Australian Government

Consumer Data Right

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

October 2023

Version Control	
May 2020	V1
October 2023	V2

Table of contents

1. The Consumer Data Right

The Consumer Data Right (**CDR**) is being rolled out economy-wide, sector-by-sector, with banking now well established and energy in progress, and other sectors to follow. The objective of the CDR is to provide consumers with the ability to efficiently and conveniently share their personal data held by businesses (**data holders**), and to authorise the secure transfer 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 gives consumers more control over their data. Consumer consent and strong privacy protections are central to the CDR. Allowing consumers to share their data with service providers of their choice leads to increased competition and drives innovation across the Australian economy.

The CDR is regulated by a framework (**CDR regulatory framework**) which consists of:

- the *Competition and Consumer Act 2010* (**CCA**), *Privacy Act 1988* (**Privacy Act**) and the *Australian Information Commissioner Act 2010*
    - the core CDR provisions are contained in Part IVD of the CCA and include the Privacy Safeguards that protect the privacy and confidentiality of CDR consumers' CDR data
- Rules made under the legislation (**Rules**)
- the *Competition and Consumer Regulations 2010,* and
- Consumer Data Standards made in accordance with the Rules (**Data Standards**).

2. About this policy

This policy sets out the Australian Competition and Consumer Commission's (**ACCC**) and the Office of the Australian Information Commissioner's (**OAIC**) general approach to compliance and enforcement for the CDR, including our[1] priorities.

This policy does not discuss how the OAIC will apply its complaint handling powers or the process for making a CDR consumer complaint.[2] It should be read together with the OAIC's Consumer Data Right regulatory action policy.

In so far as it relates to the ACCC, this policy complements the ACCC's Compliance and enforcement policy, which outlines the ACCC's approach to its enforcement functions under the CCA and other legislation and is published annually. The policies should be read together.

This policy is regularly reviewed to ensure it reflects our current approach to compliance and enforcement for the CDR.

[1] A reference in this document to 'our' or 'we' is a reference to the ACCC and OAIC.

[2] For further information on making a consumer complaint, please refer to the CDR website (cdr.gov.au).

3. Compliance and enforcement approach

Monitoring compliance and enforcement of CDR obligations is conducted by the ACCC and the OAIC.

Our approach to compliance and enforcement is underpinned by the objective of ensuring consumers can trust the security and integrity of the CDR. Consumers must be confident the CDR 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'[3] compliance with the relevant laws, Rules and Data Standards.

The CDR is a significant economy wide reform. While we understand CDR obligations are relatively new, it is the responsibility of each CDR participant to be aware of and comply with their legal obligations. CDR participants must ensure their systems and processes meet the requirements set out under the CDR regulatory framework. The ACCC, Data Standards Body[4] (**DSB**) and OAIC have published guidance to assist CDR participants to understand the nature of their obligations. Guidance is available on the CDR website and participants can also ask questions about the Rules and Data Standards via the CDR Support Portal.

For more detailed information, CDR participants should read the Rules and Data Standards, including the CX Standards and associated guidelines. Participants should also have regard to the OAIC's Privacy Safeguard Guidelines, made in accordance with requirements set out in the CCA[5] for the Information Commissioner to make guidelines for the avoidance of acts or practices that may breach the privacy safeguards.

Principles

We will adopt a strategic and risk-based approach to compliance and enforcement, recognising the co-regulatory model.

We will exercise our respective compliance and enforcement powers with integrity, professionalism and in the public interest. The OAIC's CDR regulatory action policy and the ACCC's Compliance and enforcement policy outline the principles that guide each agency when undertaking our compliance and enforcement work.

4. Fostering compliance

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

To achieve our compliance objectives, we use the following flexible and integrated strategies:

- engage with CDR participants to assist them in understanding their obligations under the CDR regulatory framework, including by publishing guidance material
- encourage a compliance culture among CDR participants

[3] 'A CDR participant is defined in the CCA as a data holder or accredited data recipient. This policy also applies to other entities regulated by the CDR framework, including accredited persons.

[4] 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.

[5] See s 56EQ of the CCA.

- enforce the law, including by resolving possible contraventions administratively, or by litigation or other formal enforcement outcomes, and
- work collaboratively, as appropriate, to implement these strategies, including through coordinated approaches.

Compliance monitoring tools

We use a wide range of information sources and monitoring tools to assess levels of compliance and identify potential breaches of the CDR regulatory framework. These are detailed below.

Table 1: Overview of information sources and compliance monitoring tools

	**Complaints / stakeholder intelligence** • Receiving information through complaints from a consumer or a representative of a consumer. • 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.
	**Participant reporting and rectification schedule** • Receiving mandatory periodic reports from data holders and accredited data recipients which provide a range of information, including a summary of CDR complaint data.[6] We use these reports to identify issues or concerning trends. • Receiving self-reported information about compliance gaps, closely monitoring rectification of these gaps and publishing a CDR public rectification schedule that provides information about them, increasing transparency for CDR participants.[7]
	**Audits and Assessments** • Undertaking audits and assessments of data holders and accredited data recipients to ensure they are complying with the CDR regulatory framework, which includes provisions of the Rules and Data Standards.[8] • Using information from audits and assessments to help certain CDR participants achieve best practice compliance, to inform public guidance, and to identify issues or concerning trends that may require further regulatory action.

[6] Rule 9.4 and metrics reporting under the Consumer Data Standards.

[7] The public rectification schedule is one mechanism used to provide transparency about non-compliance with CDR obligations. Publication on the rectification schedule may be sufficient to manage and address some instances of non-compliance. In other instances, we may put in place additional measures such as regular reporting on activities towards rectification, and publishing compliance gaps on a CDR participant's website. Listing an issue on the rectification schedule does not preclude the ACCC from pursuing compliance or enforcement action in-line with this policy.

[8] Rules 9.6 and 9.7 and, for the OAIC, s 56ER of the CCA.

Information requests and compulsory notices

- Issuing CDR participants with information requests to help inform our compliance and enforcement activity.
- Using statutory information gathering powers (as applicable) to compel the provision of information, documents, or evidence where conduct may constitute a contravention of the CDR regulatory framework.

5. Taking enforcement action

Where we consider a breach has occurred, we will take enforcement action proportionate to the seriousness of the breach and the level of harm or potential harm to CDR consumers.

We cannot pursue all matters that come to our attention. As a result, we focus on circumstances that will, or have the potential to, cause harm to the CDR regime or result in widespread or significant detriment to CDR consumers. The ACCC and OAIC will each separately exercise their respective discretion to direct resources to focus on matters that provide the greatest overall benefit to consumers. Where possible, we will consult with each other and coordinate our activities to minimise burden on CDR participants.

Our enforcement priorities are set out below. When deciding whether to pursue a matter, we will prioritise those matters which fall within those priorities. We will give particular consideration to those matters which also have the following factors:

- conduct that will, or has the potential to, cause harm to the CDR regime, including undermining consumer trust in the security and integrity of the CDR
- conduct that will, or has the potential to, result in widespread or substantial detriment to CDR consumers
- conduct that will, or has the potential to, cause harm to vulnerable consumers
- conduct that is of significant public interest or concern
- conduct by large CDR participants, recognising the potential for greater consumer detriment from breaches by entities that deal with a greater volume of CDR data, or service a greater number of CDR consumers.

Enforcement options

There are a range of enforcement options available to respond to and resolve breaches of the CDR regulatory framework. Some of these are detailed below. For further information about the enforcement options available to each agency, refer to the ACCC's Compliance and enforcement policy and the OAIC's CDR regulatory action policy.

Table 2: Overview of enforcement options

	**Administrative resolutions (ACCC and OAIC)** • Accepting a voluntary written commitment from a business to address non-compliance. • Recommending improvements to a CDR participant's 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 only)** • The ACCC may issue an infringement notice where it believes there has been a contravention that requires a more formal sanction than an administrative resolution but where the ACCC considers that the matter may be resolved without legal proceedings.
	**Court enforceable undertakings (ACCC and OAIC)** • Accepting a formal written commitment (court enforceable 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 has identified the cause of a breach and mitigated the risk of future breaches. • Where a CDR participant has not complied with an enforceable undertaking, seek court orders.
	**Suspension or revocation of accreditation (ACCC only)** • The ACCC, as the Data Recipient Accreditor, may suspend or revoke an accredited person's accreditation 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 only)** • The OAIC can make a determination to either dismiss or find a breach of a Privacy Safeguard or Rule relating to the privacy or confidentiality of CDR data, following an investigation. • The determination may include declarations or orders that the CDR participant must not repeat or continue the conduct, must take specified actions within a specified period to ensure the conduct is ceased, and/or must redress any loss or damage suffered by consumers, including compensation. • The OAIC may bring proceedings to enforce a determination.
	**Direction to notify an eligible data breach (OAIC only)** • The OAIC can direct accredited data recipients and designated gateways to notify consumers at risk of serious harm, as well as the Information Commissioner, about an eligible data breach.[9]
	**Court proceedings (ACCC or OAIC)** • Legal action is taken where, having regard to all the circumstances, the ACCC or OAIC considers litigation is the most appropriate way to achieve compliance objectives. We consider the priority factors and are more likely to use litigation where the conduct results, or has the potential to result, in harm to competition, harm to privacy rights, or substantial or widespread CDR consumer detriment. We may also prioritise action that will help clarify aspects of the law. • The court can make a range of orders including declarations, imposing pecuniary penalties, injunctions to restrain a CDR participant from engaging in the conduct, orders to comply with binding Data Standards, and orders disqualifying individuals from being directors of corporations.

Other action

In some matters, the ACCC or OAIC may decide not to pursue enforcement action to deal with a matter or issue but we may instead:

- draw the issue to the relevant CDR participant's attention and provide information to help them gain a better understanding of the CDR regulatory framework, and to encourage rectification and future compliance
- place the relevant CDR participant on notice about the ACCC's or OAIC's concerns and the possibility of future investigation and action should the conduct continue or re-emerge
- deal with the matter informally if the CDR participant has promptly and effectively corrected a possible contravention and implemented measures to prevent recurrence

[9] Section 26WE of the *Privacy Act 1988* defines an eligible data breach.

- postpone or cease an investigation with a view to reactivating the investigation should further information become available
- seek to solve the problem through compliance or advocacy activities.

Priority conduct

There are some forms of conduct which are likely to result in significant detriment to consumers and the integrity of the CDR which will always be considered as enforcement priorities. We are more likely to take action where the conduct involves:

Conduct	Indicative factors
Data holders hindering processes	• Data holders that introduce friction to required data holder functionality or processes, or otherwise discourage consumers from completing authorisation or participating in the CDR. • Data holders that refuse to disclose consumer data in response to a valid consumer data request in circumstances where a refusal to disclose is not permitted under the Rules or Data Standards.
Failure to meet compliance dates	• Data holders that repeatedly fail to meet a compliance obligation date or dates, and where we form the view they have not made sufficient efforts to comply with the obligations at the first possible opportunity after the commencement date.
Insufficient data quality	• Data holders that disclose poor quality data (for example, data that is inaccurate, incomplete, or not in the format required by the Data Standards). • For product data this may include disclosure of data that does not accurately reflect information about a product published on a data holder's website or in relevant disclosure documents. For consumer data, it could include the failure to disclose required data.
Insufficient oversight of third parties by accredited data recipients	• CDR representative principals must ensure their CDR representatives comply with their obligations under a CDR representative arrangement. This includes ensuring CDR representatives understand their Privacy Safeguard obligations, take the information security steps in Schedule 2 to the Rules and only use or disclose CDR data in accordance with their representative arrangement with the CDR representative principal. • OSP principals must ensure outsourced service providers only use or disclose CDR data in accordance with a CDR outsourcing arrangement. • Accredited data recipients must ensure sufficient oversight, including that adequate controls and systems are in place to monitor compliance with CDR representative or outsourcing arrangements.
Insufficient security measures	• Accredited data recipients who have insufficient controls and processes to protect CDR data from misuse, interference and loss, and unauthorised access, modification or disclosure.[10]

[10] 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.

	• Accredited data recipients who have insufficient controls and processes to ensure that their sponsored affiliate(s) maintain appropriate information security capabilities. • Data holders, accredited data recipients and designated gateways who fail to meet data breach notification requirements under Part IIIC of the Privacy Act,[11] or whose notifications to the OAIC indicate they have insufficient security measures in place to protect CDR data.

Misleading or deceptive conduct[12]	• 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.
	• Any other misleading or deceptive conduct that could risk the reputation of the CDR or undermine consumer confidence in the CDR ecosystem.

Misuse of CDR data	• Accredited data recipients not complying with the data minimisation principle[13] when collecting and using CDR data. • Accredited data recipients that use CDR data other than in accordance with a consumer's consent. • Accredited data recipients that do not delete or de-identify CDR data in accordance with the CDR regulatory framework. • Accredited data recipients with consent processes that do not meet the requirements of Rules. • Disclosure of CDR data that is not in accordance with the CDR regulatory framework, including accredited data recipients not taking reasonable steps to confirm that a trusted advisor is a member of one of the specified classes.

[11] Data holders are generally APP entities that will be bound by Part IIIC of the Privacy Act, and s 56ES of the CCA extends the application of Part IIIC of the Privacy Act to accredited data recipients and designated gateways.

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

[13] The 'data minimisation principle' requires that an accredited person must not seek to collect data beyond what is reasonably needed to provide the good/service for which a consumer has consented to share their CDR data, or for a longer time period than is reasonably needed.