UNLOCKING VALUE WITH CONSUMER DATA RIGHTS RULES
While the Consumer Data Right (CDR) rules are being finalised, the outline has been published. Australian banks have started their compliance journey to meet the new open banking standard.

As banks prepare themselves for the seismic transition from a closed model to being able to share high-quality and accurate data with third parties, they face two immediate needs. First, strong data governance; and second, a robust data management framework that offers adequate data privacy and security measures.
Data privacy and Open Banking gain global traction

Globally, along with changing consumer preferences, concerns regarding data collection, privacy, and security are growing. As regulators around the world continue to closely observe Europe’s Payment Services Directive 2 (PSD2) and the General Data Protection Regulation (GDPR), many are already in the advanced stages of drafting equivalent open banking standards and data protection regulations.

PSD2 regulates banks in the EU to grant third party providers access to payment accounts for account information and payment initiation. CMA (Competition and Monetary Authority) regulated the 9 largest UK private banks to form an Open Banking Implementation Entity.

Monetary Authority of Singapore “Finance-as-a-Service” playbook to boost Open API adoption. Japan to open up by 2020. Hong Kong Monetary Authority to regulate tier-1 HK banks to open up APIs. Furthermore, several Open Banking related GovTech initiatives in India, China, Singapore.

Australian Treasury Department finalising Open Banking Standards by February 2019. New Zealand: Banks recently started Open Banking pilot.

South Africa: PSD2 is watched closely. SARB (South African Reserve Bank) should “drop” a report regulating a “Sandbox API”. In Nigeria, API Banking use cases for financial inclusion gaining traction.

US CFPB pushing for customer-authorized access to data as alternative for screen scraping. Canadian government is studying the introduction of Open Banking regulation.

Fintech and Open Banking bill passed in Mexico.

The consumer data right rules framework is more than just Open Banking

The Consumer Data Right Rules Outline released by the Australian Competition & Consumer Commission (ACCC) in December 2018 focuses on much more than just opening the closed and traditional banking model. While the rules try to empower consumers with the right to correction (like the subject rights in GDPR), enabling customers to rectify their data in 30 calendar days, they also require CDR participants to draft a policy on open and transparent data management that is independent of any existing privacy policy.

The rules prescribe the need for adequate quality and security measures before data can be shared with third party providers. This provides banks with a perfect opportunity to leverage the CDR rules framework to establish a strong data governance platform focused on data quality, transparency and traceability.

Australian banks will also need to comply with other ongoing data-centric regulatory initiatives such as the Basel Committee on Banking Supervision’s standard number 239 (BCBS239) and the GDPR. In doing so they may see cross-regulatory synergies.

Proposed consumer data right rules

In response to the growing pace of technological innovation and the increasing risk and sophistication of data theft, the CDR rules underline the importance of having a strong, well-defined and well-governed data framework.

Some of the key CDR rules highlights include:

A) Multiple Regulator Model
The ACCC will be responsible for standards-setting while the Office of the Australian Information Commissioner (OAIC) will examine the privacy impacts.

B) Sector-by-sector implementation
The CDR will be implemented on a sector-by-sector basis, starting with the banking sector. This gives all other industries, especially data-centric ones such as telecommunications, more time to plan the implementation.

C) Phased implementation
The banking sector will be required to begin sharing data in phases, with the first wave to be opened up by 1 July 2019 (see Figure 2).

D) Consent / authorisation management
Data holders and data recipients will need to obtain customer consent before customer data can be shared.

E) Consumer dashboard
Data holders and recipients will need to create a consumer-facing dashboard showing all data-sharing authorisations...
(active and historical) that the customer has given. The dashboard should also record the disclosure of data.

**F) Right to correction**
Data holders and recipients must correct any CDR data which a consumer deems incorrect or redundant. They must respond to requests for rectification within 30 calendar days.

**G) Open and transparent data management**
Data holders and recipients must have a CDR policy on data management that is independent of any existing privacy policy. The policy should be easy to understand and drafted in a way that promotes consumer engagement.

**H) Notification of collection and disclosure**
Data holders and recipients must record disclosure of data in consumer dashboards.

**I) Quality and security of data**
Data holders and recipients must ensure that the CDR data being shared is accurate, current and complete for the purpose for which it is held. Recipients must also undertake adequate precautions to ensure data security.

**J) Record keeping and reporting**
Data holders and recipients will be responsible for collecting and maintaining records of complaints and disputes and reporting these biannually. They will have to retain the records for six years.

---

**Figure 2: CDR Rules Implementation Phases for Banks**

<table>
<thead>
<tr>
<th>PHASE I</th>
<th>PHASE II</th>
<th>PHASE III</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Products in scope</strong></td>
<td><strong>Products in scope</strong></td>
<td><strong>Products in scope</strong></td>
</tr>
<tr>
<td>• Savings accounts</td>
<td>• Residential mortgages</td>
<td>• Business Finance</td>
</tr>
<tr>
<td>• Call accounts</td>
<td>• Investment mortgages</td>
<td>• Personal Loans</td>
</tr>
<tr>
<td>• Term deposits</td>
<td>• Mortgage offset accounts</td>
<td>• Lines Of Credit (Personal)</td>
</tr>
<tr>
<td>• Current accounts</td>
<td>• GST and tax accounts</td>
<td>• Lines Of Credit (Business)</td>
</tr>
<tr>
<td>• Cheque accounts</td>
<td>• Credit and charge cards</td>
<td>• Overdrafts (Personal)</td>
</tr>
<tr>
<td>• Debit card accounts</td>
<td></td>
<td>• Overdrafts (Business)</td>
</tr>
<tr>
<td>• Transaction accounts</td>
<td></td>
<td>• Asset Finance</td>
</tr>
<tr>
<td>• Personal basic accounts</td>
<td></td>
<td>• Cash Management Accounts</td>
</tr>
<tr>
<td>• GST and tax accounts</td>
<td></td>
<td>• Farm Management Accounts</td>
</tr>
<tr>
<td>• Credit and charge cards</td>
<td></td>
<td>• Pensioner Deeming Accounts</td>
</tr>
<tr>
<td>Date of compliance</td>
<td><strong>Product Data</strong> – Jul 01, 2019</td>
<td>Feb 01, 2020</td>
</tr>
<tr>
<td><strong>Other Data</strong> – Feb 01, 2020</td>
<td><strong>Other Data</strong> – Feb 01, 2020</td>
<td><strong>July 01, 2020</strong></td>
</tr>
</tbody>
</table>

CDR combines aspects of different European regulations

The CDR echoes PSD2 with its requirement that banks open up their customer account information to third parties. It also incorporates several aspects of the GDPR, including the right to data rectification, active consent/authorisation management and data minimisation measures.

There are, however, key differences between the CDR and its European counterparts. For one thing, the scope of the CDR includes lending accounts while PSD2 and the GDPR do not.

The Australian and European schemes also differ in terms of actions in scope: PSD2 and UK Open Banking allow actions such as payments initiation and account opening while the CDR allows read-only access. Having said this, we are already seeing potential use cases in Australia for the combination of the CDR and the New Payments Platform (NPP) to create new digital services for businesses and consumers that effectively leverage both read and write capabilities.

(Our September 2018 paper, Open Banking and the New Payments Platform: Unlocking Real-Time Commerce, discusses this in more detail.)

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>KEY FEATURE</th>
<th>EU GDPR</th>
<th>EU PSD2</th>
<th>Australia (CDR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of Information in scope</td>
<td>Transaction data</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Account support data</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Customer identity</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>AML/CTF support</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Accounts in scope</td>
<td>Transaction/savings</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Credit cards</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Personal loans</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Mortgages</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Business loans</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Actions in scope</td>
<td>Read data</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Initiate transactions</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Open accounts</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Initiate application</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Privacy standards</td>
<td>Right to erasure</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Block solicitation/profiling &amp; SCA</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Data Protection Office</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Pseudonymisation</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Consent Management</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Consumer Dashboard</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Breach Management</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

Source: Qualitative Analysis, Accenture 2019
How CDR impacts data, technology, processes and people

The implementation of the CDR is likely to profoundly change Australia. As the banking industry adopts the rules framework and other industries follow, the impact will be widely felt by consumers and third-party providers.

Importantly, consumers will have the ability to direct that the data be safely transferred to trusted and accredited service providers of their choice. For Australian banks, the CDR will have a significant impact on the entire process, system and data landscape.

Consumers will benefit from the new regime as they will enjoy a better choice of banking products as well as potentially reduced costs due to greater competition. Along with the ease of switching between different service providers, including fintech firms and start-ups, consumers will have greater access to and visibility of their own data that banks hold.

Figure 4: Impacts of CDR on Banks

Bubble size indicates impact magnitude

1 Sharing of Customer Data
2 Consent / Authorization Management
3 Customer Dashboard
4 Open and Transparent Management of Data
5 Anonymity and Pseudonymity
6 Notifying the collection and disclosure of CDR data
7 Quality of CDR data
8 Security of CDR data
9 Correction of CDR data
10 Record keeping and Reporting

Source: Qualitative Analysis, Accenture 2019
The top three factors impacting banks today are:

1. **Sharing customer data**
   
   The data-sharing aspect of the CDR will necessitate the development of secure application programming interfaces (APIs), the implementation of data minimisation standards, and measures to ensure adequate data quality as well as data correction features. This will require a major overhaul of banking systems and processes. The entire system landscape, including ledgers, data warehouses, data marts and risk and reporting systems will need to undergo changes along with different banking processes.

   Banks will also need to invest in improving their end-to-end product and pricing data capabilities, which have typically evolved in a myriad of legacy systems and spreadsheets. This will need to become industrial-strength, automated and API-enabled to support the requirements of the CDR. And, most importantly, banks will need to ensure the data is always accurate and valid.

2. **Consent / authorisation management and consumer dashboard**
   
   The CDR will require banks to implement effective and efficient consent management policies and processes and establish dashboards. It will become essential for banks to be able to demonstrate clear governance around collecting and managing customer consent and authorisations before data is shared.

3. **Open and transparent management of data**
   
   Banks will have to create a separate data management policy as well as review all existing policies and frameworks surrounding different data management practices today, including existing data minimisation measures, data retention policies and anonymisation/pseudonymisation techniques.

   Consumers will benefit from the new regime as they will enjoy a better choice of banking products as well as potentially reduced costs due to greater competition.
Using lessons learned from similar global initiatives

Banks should use the lessons learned from global initiatives on open banking and data privacy to gain time and cost synergies when implementing CDR rules.

Banks in Europe (and globally) struggled in their journey to GDPR compliance due to the complexity of the regulation and the huge impact on data, systems and processes, coupled with the short implementation time of only two years. Another burden was the introduction of the Payment Services Directive II (PSD2), which became applicable on 13 January 2018.5

Due to the extremely complex nature of these regulations, tight timelines for implementation, and high penalties for non-compliance, banks and financial services companies across the globe have struggled to execute solutions. Whilst there are many synergies between the two sets of regulation, financial services firms have tended to address each separately. As a result, they have not been able to fully realise the benefits of undertaking a co-ordinated and combined approach.

Some of the key lessons from their experience include:

- **Concerns over reputational risk and being a trusted brand**
  For many organisations, avoiding reputational damage is viewed as more important than being compliant with regulators. E.g. Concerns over being the first to be fined in the industry.

- **First-mover advantage**
  Time to market is key. Leading market participants should take advantage of the current regulatory chaos by being first movers and thereby dictating market adoption in data privacy.

- **Align with other ongoing initiatives**
  From the outset, the CDR implementation should align with other ongoing data protection initiatives such as the GDPR. There is an opportunity to run common activities, so the entire data-driven regulatory portfolio can leverage the synergies between the different regulations.

- **Improve customer trust and experience**
  The CDR should not be viewed simply as a regulatory tick mark. Banks need to focus on delivering a differentiated positive customer experience as well as continue to maintain and improve customer trust.

- **Rotate to the new**
  Australian banks should use the CDR as a tool to rotate to the new and derive competitive advantage by leveraging the latest technologies, especially artificial intelligence, robotics, machine learning and advanced data analytics.
The countdown to compliance deadlines starts now

With a few months remaining for banks to meet their compliance obligations, it’s important to act now.

As we’ve seen in Europe, banks have struggled with implementing PSD2 and GDPR due to regulatory complexities. With a phased implementation for the CDR rules, banks in Australia will benefit by first starting with a clear, well-defined action plan and focused initiatives.

Like any other regulatory initiative, banks will need to start with an assessment of the current state of the processes, systems and policies of not only their APIs, and the quality of data they hold, but also of current processes around data retention, data minimisation and data anonymisation.
AUTHORS

Tales Lopes
Managing Director, Finance, Risk and Compliance Practice Lead for Australia and New Zealand, Accenture Financial Services
tales.s.lopes@accenture.com

Graham Rothwell
Managing Director, Asia Pacific Payments, Accenture Financial Services
g.rothwell@accenture.com

Bikram Paul Choudhury
Manager, Finance, Risk and Compliance, Accenture Financial Services
bikram.choudhury@accenture.com

REFERENCES


https://eugdpr.org/the-regulation/gdpr-faqs/
ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world’s largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 469,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

DISCLAIMER

The views and opinions expressed in this document are meant to stimulate thought and discussion. As each business has unique requirements and objectives, these ideas should not be viewed as professional advice with respect to your business.