Australian Business Software Industry Association

217 Flinders Street
Adelaide SA 5000
info@absia.asn.au | www.absia.asn.au

20 July 2020

CDR Rules Team
Australian Competition & Consumer Commission

Dear CDR Rules team,

ABSIA's Response to CDR Rules Consultation

The Australian Business Software Industry Association (ABSIA) welcomes the opportunity to make this submission on behalf of the business software industry. The Consumer Data Right (CDR) is an important initiative which impacts upon many of our members.

We have consulted with our members and present their collective views over the following pages. In summary, the business software industry's concerns are:

- Creating unnecessary barriers to participation for intermediaries, including the high cost of accreditation and ongoing compliance;
- Potential confusion about when data is "CDR data" and subject to CDR legislation versus when it is "other data" and not subject to CDR legislation;
- Conflicting data retention requirements. For example, accountants who are legally required to store certain data for set periods, have to delete this data under CDR rules;
- Not implementing prescriptive security controls (i.e. a "maturity-based approach") which avoid different interpretations that add costs, create disputes and increase cyber risk;
- Failing to leverage the experience from comparable frameworks such as the ATO's Operational Framework and ABSIA's Security Standard for Add-on Marketplaces (SSAM). Not leveraging this experience can add time and cost for all involved; and
- Ignoring potential learnings from the UK's Open Banking implementation.

ABSIA also encourages the ACCC to consult more with industry and professional associations such as ourselves, to better understand potential impacts within specific industries.

ABSIA would appreciate the opportunity to engage directly with the ACCC on these issues. For further information, please contact [redacted] ABSIA Director, on [redacted]

Yours faithfully,

[redacted]

Chris Howard
President & Director, ABSIA

ABSIA's Submission to ACCC CDR Rules Consultation

Unnecessary barriers to participation for intermediaries

A key aim of Consumer Data Right (CDR) is to spark innovation and the development of new products and solutions across the economy. The high cost of the accreditation requirements as well as ongoing compliance costs are a huge barrier to participation and innovation. While we acknowledge that standards are important to maintain appropriate levels of security and privacy, these costs are a barrier to participation especially for intermediaries.

FinTech Australia estimates that the cost of CDR accreditation is between $50,000 and $100,000 in annual compliance fees[1], but we understand that potential participants expect that costs could be up to $500,000. Banks currently have access to streamlined CDR accreditation based on existing certifications and regulations. Meanwhile, small developers are required to deal with the exact same complexity and cost as every other accredited data recipient (ADR). These small developers, and intermediaries in general, where they can sustain the upfront investment, will either need to absorb these costs themselves or pass the costs on to their users. The flow on effects of these costs to intermediaries is significant.

The ACCC must consider a tiered approach to accreditation as well as leveraging existing accreditation frameworks such as the ATO's DSP Operational Framework[2] and ABSIA's Security Standard for Add-on Marketplaces (SSAM[3]). ABSIA's experience with DSPs highlights that the absence of a tiered accreditation framework significantly constrains the participation of small and innovative software providers. It was this issue that directly led ABSIA to create, in conjunction with the ATO, the SSAM, which now supports hundreds of organisations within the DSP ecosystem.

In addition, creating and supporting multiple accreditation schemes is inefficient. Many DSPs are likely to be intermediaries within CDR. Requiring them to support a completely different accreditation process increases the compliance work and costs for the accounting, superannuation, payroll and other business software providers that the ACCC would encourage to participate in CDR.

[1] Figures quoted in Financial Technology and Regulatory Technology Inquiry issues paper

[2] https://www.ato.gov.au/General/Online-services/ATO-digital-wholesale-services/Digital-service-provider-Operational-Framework/

[3] https://www.absia.asn.au/industry-standards/addon-security-standard/

Potential confusion about data subject to CDR legislation

The types of data now subject to CDR rules have vastly changed from the original proposition. CDR rules have flowed on to other industries simply because they deal with banking data. When introducing the review into Open Banking in 2018, the purpose was described as follows:

> "Open Banking will revolutionise the financial services sector, transforming the way Australians interact with the banking system by giving consumers the right to safely share their data with other banks, other institutions and innovative FinTechs and get themselves a better deal." [4]

The industry wants clarification on whether the original purpose of Open Banking was meant to include all types of financial data, including that which flows to intermediaries, or if it happened naturally?

The evolution of how data is treated under CDR is confusing when considering the points at which CDR data becomes "normal data" within accounting software. For example, accounting software users gather many different types of data for a variety of reasons. This includes accounting, transactional and bank feed data, all of which can be potentially classified as CDR data. This data is treated no differently to the superannuation and STP data, for example, that accounting software currently collects. If there is no distinction between these data types, how are people like accountants and bookkeepers able to know when they are using CDR data and therefore handle it accordingly versus data collected via other means?

Conflicting data retention requirements

Data retention becomes a big issue when CDR data needs to be deleted when consent is not renewed or withdrawn under current CDR rules. Given accounting software providers are currently required to store financial, employee and other business records on behalf of their customers for 5-7 years there are conflicting data retention requirements. Legislation that details such record keeping requirements includes (but is not limited to) the following:

- Income Tax Assessment Act
- Corporations Act
- Fair Work Act
- Superannuation Industry (Supervision) Act

Without clarifying when CDR data stops being CDR data, it puts accounting software providers, accountants and bookkeepers in a difficult position regarding when they need to delete CDR-related data but not breach the relevant record keeping legislation. There needs to be a clear distinction between when this data stops being CDR data within accounting and other business software. This clarification should be provided along with an explanation of how CDR legislation will work with the legislation listed above on when it comes to deleting data.

---

[4] https://ministers.treasury.gov.au/ministers/scott-morrison-2015/media-releases/review-open-banking-giving-consumers-choice

If these rules do not change, it has the potential to undo much of the hard work undertaken by the business software industry to remove the red tape surrounding the automation of tax data.

Not implementing prescriptive security controls

The information security controls presented in the draft rules are quite high level leaving ADRs to make trade offs between cost and risk. It is important to understand that most standards specified by government departments are high level and involve layers of various subordinate standards which also include a range of options. The outcome is that organisations will only implement a subset of the options as supporting the full standard with all its various options is prohibitively complex and expensive.

Controls should be more prescriptive to provide clarity on what is considered to be the best practice approaches. For example, providing clarification on the preferred version of TLS instead of allowing ADRs to determine this themselves would improve the overall security of implementations.

It is critical for its effective operation that there is shared agreement on the options within the subordinate standards that will be implemented. This is particularly important where there are significant differences in the participants' market power and influence. It is also critical to ensure consistency across the various implementations to minimise the potential and cost of technical dispute resolution or large players dictating terms to smaller, less influential organisations.

If the security controls are left open to interpretation, it will also create potential auditing issues and leave decisions open to technical disputes. At the moment, there is no clear information in the draft rules on how to efficiently and fairly resolve such disputes.

We suggest that the ACCC reviews similar security standards like the ATO's DSP Operational Framework and ABSIA's SSAM which provides best practice information for each of the security requirements and outlines where specific requirements are mandatory or recommended. The SSAM and supporting information also outlines low and no cost solutions for third party software vendors to utilise.

We would also like to recommend the adoption of ISO27001 for ADRs and intermediaries.

Failing to leverage the experience from comparable frameworks

To avoid reinventing the wheel, there are many rules frameworks and existing implementations that Australia's CDR program can learn from.

From our experience, many ABSIA members have gone through the Operational Framework or the SSAM (or both). These standards should be recognised as appropriate accreditation methods for CDR. We understand that the ACCC is working through the process to broadly accept, on a principles based approach, the Operational Framework as one of the accreditation

mechanisms. In line with our previous suggestions, we encourage the ACCC to reconsider a tiered approach to accreditation, like the Operational Framework and SSAM.

Ignoring potential learnings from the UK's Open Banking implementation

Australia also has much to learn from the UK's experience with Open Banking. While it was slow on uptake, the platform has proven itself with no major breaches or issues so far. The program is now starting to see the innovation it was designed to create. The UK's Open Banking regime has proven to be quite successful without putting a huge burden on participants.

Complexity of managing consents

Open Banking is already struggling with participation. One factor adding complexity to the system is users needing to re-consent every 12 months. Even the smallest of businesses will have a relatively high number of consents to manage to keep their day to day operations running. On a larger scale, businesses with many more systems will find it virtually impossible to manage all their consents. To encourage participation, we must not overwhelm individuals and businesses with the amount of work needed to manage their consents. It is essential that the ACCC takes a holistic consumer centric approach rather than a sector by sector approach. A useful model for the ACCC to consider is the ATO's DSP Operational Framework and its RAM capability.