Australian Government

Consumer Data Right

ACCC CDR Compliance review of Authorisation Processes

ACCC Findings

February 2023

Introduction and overview of the report

The Australian Competition and Consumer Commission (ACCC) is an independent Commonwealth statutory agency that promotes competition, fair trading and product safety for the benefit of consumers, businesses, and the Australian community.

The Consumer Data Right (CDR) gives consumers greater control over their consumer data by enabling consumers to direct a data holder to safely share their CDR data with an accredited data recipient (ADR). CDR improves consumers' ability to compare between products and services to find better deals more suited to their needs and encourages competition between providers.

Among its other roles in relation to the CDR (such as accrediting potential data recipients and providing guidance to stakeholders), the ACCC is responsible for monitoring compliance with the Competition and Consumer (Consumer Data Right) Rules 2020 (CDR Rules), the Consumer Data Standards (the Standards) and Part IVD of the *Competition and Consumer Act 2010* (the Act).

This report outlines our findings regarding six data holders' compliance with their authorisation-related CDR obligations. We encourage all data holders to review the findings from this assessment and relevant guidance to ensure compliance with the CDR rules and standards.

1. ACCC review of authorisation processes

In April 2022, the ACCC initiated a targeted compliance review to assess data holders' compliance with authorisation related CDR obligations.

Authorisation is an online process that involves a consumer selecting and confirming the data they would like to share with an ADR. When a data holder receives a consumer data request from an ADR, the data holder must seek the consumer's authorisation to disclose the data to the ADR, unless an exception applies. The process includes a data holder verifying the consumer's identity by sending the consumer a one-time password to ensure that they have authority to authorise CDR data sharing.

There are a range of CDR Rules and Standards that apply to the authorisation process. Further guidance on these obligations for banking sector data holders is available on the CDR website.

Our review consisted of analysing six data holders' video records of the process by which the data holder asks eligible CDR consumers for their authorisation to disclose CDR data. We did not review records relating to the amendment of an authorisation.

Overall, we observed a good level of compliance with the CDR Rules and mandatory Banking Language CX Standards and were able to address non-compliance observed administratively. We contacted each data holder with specific feedback and communicated our recommendations to them.

The findings of our assessment are presented below in a de-identified manner.

2. Objective and scope

Authorisation is one of the first CDR touch points for consumers and it is important that it provides a good user experience.

The focus of our review was to evaluate compliance with relevant CDR Rules[1] or Data Standards[2], identify any unwarranted friction, and provide recommendations to data holders to improve their authorisation processes. In line with our Compliance and Enforcement Policy[3], where we identify areas of non-compliance, we took a risk-based approach to compliance and enforcement including ensuring that the outcome is efficient, fair, proportionate, and transparent.

3. Summary of findings

We observed three data holders were compliant with the CDR Rules and Standards and had implemented non-mandatory aspects of the CX Guidelines, resulting in best-practice authorisation processes.

We also observed instances of non-compliance:

- Two data holders were non-compliant with CDR Rule 4.23(1)
- One data holder was non-compliant with the mandatory Banking Language CX Standards.

In each case of non-compliance, we considered the impact to be minor, as the risk of potential harm to consumers and the CDR arising from the observed issues was likely to be low.

We addressed the non-compliance administratively, by seeking commitments from the data holders to rectify the issues in a timely manner.

3.1.1. Areas of non-compliance with the CDR Rules

The non-compliance we observed related to the information a data holder must give a consumer when asking for authorisation to disclose CDR data. We observed instances where the processes did not:

i. explicitly state whether the authorisation being sought for disclosure of CDR data was for a single occasion or for a period of time in accordance with Rule 4.23(1)(d)

ii. explicitly state the period of time for which data would be disclosed (where authorisation for disclosure over a period of time was sought in accordance with Rule 4.23(1)(e)) – that is, only the expiry date of the authorisation was displayed, and

iii. include a statement that the authorisation could be withdrawn at any time in accordance with Rule 4.23(1)(f).

3.1.2. Areas of non-compliance with CX Standards

We observed one instance of non-compliance with Banking Language CX Standards, where wording used to describe 'transaction details' data did not align with the requirements.

[1] Division 4.4 of the Competition and Consumer (Consumer Data Right) Rules 2020

[2] CX checklist

[3] Compliance and Enforcement Policy

We resolved this issue administratively by requesting the data holder to self-report the item of non-compliance for inclusion on the CDR public rectification schedule, and it has since been rectified.

3.2. Recommendations made

We provided recommendations to the data holders on how they could improve their authorisation processes by implementing additional aspects of the CX guidelines, including by:

i. providing instructions for how a consumer can review CDR data sharing arrangements[4] and how to withdraw their authorisation

ii. providing a link to their CDR Policy during the authentication and authorisation process[5] to provide information to consumers about how CDR data is managed[6] and how they can make an inquiry or make a complaint[7]

iii. providing functionality for a consumer to request the One Time Password (OTP) to be re-sent[8]

iv. increasing consistency of terminology by referring to the OTP on the authentication screen[9], and

v. specifically stating that the OTP can only be used for CDR data sharing and cannot be used for authorisation of other transactions of actions[10].

4. Methodology

In April 2022, we requested each data holder to provide a video record of each process (as of 31 March 2022), where the data holder asks eligible consumers for their authorisation to disclose CDR data in relation to data holder's branded products. This video record is one of the types of records required to be kept and maintained by data holders for the purposes of subrule 9.3(1)(g).

We assessed each data holder's compliance with their authorisation-related obligations by reviewing these records against the relevant CDR rules, data standards and CX guidelines.

We note that our findings, including areas of non-compliance, are based on the records provided by each data holder at a certain point in time. After providing our feedback and recommendations, data holders took remedial steps to address the identified instances of non-compliance and implemented our recommendations. Therefore, our review does not reflect data holders' current authorisation processes, nor does it necessarily represent past conduct or guarantee future conduct on the part of the relevant data holders.

[4] CX checklist ref 3AU.02.19

[5] CX checklist ref 3AU.02.20

[6] Section 56ED(3)(a) of the *Competition and Consumer Act*

[7] See sections 56ED(4)(b) (for data holders), 5(d) (for accredited persons) and 6(b) (for designated gateways) of the *Competition and Consumer Act*

[8] CX checklist ref 2AU.03.19

[9] CX checklist ref 2AU.03.04

[10] Data Standard Security Profile – Authentication Flows

5. Next steps

We continue to closely monitor data holder compliance with authorisation-related CDR obligations and engage with relevant data holders to ensure any areas of non-compliance are rectified.

In line with the Compliance and Enforcement policy, we may take enforcement action to address any conduct that does not comply with the CDR Rules or the Standards.

We also liaise closely with the Office of the Australian Information Commissioner (OAIC) on CDR issues, including authorisation-related CDR obligations.