Consumer Data Right

Consumer Data Right

Supplementary accreditation guidelines: insurance

DRAFT: 23 September 2019

Contents

Glossary

Term	Definition
accredited person	an accredited person is a person who has satisfied the Accreditor that it meets the criteria for accreditation specified in the CDR Rules and has been accredited by the Accreditor
ACCC	Australian Competition and Consumer Commission
Accreditor	Data Recipient Accreditor – currently the ACCC
AFCA	Australian Financial Complaints Authority
applicant	a person who makes an application for accreditation as an accredited person
ADI	authorised deposit-taking institution
CDR	Consumer Data Right
CDR consumer	CDR consumer is defined in the Act, see subsection 56AI(3)
CDR data	CDR data is specific information for the relevant designated sector. See s 56AI(1) of the Act. For the banking sector this is set out in Schedule 3 of the CDR Rules
CDR Rules	*Proposed Competition and Consumer (Consumer Data Right) Rules 2019 – August 2019*
data standards	has the meaning given to it in the Act
insurance obligation	insurance that is adequate, or a comparable guarantee, in light of the risk of CDR Consumers not being properly compensated for any loss that might reasonably be expected to arise from a breach of obligations under the Act; any regulations for the purposes of the Act; and the CDR rules to the extent that they are relevant to the management of CDR data. See CDR Rules, rule 5.12(2)(b)
the Act	*Competition and Consumer Act 2010*

1. Introduction

1.1. Overview

Under Part IVD of the *Competition and Consumer Act 2010* (**the Act**), the Consumer Data Right (**CDR**) regime will allow consumers to require data holders to share their data with accredited persons.

The Proposed Competition and Consumer (Consumer Data) Rules 2019 – August 2019 (**CDR Rules**) set out how the CDR is to operate[1] including the criteria that the Accreditor will apply when considering an application for accreditation.

Once accredited, an accredited person of CDR data will have ongoing obligations consistent with the criteria.[2] One such obligation is the insurance obligation. This requires an accredited person to have adequate insurance, or a comparable guarantee.[3]

This guideline aims to provide information and guidance to accredited persons to assist them meeting this obligation and is supplementary to the *CDR Accreditation Guidelines* and the CDR Rules.

Enquiries about applications for accreditation should be directed to the Director, Accreditation, Consumer Data Right Branch, at ACCC-CDR@accc.gov.au.

1.2. Objective of the insurance obligation

The CDR Rules require accredited persons to hold appropriate insurance, or a comparable guarantee, relevant to the nature and extent of their management of CDR data.

The objective of the insurance obligation is to ensure an accredited person has adequate insurance in light of the risk of CDR consumers not being properly compensated for any loss that might reasonably be expected to arise from a breach of obligations under any law relevant to the management of CDR data.[4]

1.3. Our approach

The ACCC has approached the insurance obligation in a principle-based rather than prescriptive manner. The ACCC requires that accredited persons obtain and maintain insurance that is 'adequate', rather than seeking to specify the precise insurance arrangements that the entity must meet. We have adopted this approach because:

- the adequacy of insurance arrangements will depend on a range of factors, many of which are unique to the insured. Imposing strict prescriptive requirements may lead to either under-insurance or over-insurance, and diminish the flexibility of accredited persons in obtaining insurance that is appropriate for their business.
- the insurance of data related liabilities requires an analysis of the individual entity's services, products and activities and different insurance products may be more suitable to different entities. A less prescriptive and more flexible approach should allow entities to obtain the type of insurance cover that is appropriate for their business, but also take advantage of product developments in the insurance market, including any specific data related insurance policies that may be developed over time.

---

1 The *Competition and Consumer Act 2010* sets out the CDR framework including the subject matter that the CDR Rules may cover.

2 CDR Rules, rule 5.12.

3 CDR Rules, rule 5.12(2)(b).

4 CDR Rules, rule 5.12(2)(b).

- Australia has a sophisticated general insurance market and those seeking to be accredited should be in a position to obtain accessible advice on the appropriateness of insurance cover for their business.

2. Adequacy of insurance cover

2.1. Requirement of adequate insurance

The question of 'adequacy' is central to the insurance obligation for accredited persons.

2.1.1. Applicants: accreditation

Before the Accreditor will grant accreditation, the Accreditor will need to be satisfied that the accreditation applicant has either adequate insurance or a comparable guarantee.

The Accreditor will require the applicant to provide the following documents as part of its application for accreditation:

- a written statement signed by a duly authorised representative of the applicant that:
    - details the insurance policy or policies, or comparable guarantee, held by the applicant that it considers satisfy the insurance obligation.
    - provides a detailed explanation of the basis on which the applicant has determined that the insurance policy or policies, or comparable guarantee, it holds are adequate to cover the liabilities it may incur in connection with the management of CDR data.
- a copy of a certificate of currency for each relevant policy.

2.1.2. Accredited persons: continuing obligations

Accredited persons are required to maintain adequate insurance (or a comparable guarantee) for as long as they remain accredited. Accredited persons should review their insurance, or their comparable guarantee, at least annually to ensure that it continues to satisfy the insurance obligation. Accredited persons should also review the adequacy of their insurance or comparable guarantee in light of any major changes to their business (e.g. If you start providing new products or services or there is an increase to the volume of CDR data that they hold or manage).

The Accreditor may conduct audits of accredited persons through an audit and compliance program. It is important that an accredited person considers the adequacy of its insurance under the CDR regime regularly, and has available appropriate documentation to satisfy the Accreditor of the accredited person's compliance with its ongoing obligations. Such documentation may include updated certificates of currency.

2.2. What is 'adequate'?

The 'adequacy' of insurance cover for accredited persons will be considered in light of the objective of the insurance obligation; namely, to reduce the risk of CDR consumers not being appropriately compensated by reason of an accredited person's lack of financial resources. The insurance acts to protect the financial position of the accredited person by preserving its ability to meet its liabilities and to guard against its insolvency. In the event of insolvency of the accredited person, the existence of insurance may provide third party claimants, including CDR consumers, with greater protection than might otherwise be available as unsecured creditors in the insolvency.

Accredited persons will have different businesses and risks, which will affect what insurance cover is adequate. Accredited persons will need to undertake their own analysis in order to

determine what is adequate for them. In considering whether the insurance arrangements of any accredited person are adequate, the Accreditor will have regard to the scope of cover and policy terms of the insurance arrangements taken out by the accredited person.

The ACCC is mindful that the Australian insurance market is dynamic, and that both the scope and amount of cover available in the market may change over time. The ACCC also acknowledges that the cyber insurance market in Australia is relatively new and continuing to develop. The Accreditor will have regard to the market availability of any insurance in considering the adequacy of the insurance obtained or maintained by an accredited date recipient.

2.2.1. Scope of cover and insurance products

The ACCC will not prescribe the insurance product types that must be obtained to meet the insurance obligation.

The general insurance market offers a range of product types. Of those readily available in the market, professional indemnity insurance and cyber insurance policies are two product types that may provide entities with the cover required to satisfy the insurance obligation. However, other liability policy types, either in isolation or in conjunction with other insurance policies, may satisfy the insurance obligation.

By way of example only:

- *professional indemnity insurance:* this class of insurance generally provides cover for civil liabilities of the insured arising from the provision of professional services. 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 the performance of the professional services which the insured entity or person was engaged to provide.
- *cyber insurance:* this class of insurance 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, and may include liability arising from an unauthorised access or damage to the insured's data or computer systems, or for acts or omissions of the insured in connection with data. Many policies also offer certain incident response services providing access to expert vendors. This usually comprises of 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.

Some accredited persons are likely to be providing professional services in connection with the receipt and use of CDR data. In such circumstances, civil liability incurred by the accredited person to CDR consumers in connection with the management of CDR data may 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 be limited by the nature of the event that gives rise to the claim. For example, cover under some policies arises only where an external malicious attack on the insured's systems has occurred (that is, a 'cyber-attack').

It is incumbent upon all accredited persons to consider which type of insurance is required to meet the insurance obligation.

The Accreditor will have regard to at least the matters set out in Table 1 below in considering whether the insurance obligation has been met. These matters should be taken into account by any accredited person when considering their compliance with the insurance obligation.

Table 1: Adequacy of insurance: business activities and types of insurance

Factor	Comment
Nature of the services or products provided	Accredited persons should consider whether the services or products they intend to provide are professional and where liability for such services or products would ordinarily be covered under a professional indemnity insurance.
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 such CDR data. Bearing in mind that certain types of CDR data may be more sensitive or may be received under the CDR regime more frequently.
Volume of CDR data held	Accredited persons should consider the volume of the CDR data that they do, or expect to, hold and manage. The greater the volume of data held or managed the greater the potential loss and damage in the event of a breach of the proposed legislation, CDR Rules or 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 such 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 any 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 and otherwise insurance cover should extend across those activities.
Scope of cyber cover	Accredited persons should ensure that third party liability in any cyber insurance policy extends to the nature of the services or products it intends to provide and the likely liability of the accredited person with respect to CDR data. Coverage should not be limited to malicious 'cyber-attacks' or contain other coverage limitations that would make it unresponsive to claim that might arise

2.2.2. Policy terms

When considering whether the insurance is adequate, the Accreditor will also have regard to at least the matters set out in Table 2 below.

Table 2: Adequacy of insurance: policy terms

Factor	Comment
Policy limit	The adequacy of the policy limit requires an analysis of the nature of services or products to be provided and the nature and the volume of CDR data held or managed by the accredited person (refer to Table 1). The accredited person should ensure that its annual aggregate insurance cover is adequate to provide an indemnity for claims made by CDR consumers in respect to its activities.
Scope of cover	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.

Factor	Comment
	Fraud/dishonesty: The policy must cover fraud/dishonesty/infidelity by officers, employees and other representatives of the accredited person (although 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). *Retroactive cover:* If the accredited person had an immediately previous similar insurance policy, the policy must provide retroactive cover to the earlier of: • 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.
Persons covered	The insurance must name the accredited person as a named insured. Policies that cover corporate groups may satisfy the insurance obligation provided the accredited person is named, and the accredited person is satisfied that the cover is adequate, notwithstanding its broader application to related companies.
Exclusions	The insurance must not exclude the following: *External dispute resolution claims:* Policies cannot exclude claims brought in Australian Financial Complaints Authority (AFCA), as it is the designated external dispute resolution scheme that will apply to accredited persons. *Privacy and data exclusions:* Policies should not exclude liability for privacy and data related claims of the nature that might be made by a CDR consumer against an accredited person in respect of CDR data.

Accredited persons must consider the terms of the insurance as a whole, and ensure that the cover is adequate in the circumstances. The size of any deductible, the application of sub-limits and any endorsements that would limit the availability of cover for claims by or on behalf of CDR consumers should be considered closely to ensure that the insurance is adequate.

2.3. Multiple policies

The insurance obligation may be met by more than one policy of insurance. For instance, cover across a professional indemnity insurance policy and a cyber-insurance policy may be considered necessary to meet the insurance obligation.

2.4. Obtaining insurance advice

Accredited persons are encouraged to seek advice on the adequacy of cover from competent and appropriately experienced advisers. External consultants, advisers, actuaries, or brokers will be able to assist in assessing the entity's exposure and identifying the appropriate insurance and policy terms to satisfy these requirements.

2.5. Comparable guarantee

In limited circumstances, the Accreditor will consider an accredited person to have satisfied the insurance obligation where a comparable guarantee provides the same level of protection to CDR consumers as would have been provided by 'adequate' insurance.

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

Any application on the basis of a guarantee should be accompanied by supporting documentation appropriate to the circumstances. This documentation includes:

- a statement on terms the same as those required under paragraph 2.1.1. above
- 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. Exemptions

Certain entities are exempt from the insurance obligation. These entities are authorised deposit-taking institutions (ADIs) (other than restricted ADIs).[5]

All other entities must comply with the insurance obligation, including subsidiaries of ADIs.

[5] CDR Rules, Schedule 3, clause 7.4(2)