for overseas disclosure are met. As there are currently no CDR Rules made specifically in relation to Privacy Safeguard 8, an accredited data recipient cannot rely on this exception.

14. How does the ADR identify information security and privacy risks?

1.1 Privacy Safeguard 1 requires all CDR entities to take steps that are reasonable in the circumstances to establish and maintain internal practices, procedures and systems that ensure compliance with the CDR regime, including the privacy safeguards and CDR Rules.

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

1.39 An entity should implement risk management processes that allow identification, assessment and management of privacy risks, including CDR security risks. As part of this, accredited persons/accredited data recipients should consider their obligations to implement strong minimum information security controls under Schedule 2 to the Rules.

RSM

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

- **Misuse:** occurs where CDR data is used for a purpose not permitted by the CDR. For example, misuse would occur if an employee of a CDR entity browses consumer statements to discover information about someone they know.
- **Interference:** occurs when there is an attack on CDR data that interferes with the CDR data but does not necessarily modify its content. For example, interference would occur if there is a ransomware attack that leads to the data being locked down and ransomed.
- **Loss:** refers to the accidental or inadvertent loss of CDR data where the data is no longer accessible and usable for its purpose, or in circumstances where it is likely to result in authorised access or disclosure. Examples of loss include physical loss by leaving data in a public place, failing to keep adequate backups in the event of systems failure or as a result of natural disasters.8
- **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.

15. What policies and procedures are needed to comply with CDR information security requirements?

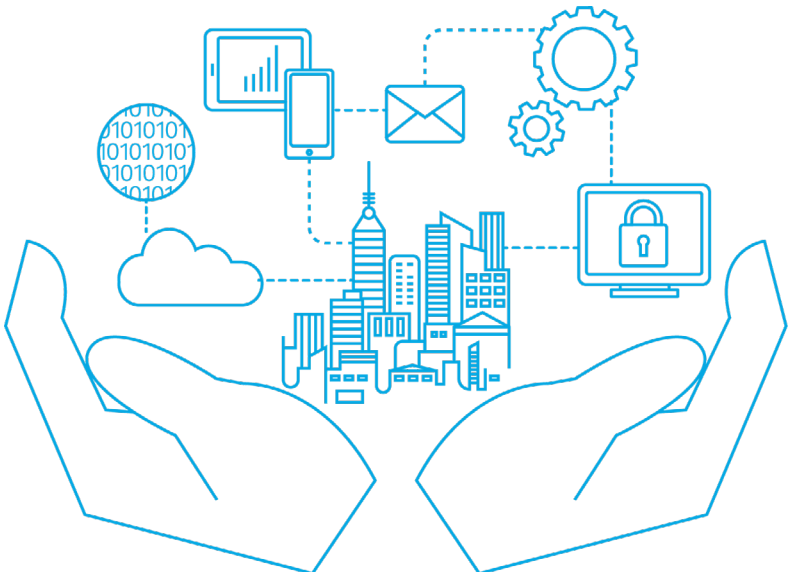
12.24 The CDR Rules require an accredited data recipient to establish and maintain a formal governance framework for managing information security risks relating to CDR data. A formal governance framework refers to policies, processes, roles and responsibilities required to facilitate the oversight and management of information security.

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

16. What needs to be included in the description of the CDR data environment?

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



17. What needs to be included in the information security incident response plan?

12.72 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.

18. What is a material change to the CDR data environment?

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

19. What do you need to do if you correct CDR data?

13.59 Where an accredited data recipient corrects CDR data to comply with Privacy Safeguard 13, it should consider whether it needs to take action under Privacy Safeguard 12 to destroy or de-identify the original data.

20. How do you comply with Privacy Safeguard 2?

2.1 Privacy Safeguard 2 provides that a consumer must have the option of not identifying themselves, or of using a pseudonym, when dealing with an accredited person (who is or who may become an accredited data recipient of the consumer's CDR data) in relation to that data.

It is very difficult to deal with a consumer on an anonymous or pseudonymous basis in CDR, as a consumer is required to provide an email address or mobile phone number to provide consent, and this is then used to provide a consent dashboard. This identifying information could theoretically be used (with other information) to identify any consumer. This removes the ability for an ADR to hold individual data that is de-identified and means that the only way to hold de-identified data is likely by summarising data about multiple consumers.

RSM Australia is a leading provider of audit, tax and consulting services to entrepreneurial growth-focused organisations. RSM Australia's CDR information security accreditation assurance experience is second to none having completed CDR information security assurance reports for 50% of the current FinTech ADRs, including Frollo, Intuit, Adatree, Finder, Basiq, Zepto and TrueLayer. RSM Australia assists ADR applicants with:

- ADR application advisory support
- CDR Control Assessment Program or ISO 27001 Lead Auditor internal audit
- CREST accredited Penetration Testing as per CDR Schedule 2 Part 2 – Vulnerability Management
- CDR Security by Design/Gap Assessment
- Defining CDR data environment boundaries
- CDR Pre-Audit/Readiness Assessment
- Independent reasonable assurance audit report (ASAE 3150/3402 or SOC 1/2) for the unrestricted ADR application
- Assurance to a sponsor that an affiliate or representative agent complies with the CDR information security requirements.

Darren Booth
Director and National Head of Cyber Security and Privacy Risk Services

E: Darren.Booth@rsm.com.au
T: +61 3 9286 8158

If you have any questions or would like to discuss how to become an Accredited Data Recipient to access Consumer Data Right (CDR) data for Open Banking or Open Energy, please get in touch with Darren Booth at **Darren.Booth@rsm.com.au.**

For further information, please also visit our website **here**.