# Obligations and Opportunities of CDR

Version 1

**Voruna Pty Ltd**

CDR Compliance, Simplified.

voruna.com.au

# Contents

# 1.0 Introduction and Overview

**Key Objective:** This whitepaper aims to provide a clear overview of the upcoming CDR compliance obligations that non-bank lenders (NBLs) must adhere to, detailing the key regulatory requirements and their implications for businesses in the sector. By outlining the obligations related to product and consumer data sharing, we aim to offer practical guidance on how NBLs can ensure timely and efficient compliance, helping businesses avoid penalties and leverage opportunities in the evolving regulatory landscape.

The Consumer Data Right (CDR) is a regulatory framework introduced in Australia to give consumers greater control over their personal data. It mandates that businesses holding certain types of consumer data must make this data available to accredited third parties upon consumer request, thereby promoting transparency, competition, and consumer choice. In recent years, the CDR has expanded to include non-bank lenders (NBLs) (Australian Treasury, 2024a), further widening the scope of data-sharing obligations. This expansion is designed to ensure that the financial services sector operates with greater accountability and responsiveness to consumer needs.

As non-bank lenders increasingly become subject to CDR rules, it is essential for stakeholders to understand the obligations and prepare accordingly. Failure to comply with the CDR framework can result in regulatory penalties, reputational damage, and missed opportunities for growth in the evolving digital economy. This whitepaper highlights the need for businesses to act proactively in implementing the necessary systems and processes to comply with the phased CDR rollout, which starts in 2026.

The scope of this paper covers the following key areas:

- **Regulatory Scope and Data Holder Duties:** Understanding what data needs to be shared and the timelines for compliance.
- **Participation Thresholds and Phased Rollout:** Clarifying the criteria for qualifying as an initial or large provider and the phased implementation of the CDR.
- **Other Compliance Expectations:** Detailing additional requirements such as consent management, testing protocols, and incident management.
- **CDR in Action:** Considering the potential opportunities and observing case studies in banking.

This whitepaper is intended for business stakeholders, including executives, compliance officers, and IT managers, who are responsible for ensuring their organisations meet CDR obligations in a timely and efficient manner.

# 2.0 CDR Compliance Obligations for NBLs

## 2.1 Regulatory Scope and Data Holder Duties

Under CDR legislation, designated Data Holders **must disclose required product and consumer data** to any accredited Data Recipient upon consumer request and consent (ACCC, 2020). In practice, this means a Data Holder's systems must be capable of providing:

**(a) Product Reference Data** – public information about lending products (e.g. interest rates, fees, features) (ACCC, 2020, *p2*).

**(b) Consumer Data** – private customer-specific data (e.g. customer details, loan account data, transaction histories) when an accredited third party asks, with the customer's permission. Unless an exception applies, failure to share the requested data in the mandated format and timeframe would breach the CDR Rules (ACCC, 2020, *p2*). Consumer data request types are captured by;

i. **Non-Complex Requests**: involving individual consumers, such as accessing personal account details or transaction histories.

ii. **Complex Consumer Data Requests**: involve more complicated scenarios (Australian Treasury, 2024b, *p15*), including:

- *Secondary Users*: Requests made on behalf of individuals who are not the primary account holders but are authorised users.
- *Joint or Partnership Accounts*: Requests related to accounts held jointly or within business partnerships, requiring coordination among multiple account holders.
- *Nominated Representatives*: Requests made on behalf of business entities or organisations where data authorisations are managed by designated representatives.

Data holders are required to comply with above requests to a historical limit of 2 years (Australian Treasury, 2024a, *p2*). In-scope products will include standard consumer lending products (e.g. personal loans, credit cards, mortgages, BNPL) but exclude certain niche products/trial products. To avoid undue burden: products like consumer leases, reverse mortgages, margin loans, non-standard asset finance, or any product with <1000 customers may be excluded from mandatory data sharing (voluntary only) (Australian Treasury, 2024a, *p21*).

## 2.2 Participation Thresholds and Phased Rollout

The Treasury's (2024b, *p15-16*) draft rules propose phased rollout for two specific categories of organisations:

**Initial Provider**, following conditions are met:

- The total value of resident loans and resident finance leases reported by the lender and its associated non-bank lenders for the most recent month is over $10 billion.
- The average total value of these loans and leases over the 12 months is also over $10 billion.

**Large Provider**, following conditions are met (and do not qualify as an initial provider):

- The total value of resident loans and resident finance leases reported for the most recent month and the 12-month period preceding is over $1 billion each.
- Either:
  (a) The lender must have more than 1,000 customers.
  (b) The lender is accredited by a relevant regulatory body.

INITIAL

**Tranche 1 (13 July 2026)** – **Product data sharing begins for large and initial providers**. Must publish standardised product reference data via open APIs. This ensures basic product information is available as early as possible in accordance with Part 2 of CDR rules.

**Tranche 2 (9 November 2026)** – **Consumer data sharing for initial providers**. The biggest non-bank lenders must start sharing customer-specific data for simple (non-complex) requests by this date in accordance with Part 4 of CDR rules.

**Tranche 3 (15 March 2027)** – **Complex requests for initial providers**. The largest lenders must handle **complex data requests** (e.g. joint accounts, secondary users) by now in accordance with Part 4 of CDR rules.

LARGE

**Tranche 4 (10 May 2027)** – **Consumer data sharing for large providers** begins. Medium-sized lenders above the threshold must fulfill consumer data requests (excluding complex ones) by this date.

**Tranche 5 (13 September 2027)** – **Complex requests for large providers**. All remaining in-scope lenders must be fully compliant, including sharing data for joint accounts or secondary users if applicable.

*Further detail on rules (including accompanying summaries) presented by Australian Treasury (2024b, *p18*)

These dates mean that by **mid-2026** Data Holders need at least their product reference data APIs live, and by **mid-2027** most customer data-sharing capabilities must be operational for mandated lenders. ACCC and Treasury have explicitly structured this to start with simpler use cases and larger entities first.

## 2.3 Other Compliance Expectations

Beyond data sharing itself, the CDR obligations require data holders to implement consumer-friendly processes. The Consumer Data Right (2024) body presents an explicit set of requirements (adapted below):

**Website and App Requirements:** Data holders must ensure their websites and apps enable consumers to authorise data sharing. They must include features allowing users to view, manage, and withdraw data authorisations, providing transparency regarding the authorisation details, such as the period, expiration, and status.

**The Consumer Data Standards:** The Consumer Data Standards, developed by the Data Standards Body, consist of five components: CX standards, CX guidelines for implementation, security profiles covering encryption and token transfers, API standards for data requests, and non-functional requirements (availability, traffic, and data quality) for data holders. These are at the core of ensuring consistency and security in how data is shared.

**Test Approach for Providers:** Providers must pass the Conformance Test Suite before joining the CDR system. This testing ensures their systems align with CDR standards and prepares them for ongoing operation, with detailed guidance available for new and existing providers.

**System Production Incidents:** In case of technical incidents, the CDR Service Management Portal facilitates communication between participants and the ACCC's technical operations team, helping maintain system integrity and resolving issues efficiently.

# 3.0 CDR in Action

## 3.1 Opportunities

CDR gives customers more control over their data, which can enhance their trust in institutions that offer transparent data practices. When a lender enables easy, consent-driven data sharing, **customers are empowered** to use their financial data in beneficial ways (for example, to get better advice or compare options), leading to higher satisfaction. The CDR ecosystem includes consumer protections and an accreditation of trust, so customers know they are sharing data safely under a regulated regime. Non-bank lenders that participate can align themselves with this trusted system, improving engagement by showing they respect customer choice and privacy. In practical terms, offering CDR means, for instance, a borrower can seamlessly import their account data into a budgeting tool or loan comparison site – a convenience that reflects well on the data-holding lender even if the data is leaving that institution.

Opening data can **level the playing field between banks and non-bank lenders**. Consumers will be able to see non-bank lenders' products alongside bank products easily, and even share their non-bank lending data when applying for other services. This promotes competition and can drive more business toward nimble non-bank players (Bolam, 202). In fact, the government explicitly notes that expanding CDR to non-bank lending is meant to *"promote greater competition and innovation in the market"* (Jones, 2025). Non-bank lenders can capitalise on this by innovating niche products and using the CDR channel to reach customers. For example, as consumers compare loan offers through fintech apps, a non-bank lender's unique product (say, a renovation loan or green energy loan) can stand out, whereas previously that product data might not have been readily accessible. One industry expert described the inclusion of non-bank lenders in CDR as bringing *"game-changing benefits for both consumers and lenders"*, by allowing consumers to combine bank and non-bank data for better decision-making (Booth, 2025).

As data holders, non-bank lender APIs can be integrated by fintech partners to create blended services. For instance, a personal finance management app could pull a customer's loan data from a non-bank lender and their savings account data from a bank to provide a 360° financial view. This kind of integration often results in the customer discovering more about the non-bank's products (e.g. seeing their loan details in context), potentially driving cross-sell or referrals. Moreover, non-bank lenders can choose to become accredited data recipients themselves, enabling them to ingest banking data or energy data to enrich their own offerings. For example, an NBL could use CDR to retrieve a prospective borrower's banking transaction history instantly, making credit assessments faster and more accurate. Data sharing through CDR is standardised and legally compliant, which means partnerships can be formed more quickly (no need for bespoke data agreements in many cases) and with less risk. Some non-bank lenders are already eyeing cross-industry opportunities – for instance, bundling loan products with services like energy plans or insurance – by leveraging data made available through CDR (Bolam, 2025). By participating in the CDR ecosystem, non-bank lenders effectively join a **network of interoperable services**, positioning themselves to collaborate in ways that can expand their customer reach and create new revenue streams.

The CDR standards demand high data accuracy and consistency, which incentivises lenders to clean and organise their data infrastructure – an effort that can yield benefits beyond CDR (e.g. better internal data analytics). Once in place, CDR APIs can replace slower or less secure methods of data exchange, such as customers emailing spreadsheets or third parties (unduly) web scraping the lender's website. CDR rollout is actually seen as a pathway to eventually phase out practices like scraping (Jones, 2025). By getting on the front foot with CDR, a **non-bank lender can modernise its technology stack in line with industry best practices**. Additionally, using a well-defined API and consent model reduces the ad-hoc handling of data requests (for example, responding to customer data access requests can be as simple as directing them to use CDR). Compliance reporting is also standardised; lenders submit reports on CDR metrics and any incidents on a schedule, benefiting from clear guidance. All of this can mean lower long-term compliance costs. Rather than maintaining multiple bespoke interfaces for data sharing with partners or auditors, the lender has one robust interface that meets legal requirements and can serve multiple purposes. In essence, investing in CDR compliance can help non-bank lenders streamline how data is managed and shared, promoting efficiencies while also ensuring they meet all regulatory obligations under an audited framework.

## 3.2 Case Studies

### Case Study 1: Commonwealth Bank of Australia (CBA)

As one of the first institutions required to comply with CDR in banking (open banking), CBA proactively adopted the framework (CBA, 2021, *p46*). Initially, CBA faced challenges aligning legacy IT infrastructure with CDR API standards, requiring significant investments in technology upgrades and staff training (CBA, 2022). Despite these challenges, CBA reported enhanced customer trust and engagement due to increased transparency and control over personal data. Moreover, compliance positioned CBA competitively, enabling strategic partnerships with fintech providers, driving innovation, and broadening its customer acquisition channels (CBA, 2021, *p16*).

### Case Study 2: Regional Australia Bank (RAB)

Regional Australia Bank, an early adopter of CDR (RAB, 2020), quickly capitalised on open banking by integrating new financial management tools into its customer offerings (DSB, 2021, *p7*). Initial hurdles included navigating complex CDR standards and adapting to rigorous security requirements (DSB, 2020a, *p6*). By successfully managing these challenges, the bank significantly improved customer experience and satisfaction, reporting a noticeable increase in customer retention and attracting new users through enhanced product offerings, enabled by seamless data integration (DSB, 2020b, *p10*).

### Case Study 3: Up Bank

Up Bank, a mobile-only digital bank launched in 2018 through a collaboration between fintech Ferocia and Bendigo / Adelaide Bank, has been at the forefront of integrating the Consumer Data Right (CDR) into its operations (Bendigo Bank, 2021). By becoming a CDR participant, Up enables its customers to securely share their banking data with accredited third-party providers, such as budgeting tools and loan services, enhancing user control and fostering financial innovation (Up Bank, 2021). Up's proactive approach to CDR compliance is evident in its transparent Consumer Data Right policy, which outlines how customer data is managed and shared. This commitment not only ensures regulatory adherence but also builds customer trust by emphasising data security and user consent (Up Bank, 2024). By leveraging CDR, Up Bank has positioned itself as a leader in open banking, offering enhanced services that align with modern consumer expectations for data portability and personalised financial solutions; earning them sweeping awards in 2021 (Up Bank, 2021).

# 4.0 References


Australian Competition and Consumer Commission (ACCC). (2020). *Competition and Consumer (Consumer Data Right) Rules 2020*. ACCC. https://www.accc.gov.au/system/files/CDR%20Rules%20-%20Final%20-%206%20February%202020.pdf

Australian Treasury. (2024a). *Expanding the CDR to non-bank lending and narrowing the scope of CDR data in banking*. Australian Treasury. https://treasury.gov.au/sites/default/files/2024-11/c2024-598346-is-scope.pdf

Australian Treasury. (2024b). *Competition and Consumer (Consumer Data Right) Amendment (2024 Measures No. 2) Rules 2024*. Australian Treasury. https://treasury.gov.au/sites/default/files/2024-11/c2024-598346-ed.pdf

Bendigo Bank. (2021). *Bendigo and Adelaide Bank to acquire Ferocia to accelerate digital strategy, Up's growth and shape the future of banking*. Bendigo Bank. https://www.bendigobank.com.au/media-centre/bendigo-and-adelaide-bank-to-acquire-ferocia/

Bolam, B. (2025). *How the evolution of the CDR unlocks new opportunities for non-bank Lenders*. CFOtech. https://cfotech.com.au/story/how-the-evolution-of-the-cdr-unlocks-new-opportunities-for-non-bank-lenders

Booth, J. (2025). *Non-bank lenders join the CDR!*. Biza.io. https://biza.io/non-bank-lenders-join-the-cdr/

Common Wealth Bank (CBA) (2021). *2021 Annual Report*. Common Wealth Bank. https://www.commbank.com.au/content/dam/commbank-assets/about-us/2021-08/2021-annual-report_spreads.pdf

Common Wealth Bank (CBA). (2022). *Submission in response to the Statutory Review of the Consumer Data Right – Issues Paper*. Australian Treasury. https://treasury.gov.au/sites/default/files/2022-09/c2022-314513-commonwealth_bank_of_australia.pdf

Consumer Data Right (CDR). (2024). *IT requirements for data holders*. Australian Government. https://www.cdr.gov.au/for-providers/it-requirements-data-holders

Data Standards Body (DSB). (2020a). *Data Standards Advisory Committee meeting minutes – 12 August 2020 (Banking)*. Data Standards Body. https://dsb.gov.au/sites/consumerdatastandards.gov.au/files/uploads/2020/09/DSB-Committee-Minutes_Banking_Aug-2020_Final.pdf

Data Standards Body (DSB). (2020b). *Data Standards Advisory Committee meeting minutes – 11 November 2020 (Banking)*. Data Standards Body. https://dsb.gov.au/sites/consumerdatastandards.gov.au/files/uploads/2020/12/DSB-Committee-Minutes_Banking_Nov-2020.pdf

Data Standards Body (DSB). (2021). *Data Standards Advisory Committee meeting minutes – 12 May 2021 (Banking)*. https://dsb.gov.au/sites/dsb.gov.au/files/2025-04/210512%20DSAC%20Minutes_Banking.pdf

Jones, S. (2025). *Consumer Data Right expansion to deliver a better deal for consumers*. Australian Treasury. https://ministers.treasury.gov.au/ministers/stephen-jones-2022/media-releases/consumer-data-right-expansion-deliver-better-deal

Office of the Australian Information Commissioner (OAIC). (2024). *Openness and transparency: Energy retailers' management of Consumer Data Right data*. Office of the Australian Information Commissioner. https://www.oaic.gov.au/__data/assets/pdf_file/0033/241989/Energy-retailer-CDR-policy-assessment-summary.pdf

Origin Energy. (2024). Consumer Data Right (CDR) Rules – Operational Enhancement Amendments – Consultation Paper. Australian Treasury. https://treasury.gov.au/sites/default/files/2024-11/c2024-600257-origin_energy.pdf

Regional Australia Bank (RAB). (2020). *Regional Australia Bank becomes CDR compliant*. Regional Australia Bank. https://www.regionalaustraliabank.com.au/about-us/the-inside-story/articles/regional-australia-bank-becomes-cdr-compliant

Up Bank. (2021). *Up is Open for Business with Open Banking*. Up Bank. https://up.com.au/blog/open-for-business-with-open-banking/

Up Bank. (2021). *Up: Most Trusted*. Up Bank. https://up.com.au/press-releases/up-most-trusted/

Up Bank. (2024). *Consumer Data Right Policy*. Up Bank. https://up.com.au/cdr-policy/