



Australian Government



Consumer
Data Right

Supplementary accreditation guidelines: insurance

Version 2

December 2022

Table of Contents

1. Introduction.....	2
1.1. Consumer Data Right.....	2
1.2. Insurance obligation.....	2
1.3. This guideline	3
1.4. More information	3
2. Adequacy of insurance cover	4
2.1. What does ‘adequate’ mean?	4
2.2. How will ‘adequacy’ be determined?.....	4
3. Meeting and maintaining the insurance obligation	5
3.1. Documents an applicant must provide	5
3.2. Ongoing review of policies	5
3.3. Audit.....	5
4. Insurance products.....	6
4.1. Product types	6
4.2. Obtaining insurance advice	6
4.3. Scope of cover and policy terms	6

1. Introduction

1.1. Consumer Data Right

The Consumer Data Right (CDR) gives consumers the right to require a service provider that holds their personal data (**data holder**) to share that data with another service provider (**accredited data recipient**).

CDR aims to give consumers more access to and control over their personal data. Being able to share data easily and efficiently between service providers will make it easier for consumers to compare and switch between products and services. This will encourage competition between service providers, leading to more innovative products and services and the potential for lower prices.

CDR is being implemented sector by sector. Banking was the first sector to be brought into CDR. The energy sector is the next.

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

A glossary of common terms is published on the [CDR Support Portal](#).

1.2. Insurance obligation

One of the obligations that accredited persons must meet is the **insurance obligation**. Accredited persons must hold appropriate insurance, or a comparable guarantee, that is ‘adequate’ to cover the risks associated with their handling of CDR data (see section 2).

Once a person is accredited, they must continue to meet their obligations under the CDR Rules, including the insurance obligation.¹

The insurance obligation ensures that an accredited person has adequate insurance to compensate CDR consumers for any loss² that might reasonably be expected to arise from a breach of obligations under any law relevant to the management of CDR data.³

Insurance will protect the financial position of the accredited person by preserving their ability to meet their liabilities and to guard against their insolvency. If the accredited person does become insolvent, the insurance may give third-party claimants (including CDR consumers) greater protection than might otherwise be available as unsecured creditors in the insolvency.

1.2.1. Exemptions

Certain entities are exempt from the insurance obligation. These entities are authorised deposit-taking institutions (ADIs) other than restricted ADIs.⁴ All other entities must comply with the insurance obligation, including subsidiaries of ADIs.

¹ CDR Rules, rule 5.12.

² A breach of any of the following to the extent that they are relevant to the management of CDR data: obligations under the Act; any regulation made for the purposes of the Act; and the CDR Rules (CDR Rules, rule 5.12(2)(b)).

³ CDR Rules, rule 5.12(2)(b).

⁴ CDR Rules, Schedule 3, clause 7.4(2).

1.3. This guideline

This guideline supplements the [Accreditation guidelines](#) and the CDR Rules. It provides general information to applicants and accredited persons about the insurance obligation. It does not express any view on the adequacy of any particular insurance policies or arrangements.

1.4. More information

Prospective applicants can find answers to [frequently asked questions](#) (FAQs) about accreditation and applications for accreditation on the CDR Support Portal. If the applicant has a query that is not addressed in the FAQs, they should email ACCC-CDR@acc.gov.au.

2. Adequacy of insurance cover

2.1. What does 'adequate' mean?

Accredited persons are responsible for obtaining and maintaining insurance that is 'adequate'. However, there is no strict definition of 'adequate'. What is adequate for a particular accredited person will depend on a range of factors, many of which are unique to the insured.

The CDR Rules do not contain strict prescriptive requirements for insurance because those requirements may not be appropriate in all cases. A prescriptive approach might cause accredited persons to be either under-insured or over-insured, or it may diminish their flexibility to obtain insurance that is appropriate for their business.

Accredited persons will have different businesses and risks. These differences will affect what insurance cover is considered adequate. Accredited persons will need to analyse their services, products and activities to determine what is adequate for them.

Australia has a sophisticated general insurance market. Applicants for accreditation should seek advice on the appropriateness of insurance cover for their business (see section 4.2).

2.2. How will 'adequacy' be determined?

2.2.1. Factors the Accreditor will have regard to

Before granting accreditation, the Accreditor must be satisfied that the applicant will be able to comply with the insurance obligation once they are accredited.⁵

The Accreditor will consider the 'adequacy' of insurance cover in light of the objective of the insurance obligation: to reduce the risk of CDR consumers not being appropriately compensated for loss because of an accredited person's lack of financial resources.

When considering the adequacy of the insurance cover of an accredited person, the Accreditor will have regard to the scope of cover and policy terms of the accredited person's insurance (see section 4.3).

The Accreditor will also have regard to the market availability of any insurance. The Australian insurance market is dynamic, so both the scope and amount of cover available in the market may change over time. Also, the cyber insurance market in Australia is relatively new and continuing to develop.

2.2.2. Comparable guarantee

A person may hold a **comparable guarantee** that provides the same level of protection to CDR consumers as 'adequate' insurance would provide. In those cases the Accreditor will consider the person to have satisfied the insurance obligation.

A comparable guarantee must be:

- provided by a related company to the applicant or the accredited person
- provided by a company that is of substance

⁵ See section 2.2.2 of this guideline for information about applying for accreditation with a comparable guarantee.

- on terms that are appropriate in the circumstances, including with respect to the value and limitations that apply to the guarantee.

A person who is applying for accreditation using a comparable guarantee should make sure they have appropriate supporting documentation – for example:

- a statement on terms the same as those set out in section 3.1 below
- the terms of the guarantee and sufficient details about the guarantor to enable the Accreditor to consider the financial capacity of the guarantor to meet the terms of the guarantee.

3. Meeting and maintaining the insurance obligation

3.1. Documents an applicant must provide

As part of their application for accreditation, applicants must provide:

- a written statement, signed by a duly authorised representative of the applicant, that:
 - details any insurance policies it holds to meet the insurance obligation
 - explains in detail how the applicant has determined that this insurance is adequate to cover the risks they may be exposed to in their management of CDR data. Applicants should consider the matters discussed in section 4.3
- a copy of a certificate of currency for each of the relevant policies
- a copy of a policy document (or policy wording) for each of the relevant policies.

3.2. Ongoing review of policies

Accredited persons must continue to hold adequate insurance (or a comparable guarantee) for as long as they remain accredited.

To ensure their insurance continues to satisfy the insurance obligation, accredited persons should review their insurance (or their comparable guarantee) at least once every 12 months.

If the accredited person has made any major changes to their business – for example, if they provide a new product or service or if the volume of CDR data they hold or manage increases – they should ensure that their insurance or comparable guarantee remains adequate to cover their risks.

3.3. Audit

The Accreditor may conduct audits of accredited persons.

The accredited person must make sure they have appropriate documentation (such as updated certificates of currency) to satisfy the Accreditor that they continue to comply with their obligations.

4. Insurance products

4.1. Product types

The general insurance market offers a range of product types. As mentioned in section 2.1, there is no prescribed type of insurance product that must be obtained to meet the insurance obligation.

As a general guide, 2 product types that may provide the cover required to satisfy the insurance obligation are:

- Professional indemnity insurance: Although the scope of cover may differ between insurance carriers, professional indemnity insurance generally provides cover for the third-party liability of the insured entity (and certain insured persons) arising from acts or omissions in performing the professional services that the insured entity or other insured person was engaged to provide.
- Cyber insurance: This generally provides cover for certain first-party losses and third-party liabilities resulting from cyber incidents. The scope of what is covered will vary from policy to policy. Many policies available in the market cover third-party liability arising from privacy breaches and cyber incidents. These policies may include liability arising from unauthorised access or damage to the insured's data or computer systems; or from acts or omissions of the insured in connection with data. Many policies also offer incident response services. These policies usually give the insured access to response services such as IT forensic experts to identify, control and rectify the cyber incident; lawyers to advise on compliance with the notifiable data breach scheme; and public relations consultants to mitigate reputational damage.

An accredited person might need more than one policy to meet their insurance obligation. For instance, they might need to have both a professional indemnity insurance policy and a cyber insurance policy.

There may be other policy types, either in isolation or in conjunction with other insurance policies, that may satisfy the insurance obligation.

4.2. Obtaining insurance advice

Accredited persons should seek advice from competent and appropriately experienced advisers on the adequacy of cover. External consultants, advisers, actuaries or brokers will be able to assess an applicant's or accredited person's exposure and identify the appropriate insurance and policy terms to satisfy these requirements.

4.3. Scope of cover and policy terms

Accredited persons must consider which type of insurance is required to meet the insurance obligation.

Accredited persons are likely to be providing professional services that involve the receipt and use of CDR data. Therefore, the civil liability incurred in managing CDR data may need to be covered under a professional indemnity insurance policy.

Some cyber insurance policies will provide cover for third-party liability in connection with the management of CDR data. However, some policies may not cover this. For example, some policies only cover incidents where an external malicious attack (that is, a 'cyber-attack') on the insured's systems has occurred.

To ensure their cover is adequate in the circumstances, accredited persons must consider the terms of the insurance as a whole, including:

- the size of any excess or deductible
- the application of sub-limits
- any endorsements that would limit the availability of cover for claims by or on behalf of CDR consumers.

When considering whether the applicant would be able to comply with the insurance obligation, the Accreditor may consider matters set out in Table 1. The applicant should address these matters, as well as any other relevant matters, in their written statement for accreditation. Note that the matters the Accreditor may consider are not limited to those listed in Table 1.

Table 1: Adequacy of insurance: scope of cover and policy terms

Factor	Comment
Nature of the services or products provided	Accredited persons should consider whether the services or products they intend to provide are professional in nature and whether professional indemnity insurance is required.
Nature of CDR data likely to be managed	Accredited persons should consider the nature of the CDR data that they expect to receive or that they hold and ensure that the insurance cover is appropriate for the risks associated with that type of CDR data. They should be aware that certain types of CDR data may be more sensitive or may be received under the CDR more frequently.
Volume of CDR data held	Accredited persons should consider the volume of the CDR data that they hold and manage (or that they expect to hold and manage). The greater the volume of data held or managed, the greater the potential risk associated with breach of the Act, the CDR Rules or the data standards.
Financial resources	Accredited persons should consider what financial resources are required to cover the excess and any gaps in cover due to various exclusions in the insurance cover and ensure those financial resources are available.
Scope of professional indemnity cover	Accredited persons should consider the extent to which their services or products relate to the management of CDR data. The scope of services or products (professional or otherwise) covered by an insurance policy should extend to the services or products being provided with respect to CDR data. Other aspects of the insurance cover should also extend to activities related to management of CDR data.
Scope of cyber cover	Accredited persons should ensure that their cyber insurance policy covers third-party liabilities for the services or products they intend to provide and their potential risks in handling CDR data. The insurance should not contain coverage limitations that could apply to claims concerning their management of CDR data.

Factor	Comment
Scope of cover (general)	<p>The insurance should provide cover for claims made against the accredited person by or on behalf of CDR consumers for any civil liability with respect to the management of CDR data.</p> <p>Fraud/dishonesty: The policy must cover fraud/dishonesty/infidelity by officers, employees and other representatives of the accredited person. (Fraud cover is not required for sole traders or for companies that have one director who is also the company’s only shareholder and only employee of the company.)</p> <p>Retroactive cover: If the accredited person had an immediately previous similar insurance policy, the policy must provide retroactive cover to the earlier of:</p> <ul style="list-style-type: none"> • the retroactive date specified in the immediately previous similar insurance policy • the commencement date of the first insurance policy in the series of similar continuous policies.
Policy limit	<p>The applicant must consider whether the policy limit is adequate. They will need to analyse the nature of services or products they will provide and the nature and volume of CDR data they will hold or manage.</p> <p>The accredited person should ensure that their annual aggregate insurance cover for certain events is adequate to provide indemnity for CDR consumer claims made in respect to their activities.</p>
Persons covered	<p>The insurance policies must specify the accredited person as a named insured. A policy that covers corporate groups may satisfy the insurance obligation if the accredited person is named and if the accredited person is satisfied that the cover is adequate, despite the fact that the policy also applies to related companies.</p>
Exclusions	<p>The insurance must not exclude:</p> <ul style="list-style-type: none"> • <i>External dispute resolution claims:</i> Policies cannot exclude claims brought in the Australian Financial Complaints Authority (AFCA), as it is the designated external dispute resolution scheme that will apply to accredited persons. • <i>Privacy and data exclusions:</i> Policies should not exclude liability for privacy and data related claims that a CDR consumer might make against an accredited person in respect of CDR data.