IDC ANALYST CONNECTION

Sponsored by: Okta

The Consumer Data Right (CDR) initiative in Australia is a positive step in empowering Australian businesses towards an open data economy and business transformation. It promises far-reaching value for consumers and businesses through creation and delivery of innovative, data-driven services and solutions. It is imperative for businesses to invest appropriately in preparing and building the requisite infrastructure to enable data management, data sharing, and in particular, data security and privacy.

Consumer Data Right in Australia - Opportunities and Challenges

July 2022

Questions posed by: Okta

Answers by: Dr. Chris Marshall, Vice President; and Sandeep Sharma, Senior Research Manager, IDC Asia/Pacific

Q1. How can CDR (Consumer Data Right) and the drive towards an open data ecosystem create innovative services and deliver value for consumers in Australia? How might it benefit Australian businesses?

Data provides the basic fuel needed for the digital transformation of the Australian economy. But the data's usefulness depends largely on how well it is captured, managed, described, and shared. The Consumer Data Right (CDR) supports Australian data sharing and monetisation by addressing consumers' concerns regarding data ownership, control, and privacy, giving consumers control of their data while enabling regulated usage by third parties. For example, CDR enables consumers to compare products quickly, receive personalised recommendations and user experiences, and access to innovative new solutions without sacrificing data security, privacy, and ownership. Businesses, on the other hand (especially fintech firms), can avail of consumer data to launch emerging solutions in lending, personal finance, energy usage optimisation, insurance.

CDR is not merely a regulation to support consumers, it is also poised to increase data availability for businesses in the country — and is expected to spur innovative new digital businesses, products, and services. **According to the IDC *APeJ CEO Study 2022*, Australia and New Zealand organisations derived 28% of their revenues from digital products, solutions, and experiences in 2022, and this is expected to reach 43% by the end of 2027.** ANZ businesses are considering multiple digital business models including industry digital ecosystems (72%), as a service (55%), direct to consumer (52%), and data monetisation (41%) to accomplish this. Sectors impacted by CDR will see the emergence of newer players that will provide innovative new services. Increased competition will drive greater market efficiencies and, ultimately, benefit consumers. CDR promises less friction, and more timely and transparent delivery of citizen services.

Q2. Which industries stand to benefit from CDR? What are the likely use cases across different industries?

Banking has been the initial beneficiary of the Open Data and CDR initiative since early 2019/20. To date, all the major banks and non-major banks can share and use consumer data for multiple use cases. These include sharing data about personal finance (budgeting advice, access to bank accounts, savings tools, simplified investment tools, loans); consumer and business lending; buy now pay later (BNPL); mortgage and real estate lending; payments.

The CDR program will be extended in phases to other sectors such as energy and utilities (in October 2022), followed by telecommunications, superannuation, insurance. The **energy sector** in the country might leverage data from CDR in myriad innovative use cases such as subscription and energy as a service; crafting tariffs structures based on customer profiles; and so on. In the **telecommunications** space, consumers might access more accurate information about their usage, product plans, and switch more easily between providers.

Overall, with the growth of the digital economy in Australia, the CDR initiative will serve as a platform for data sharing and value creation activities across a multitude of sectors and across countries, thereby paving the way for an open data economy. Some of the sectors that could witness growth in value and innovation in the future due to the application of the CDR include healthcare, education, retail, and supply chain, travel and transportation, agriculture, and the public sector (government services delivery). Additionally, with the necessary standards and infrastructure in place, and combined with the equivalence of principles and interoperability with regard to standards and governance of the data sharing initiatives in other countries, this could potentially lead to a more integrated cross-border data sharing ecosystem.

Q3. CDR has already been implemented for open banking. How successfully has banking adopted CDR? And how has the banking industry's success, or lack of it, impacted related industries such as fintech in Australia?

Since the launch of the CDR in 2020 in banking, banks, large and small, have seized this opportunity to establish new processes around existing products including savings accounts, credit card accounts, lending, mortgages, and transaction accounts. As of the end of June 2022, a total of 76 data holders and 31 data recipients (both active as well as accredited) exist in the CDR banking ecosystem in Australia. It is still early days for open banking in Australia; however, fintech players are starting to partner with banks to provide new products and services to consumers and businesses. We expect many new use cases to develop such as lending (where data sharing will be leveraged for income and expense verification, and credit scoring), personal finance and money management, customer onboarding, identity verification, and so on. Meniga, a fintech firm in Australia, leverages consumer data to provide personal finance solutions; Frollo is one of the leading companies in the country that collaborates with banks and financial services firms and provides financial wellness solutions; the Commonwealth Bank of Australia has launched x15ventures that aims to fund and create 25+ innovative ventures by 2024. It has already launched ventures such as Home-in (to make the process of home purchases smoother for consumers), and Credit Savvy (to enable consumers to access their credit score and credit health for further activities).

However, there are challenges that hinder adoption and lead to a slower than expected uptake in the near- to mid- term. Data holders and recipients are required to make significant investments in several data management, sharing, and security initiatives. It might be cumbersome for the data holders specifically to ingest and integrate data from a myriad of sources and ensure data quality and integrity at the same time. Data movement, duplication (or replication) could prove to be expensive for enterprises and SMEs. There needs to be conscious investments in data sharing policies and technology platforms (for instance, API platforms, data sharing dashboards). Data security and privacy have to be impenetrable to prevent unwarranted data leaks, and will need investments in identity and access management, API security, threat management. These investments (to get accredited) could be a cause for concern, especially for SMEs. In the recent past, organisations, such as fintech firms and SMEs in particular, have also been disheartened by the complexity of accreditation rules, and limited practical use cases that might not prove to be of any real value for consumers. Lower value creation is also dependent upon relatively lower levels of customer awareness and trust of data sharing.

Q4. What has the experience been like for current data holders, given the consistent evolution of CDR? What lessons might apply to future CDR implementations?

Based on the experience of banks, CDR can be seen as a platform for innovation and not as a compliance directive. There are significant first-mover advantages in leveraging the initiative to increase business efficiency, craft new solutions, optimise supply chains, and so on. Businesses need to build a strong data management and governance mechanism (for data protection, privacy, and compliance), supported and protected by a robust cybersecurity infrastructure.

In many organisations, an overhaul of the existing IT, data, and cybersecurity infrastructure is long overdue. Interconnectedness is the key here, and should be driven by a comprehensive API management strategy and platform (replete with API security). Considering the significant cost implications, it is also imperative for businesses to identify and prioritise use cases to reap advantages from CDR. Security, identity and access management solutions that enable data sharing, consumption, and monetisation are no longer merely nice to have — they have become a necessity for compliance.

Q5. What business and IT architectures are best suited for seamless adoption of CDR? How does this vary for enterprises and smaller businesses? What should be the adoption road map for businesses?

CDR requires businesses to invest in several capabilities to strengthen processes, technologies, and resources related to the twin areas of data management and governance, and cybersecurity. Data quality and security are critical avenues for both data holders and recipients in the open data ecosystem — the necessary safeguards have to be in place to ensure these. A well-defined data governance framework (and associated IT infrastructure) is also required. Businesses must ensure that there is a comprehensive assessment of the current state of processes, systems, and policies around data management, data sharing, and cybersecurity. The architecture must include a robust API management and security platform, as this will form the basis for openness and interconnectedness. In addition, firms need adequate processes and technologies for data retention, minimisation, anonymisation, erasure, consent management, and consumer dashboards. Businesses should leverage a comprehensive identity and access management platform combined with data protection solutions.

Larger enterprises with their financial and manpower strengths could decide to implement CDR either on their own or with limited help from external parties. On the other hand, small businesses must clearly define the use cases, build a business case, start small, and almost certainly enlist the support of an external partner for their CDR implementation process.

The adoption road map for businesses (both large and small) includes the creation of a broader open data strategy, governance framework, followed by identification of relevant use cases in select business functions/processes. This may be followed by a strategic assessment of the necessary infrastructure (and gaps) in technologies and processes in data management and cybersecurity. The next step has to be sustained investments in relevant technologies (particularly data security, privacy, identity and access management, and API platforms) to craft an open data platform. Continuous monitoring (KPI assessment) and feedback have to be built in as a key activity as well.

Q6. Security, privacy, and trust are central pillars in the overall schema of CDR implementation. What best practices in identity and access management should be considered by businesses?

The success of an open data strategy and the CDR implementation is largely dependent upon the centrality of cybersecurity infrastructure. Businesses must invest significantly in securing their API infrastructure and communication channels. API security standards must be decided upon and followed. Data usage (in motion, at rest, or in use) has to be protected at all times. Identity and access management (IAM) assumes importance and is critical to the overall CDR implementation. Businesses must follow several best practices in the area of IAM. They must follow the principles of zero trust and the principle of least privilege. This must be ably supported by a strong, interoperable identity management platform that can automate workflows and processes as much as possible. Use of multifactor authentication is advisable to ward off threats. Additionally, businesses must also leverage role-based as well as attribute-based access control policies. Continuous monitoring of the cybersecurity infrastructure is key; it needs to be backed up with proactive security measures such as security audits, and the usage of emerging technologies such as AI.

About the Analysts

	Dr. Chris Marshall, *Vice President, Data, Analytics Asia/Pacific* His core research coverage includes the development of data analytics and machine learning competencies and their implications — the threats and opportunities facing organisations as they seek to augment and automate their knowledge-based work.
	Sandeep Sharma*, Senior Research Manager* Sandeep advises tech buyers (CIOs and lines of business) on strategic initiatives such as digital transformation, open data, services procurement and outsourcing, and others.

IDC Custom Solutions

IDC Asia/Pacific

83 Clemenceau Avenue
#17-01 UE Square West Wing
Singapore 239920
T 65.6226.0330
Twitter @IDC
idc-community.com
www.idc.com