ACCC/OAIC Compliance and Enforcement Policy for the Consumer Data Right

May 2020

Version control	
8/05/2020	V1

Contents

1. About this policy

The Consumer Data Right (**CDR**) is a data portability reform that will be rolled out economy-wide, sector-by-sector, starting with banking. The objective of the CDR is to provide consumers with the ability to efficiently and conveniently access their personal data held by businesses (**data holders**), and to authorise the secure sharing of that data to trusted and accredited third parties (**accredited data recipients**). The CDR also requires businesses to provide public access to information on specified products that they offer.

The CDR will give consumers more control over their data. Consumer consent and strong privacy protections will be central to the CDR regime. Allowing consumers to share their data with service providers of their choice will lead to increased competition and will drive innovation across the Australian economy.

The CDR regime will be implemented and regulated by a framework that consists of:

- Legislation including the *Treasury Laws Amendment (Consumer Data Right) Act 2019*), which makes amendments to the *Competition and Consumer Act 2010* (**CCA**), *Privacy Act 1988* and the *Australian Information Commissioner Act 2010*
    - the core amendments are contained in Part IVD of the CCA, which also sets out the Privacy Safeguards that protect the privacy and confidentiality of CDR consumers' CDR data
- Rules made under the legislation (**Rules**)
- Consumer Data Standards made under the Rules (**Data Standards**).

This policy aims to help consumers and CDR participants understand the approach that the Australian Competition and Consumer Commission (**ACCC**) and the Office of the Australian Information Commissioner (**OAIC**) will adopt to encourage compliance and prevent breaches of the CDR regulatory framework. This policy does not discuss how the OAIC will apply its complaint handling powers or the process for making a CDR consumer complaint. [1]

We will regularly review and update this policy to ensure it reflects our current approach to compliance and enforcement.

[1] For further information on making a consumer complaint, please refer to the OAIC website.

2. Compliance and enforcement approach

Monitoring compliance and enforcement of the CDR regulatory obligations will be jointly conducted by the ACCC and the OAIC.

Our approach to compliance and enforcement will be underpinned by the objective of ensuring that consumers can trust the security and integrity of the CDR regime. Consumers must be confident that the CDR regime works as intended and that the regulatory framework put in place will protect their interests. Consumers should be able to trust that we are monitoring and enforcing CDR participants'[2] compliance with the relevant laws, Rules and Data Standards. This is particularly important as the CDR is rolled out more broadly.

The CDR is a significant economy wide reform and we recognise that there may be a period of transition for CDR participants to ensure their systems and processes fully meet their obligations under the CDR regulatory framework.

While it is the responsibility of each CDR participant to be fully aware of its obligations under the CDR regulatory framework, the ACCC has had considerable engagement with data holders and prospective data recipients regarding these obligations.

Further, the Data Standards Body[3] (**DSB**) and the OAIC have published guidelines to assist CDR participants to understand the nature of their obligations under the CDR framework. For more information, CDR participants should read the Data Standards, including the CX Standards and associated guidelines, as well as the Privacy Safeguard Guidelines.

We will continue to engage with CDR participants going forward.

Principles

We will adopt a strategic risk-based approach to compliance and enforcement. This approach recognises the joint regulatory model and that breaches of the legislation (including the Privacy Safeguards, Rules and Data Standards) will be dealt with efficiently and effectively.

We will exercise our compliance and enforcement powers with integrity, professionalism and in the public interest. We are guided by the following principles when undertaking our compliance and enforcement work:

Accountability – we are accountable for our actions, which can be reviewed by a range of agencies including the Commonwealth Ombudsman, Parliamentary Committees and the courts.

Efficiency – we strive to perform our roles in an efficient and timely manner to avoid costly delays and uncertainty for consumers and CDR participants.

Fairness – we strive to exercise our powers in a manner which is procedurally fair and provides natural justice.

Proportionality – our regulatory measures and actions will be proportionate to the conduct and the resulting harm or potential harm.

Transparency – to the extent permitted by law, we will be open and transparent about how we use our regulatory powers, what action we take and why. We will ensure that matters finalised by litigation or other formal resolution are made public.

---

[2] 'CDR participants' refers to data holders, accredited data recipients and their respective related entities.

[3] The Data Standards Body is responsible for the development of common technical standards to allow Australians to access data held about them by businesses and direct its safe transfer to others.

3. Fostering compliance

Fostering a culture of compliance is critical to achieving the objectives of the CDR. Our approach to compliance is focused on preventing and addressing consumer harm and ensuring the effective, efficient and lawful operation of the CDR regime. We are committed to driving a high level of compliance within the CDR regime and will use the most appropriate tools available to us in order to achieve our compliance objectives.

We seek to:

- engage with CDR participants to assist them in understanding their obligations under the CDR regulatory framework
- encourage a compliance culture within the CDR regime
- enforce the law, including by the resolution of possible contraventions administratively or by the use of formal enforcement action, and
- work with stakeholders to implement the above strategies, including through coordinated approaches.

Compliance monitoring tools

We will use a wide range of information sources and monitoring tools to assess levels of compliance and identify potential breaches of the relevant legislation (including Privacy Safeguards, Rules and Data Standards). These are detailed below:

	**Stakeholder intelligence / complaints** • Receiving information from stakeholders (including CDR consumers, businesses, consumer groups and other government agencies). • Receiving intelligence and reports from approved external dispute resolution bodies to address preliminary or sector specific concerns. For the banking sector, the approved external resolution body is AFCA.
	**Business reporting** • Receiving mandatory periodic reports from data holders and accredited data recipients which provide a range of information, including a summary of CDR complaint data.[4] • We will use these reports to track compliance and identify any issues or concerning trends.

[4] Rule 9.4

	**Audits and Assessments** • Undertaking audits and assessments of data holders and/or accredited data recipients to ensure they are complying with the relevant legislation (including the Privacy Safeguards, Rules and Data Standards).[5] • Taking required action to resolve identified compliance problems, inefficiencies or potential risks of harm to consumers. • We will use these powers to ensure that CDR data is managed in accordance with the legislation, for example consumer consents are properly obtained, and that data holders and accredited data recipients have appropriate security protections and measures in place.
	**Information requests and compulsory notices** • Issuing data holders or accredited data recipients information requests to help inform our compliance and enforcement activity. • Using statutory information gathering powers to compel the provision of information, documents or evidence where conduct may constitute a contravention of the CCA.

[5] Rules 9.6 and 9.7

4. Taking enforcement action

Ultimately, prevention of a breach of the CDR regulatory obligations through our compliance activities is preferable to taking action after the breach has occurred. However, when we consider a breach has occurred, we will take regulatory action proportionate to the seriousness of the breach and the level of harm or potential harm.

We use a risk-based approach to monitoring and assessing compliance matters and taking enforcement action. We cannot pursue all matters that come to our attention. Our role is to focus on those circumstances that will, or have the potential to, cause significant harm to the CDR regime or result in widespread consumer detriment. We prioritise and focus on matters that provide the greatest overall benefit to consumers. In deciding whether to take enforcement action, we will consider each case on its merits and the relevant circumstances.

In deciding on the appropriate enforcement approach, we will consider the following non-exhaustive list of factors:

- the nature and extent of the conduct constituting the breach, including the period over which the conduct occurred and the number of related breaches
- the size of the business engaging in the conduct, due to the greater potential for consumer detriment
- the impact of the conduct, including harm or increased risk of harm to consumers
- whether the conduct was deliberate, repeated, reckless or inadvertent
- whether the conduct involved, or was directed or overseen by, senior management
- the extent of any realised or potential future gain from the conduct
- whether the conduct indicates systemic issues that may pose ongoing compliance or enforcement problems
- whether action is already being taken to address the issue by another enforcement agency or other organisation (for example, the external dispute resolution body)
- the actions of the business in relation to the conduct, including whether the conduct was self-reported, the timing of the self-report and whether the business has taken any action to rectify the breach and avoid reoccurrence
- whether the business has displayed a corporate culture of compliance, including effective compliance programs, and whether corrective measures have been taken in response to any past breaches
- the level of cooperation with the ACCC during testing, assurance and compliance processes
- the specific and general educational, deterrent or precedent value of enforcement action, including whether pursuing court action (where applicable) would test or clarify the law, and
- whether the conduct requires urgent action or intervention by the ACCC and/or the OAIC.

When taking enforcement action, we seek to:

- stop the unlawful conduct
- deter the offending conduct (both specifically and generally)

- ensure future compliance with the legislation (including the Privacy Safeguards, Rules and Data Standards)
- encourage the proper use of CDR data
- penalise offenders (where warranted), and
- instil public confidence in the role of the ACCC and the OAIC in ensuring consumers are appropriately protected within the CDR regime.

Enforcement options

There are a range of enforcement options available to respond to and resolve breaches of the CDR legislation (including the Privacy Safeguards, Rules and Data Standards). These are detailed below:

	**Administrative resolutions** • Accepting a voluntary written commitment from a business to address a non-compliance issue. • Recommending improvements to a CDR participants' internal practices and procedures (for example, by implementing a compliance program, improving internal operational procedures or ensuring appropriate staff training). • Monitoring compliance with voluntary commitments.
	**Infringement notices (ACCC)** • Issuing data holders or accredited data recipients with infringement notices if we consider a breach has occurred.
	**Court enforceable undertakings** • Accepting a formal written commitment (undertaking) from a CDR participant that it will take or refrain from certain action. For example, an undertaking may include commitments to do an internal audit to ensure that the CDR participant has identified the root cause of a breach and the risk of future breaches is mitigated. • Seeking court orders, including declarations of a breach, injunctions and penalties, if a CDR participant has not complied with an enforceable undertaking.

	**Suspension or revocation of accreditation (ACCC)** • The Data Recipient Accreditor (currently the ACCC) may suspend or revoke an accredited person's accreditation status under certain circumstances (see Rule 5.17 for details). For example, if the Data Recipient Accreditor reasonably believes that a revocation or suspension is necessary in order to protect consumers. • An accredited data recipient is prohibited from seeking to collect data while a suspension is in effect.
	**Determination and declarations power (OAIC)** • Making a determination to either dismiss or substantiate a breach of a Privacy Safeguard or Rule relating to the privacy or confidentiality of CDR data, following an investigation. • The determination may include a declaration or order that the CDR participant should not repeat or continue the conduct, take relevant steps within a specified period to ensure the conduct is ceased and redress any loss or damage suffered by consumers, including compensation.

	**Court proceedings**
	• Initiating legal action for a breach of the legislation (including the Privacy Safeguards, Rules and/or Data Standards).
	• The court can make a range of orders including civil penalties, action to remedy a breach, an injunction to restrain a CDR participant from engaging in the conduct, and orders disqualifying individuals from being directors of corporations.
	• We are more likely to initiate court proceeding where the conduct:
	  ○ results, or has the potential to result, in competitive harm or substantial consumer detriment
	  ○ is widespread, such that enforcement action is likely to have a significant deterrent effect, or
	  ○ involves a CDR participant that has a history of previous breaches of competition, consumer or privacy laws.

Priority conduct

There are some forms of conduct which are likely to result in significant detriment to consumers and the integrity of the CDR regime which will always give grounds for the consideration of enforcement action. The ACCC and OAIC are more likely to take action where the conduct involves:

Data holder refusal	• Data holders that repeatedly refuse to disclose, or frustrate the process of disclosure, consumer data by intentionally circumventing the Rules or Data Standards, in response to valid consumer data requests in circumstances where a refusal to disclose is not permitted (for example, where disclosure would create risks of harm or where provided for in the data standards)[6].

Misleading or deceptive conduct[7]	• Conduct that misleads or deceives a person into believing that another person is a CDR consumer or that a valid request or consent has been made.
	• 'Holding out', which involves:
	  ○ a person creating or fostering the perception by others that they are an accredited data recipient, when they are not, or
	  ○ a person failing to correct the perception that they are accredited, when they are not.
	• Conduct by a data recipient involving a false or misleading representation regarding the nature or benefits of the CDR service provided.

Invalid consent	• Accredited data recipients collecting CDR data without valid consent.
Misuse or improper disclosure of CDR consumer data	• Intentional misuse or improper disclosure of CDR consumer data by an accredited data recipient, which is inconsistent with the consent provided by a CDR consumer, particularly where consent has been withdrawn. • This would include conduct that deliberately seeks to circumvent the 'data minimisation' principle.
Insufficient security controls	• CDR participants who have insufficient controls and processes to protect CDR data from misuse, interference and loss, and unauthorised access, modification or disclosure.[8]

We note that these priorities will be subject to review and change as the CDR regime matures and is rolled out more broadly.

[6] See Rules 2.5, 3.5 and 4.7.

[7] The ACCC can also take action for alleged misleading or deceptive conduct under the Australian Consumer Law.

[8] The ACCC will only accredit CDR participants who have sufficient security controls. However, if the CDR participant demonstrates it does not have sufficient security controls in practice, or it departs from the security controls it has demonstrated to achieve accreditation, then enforcement action may be warranted.