HERBERT
SMITH
FREEHILLS

APPROACHING CDR ACCREDITATION: POSITIONING FOR SUCCESS

20 November 2020 | Insight
Legal Briefings – By **Julian Lincoln, David J Ryan and Siobhan Lane**

As Australia rolls out its new consumer data right regime, we assess the key role of accreditation for firms dealing in data

THE CDR ACCREDITATION LANDSCAPE

Several months after consumer data sharing under Australia's Consumer Data Right (**CDR**) framework commenced (1 July 2020) for the banking sector, only six entities have been successfully accredited as data recipients. To date, significant traction on CDR opportunities has not been apparent, which may well have been influenced by the impacts of and progressive recovery from COVID-19. As levels of activity in the Australian fintech sector continue to rise, now is an opportune time for organisations seeking to enter this growth sector to engage with the CDR accreditation process to ensure that they are best positioned to become competitive in the CDR ecosystem.

Although the ACCC recently concluded its consultation on changes to the CDR Rules to provide for different tiers of accreditation (which will be beneficial to encourage more fintechs to enter the CDR ecosystem), by making the investment now to become accredited at the unrestricted level, organisations can position themselves to exploit opportunities presented by the CDR, now and into the future. Further, if CDR data access is expanded to "write" access (as is currently being considered by the Inquiry into Future Directions for the Consumer Data Right), opportunities for accredited data recipients (**ADRs**) to provide functions such as payment initiation (and facilitate payments more broadly) are likely to provide organisations with broader opportunities to bring compelling offerings to the market.

The ACCC's Accreditation Guidelines for the CDR detail process and technology aspects of accreditation. Businesses are recommended to focus in particular on the following three key areas when working to become CDR-ready:

- maintaining a robust information security capability;
- managing relationships with outsourced service providers; and
- obtaining adequate, risk-based insurance.

INFORMATION SECURITY

Under the Accreditation Guidelines, accredited entities are required to implement and maintain an information security (**IS**) capability that is '*appropriate and adapted to respond to risks to information*' having regard to factors such as the extent and nature of threats to CDR data and the potential loss or damage to CDR consumers if all or part of the consumer's data were to be lost, interfered with or disclosed. When applying for accreditation, an applicant must provide an assurance report to demonstrate that it satisfies the CDR regime's IS requirements. Notably, accreditation applications may now use ISO 27001 certification, in conjunction with an assurance report covering the controls not covered by the ISO 27001 certification, to evidence that they meet the CDR IS requirements for accreditation. To meet the CDR framework's IS requirements organisations will need to take actions including:

While organisations can leverage their existing IS governance and capabilities as a baseline, systems and processes must be revised and adjusted to meet the CDR IS requirements. At a minimum, organisations are expected to:

IMPLEMENT PROCESSES TO LIMIT THE RISK OF INAPPROPRIATE OR UNAUTHORISED ACCESS TO THE CDR ENVIRONMENT

Implementing appropriate staff training is critical for managing unpredictable cyber security and privacy risks, especially as employees continue to work remotely during the coronavirus pandemic. To address this risk, organisations should consider:

- conducting background checks on all personnel prior to granting access to the CDR environment; and
- introducing CDR-specific training to educate personnel about (i) the security and privacy risks associated with the CDR data environment and (ii) what they can and cannot do when interacting with the CDR data environment.

SECURE THE NETWORK AND SYSTEMS WITHIN THE CDR DATA ENVIRONMENT

To address the security requirements in the Accreditation Guidelines, organisations should apply a range of robust technical controls, including:

In light of the heightened risk profile of staff working remotely, organisations should also seek to deploy the most recent and appropriate security patches, harden end-user devices in accordance with accepted industry standards, and consider using two factor authentication for internet facing systems and portals (to the extent not already part of standard operating procedures).

For CDR entities which are also APRA-regulated entities, it is important to appreciate the differences between the security requirements and expectations mandated under APRA's Prudential Standard CPS 234 and those included in the Accreditation Guidelines. Undertaking a detailed gap analysis between the two regimes will ensure a better and more transparent risk management position internally and also facilitate negotiations with third party service providers where contractual uplifts are required to ensure compliance.

MANAGE INFORMATION ASSETS WITHIN THE CDR DATA ENVIRONMENT OVER THEIR LIFECYCLE

Introducing data loss and leakage prevention mechanisms will help to prevent CDR data leaving the confined CDR data environment. To do so, organisations must: (i) block access to unapproved cloud computing services, (ii) record and monitor outbound emails (including recipient, file size and frequency); and (iii) mask CDR data, prior to being made available in non-production environments. Robust CDR data backup, retention, deletion and de-identification processes should also be documented and implemented.

OUTSOURCED SERVICE PROVIDERS

When implementing CDR data management frameworks, CDR participants may consider engaging outsourced service providers (**OSPs**) to augment internal capability and capacity. OSPs may help organisations to meet their CDR needs by providing specialised capability or expertise in areas such as data infrastructure, cyber security and data risk management.

Recent amendments to the CDR Rules have also expanded the circumstances in which ADRs can engage accredited intermediaries to perform functions on their behalf (see further detail about this recent development here). As a result of these amendments, accredited intermediaries can now *collect* CDR data on an ADR's behalf as part of a Combined Accredited Person (**CAP**) arrangement. Expanding the roles of intermediaries in this way (with future expansion also likely if further accreditation levels are introduced) opens up further opportunities for ADRs to operationalise and expand their service offering.

Despite the broadening of the circumstances in which OSPs can be used, any use or disclosure of CDR data by an OSP (regardless of whether the OSP is an accredited intermediary or not) is taken to have been undertaken by the ADR. As such, even if an OSP breaches the CDR IS obligations (including subsequent incident management and reporting requirements), the ADR itself remains liable. This consideration is particularly important because, regardless of the risk allocation provisions that are included in any arrangement with an OSP, ADRs are not able to transfer regulatory or reputational risk. As such, ADRs are unlikely to be compensated for all losses suffered in the event of an OSP's breach (even if full financial recovery is provided). Given this context, ADRs should be conscious of balancing the potential benefit of outsourcing against risks associated with potential breaches, expanding the CDR data environment, and potential impacts on insurance obligations as a result of increased third party interaction with CDR data.

If an ADR decides to engage an OSP, it should:

- undertake thorough initial due diligence on both the OSP and the relevant solution to identify any deficiencies in the OSP's relevant controls (as well as part of an ongoing formal controls assessment program);
- precisely define the roles of any OSPs and the terms on which they disclose any CDR data to OSPs; and
- implement frameworks such as security questionnaires, site visits, third party IS audit and assurance and back-to-back IS governance policies and controls on OSPs where possible.

INSURANCE REQUIREMENT

Entitles seeking accreditation are required to obtain adequate insurance cover (or a comparable guarantee) to guard against the risk of CDR consumers not being properly compensated for any loss that might reasonably be expected to arise from a breach of the ADR's CDR obligations in managing CDR data.

The regulators' have not prescribed specific insurance products that must be obtained to meet the CDR insurance obligations. Whilst the Accreditation Guidelines suggest that professional indemnity insurance or cyber insurance could provide the required level of cover, we are yet to see how the insurance market will respond to the CDR (particularly whether extensions to existing policies will be offered, or if specific CDR products will be launched). Against this backdrop, when planning to meet the stipulated insurance requirements, entities should:

UNDERTAKE A BESPOKE RISK ASSESSMENT TO DETERMINE DATA-RELATED RISKS REGARDING THE ENTITY’S SERVICES, PRODUCTS AND ACTIVITIES (INCLUDING CDR DATA MANAGEMENT)

Entities should:

- consider the boundaries of their CDR data environment.
- aim to limit the volume of CDR data that they collect and process to decrease their risk profile. If an entity manages sensitive data, it will likely require a more comprehensive insurance framework.
- review the scope of available insurance options and any applicable policy limits (including annual aggregate insurance limits) to determine if the services and/or products provided will be captured.
- consider their financial ability to cover the excess and any gaps in cover due to insurance exclusions, and review insurance options accordingly. External dispute resolution claims, and privacy and data related claims must not be excluded.
- if engaging OSPs, consider whether third party liability is covered. If not, relationships with OSPs (and associated risks) should be managed appropriately. Entities should also consider if their employees and associates are covered by the different policies.

OBTAIN APPROPRIATE INSURANCE COVER FOR YOUR BUSINESS

In light of future opportunities that may arise, entities should consider entering into flexible insurance arrangements that can be modified if required to respond to different risk profiles (especially if write access is permitted in future). Additionally, as the CDR develops, the insurance market may offer CDR-specific insurance policies which entities may consider obtaining.

CONTINUALLY REVIEW INSURANCE COVER (OR COMPARABLE GUARANTEE) AT LEAST ANNUALLY TO ENSURE THAT IT CONTINUES TO SATISFY THE INSURANCE OBLIGATIONS

If there are any major changes to the business, such as a new product offering or increase in CDR data type or volume, insurance cover may need to be adapted.

FUTURE OPPORTUNITIES

The accreditation process is not straight-forward and requires interested businesses to evaluate the current and future state of their IT systems, personnel and operations. When establishing their CDR environments, prospective ADRs should be mindful of both currently known accreditation requirements and how future potential CDR opportunities may require changes to be made to their IS capabilities, relationships with third parties, and insurance. ADRs should also review the ACCC and OAIC's compliance and enforcement policy to ensure they understand the risks of non-compliance with these ongoing obligations (see our article on CDR compliance and enforcement here).

Ultimately, if CDR participants are provided with new forms of access to CDR data in the future, having existing data controls, governance frameworks and infrastructure that can be adapted to enable opportunities that present will be key to achieving leadership in Australia's knowledge economy. Organisations that wish to take advantage of the CDR but are challenged by the complexity of the accreditation process are encouraged to speak to our CDR experts.

Please click here to return to our CDR showcase page

SHARE

Share to Facebook Share to Twitter Share to LinkedIn Email Print

Show Share Links

RELATED TOPICS

Emerging Technologies

FEATURED INSIGHTS

FEATURED INSIGHTS

HELPING YOU STAY AHEAD OF THE BIG ISSUES

BROWSE BY:

- TECH, DIGITAL & DATA

- GEOPOLITICS AND BUSINESS

- NEW BUSINESS LANDSCAPE

RELATED ARTICLES

Tax in M&A in the UK and Europe – What you need to know

Crypto winter is here – what does it mean for insolvency practitioners?

Deal or no deal? Bring disputes lawyers in early to close that deal

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

JULIAN LINCOLN
PARTNER, HEAD OF TMT & DIGITAL AUSTRALIA, MELBOURNE
+61 3 9288 1694
Julian.Lincoln@hsf.com

PETER JONES
PARTNER, SYDNEY
+61 2 9225 5588
peter.jones@hsf.com

DAVID J RYAN
SPECIAL COUNSEL, MELBOURNE
+61 3 9288 1831
david.j.ryan@hsf.com

KAMAN TSOI
SPECIAL COUNSEL, MELBOURNE
+61 3 9288 1336
kaman.tsoi@hsf.com