21 October 2022

Consumer Data Right Division
The Treasury
Langton Crescent
PARKES ACT 2600

BY EMAIL: data@treasury.gov.au

Dear Consumer RIghts Division,

Joint submission: CDR Rules - expansion to the telecommunications sector and other operational enhancements

Xero, Intuit and MYOB welcome the opportunity to provide feedback on Treasury's latest draft CDR Rules (the **Rules**) update released for consultation on 15 September 2022.

Xero, Intuit and MYOB are leading digital service providers (DSPs) supporting the majority of small businesses across Australia. To enable SMEs to grow their business and track business management processes, we offer services that enable our collective customers to securely share their banking data to their nominated accountant, bookkeeper or business manager (including relevant third-party apps) so they can track business growth, monitor cash flow and business trends, and stay compliant.

We consider the introduction of the Business Consumer Disclosure Consent (BCDC) and seven-year consents for businesses within the CDR framework as an appropriate and important addition to the regime, and welcome its proposed inclusion. These proposals better reflect the UK Open Banking regime model, which has played an important part in accelerating participation from individuals and non-individuals alike. With 2.4 million small businesses who stand ready to benefit from the BCDC, we are enthused by this proposal and see it as an important step to maximise the participation of small businesses within the CDR regime.

We note Australia's strong and overlapping privacy and security regulatory landscape for businesses, including but not limited to the Privacy Act, the ATO DSP Operational Framework, and the SSAM, will provide necessary protections for transfers of data for a business purpose under the BCDC. The Government has stated reforms to the Privacy Act will be consulted upon by the end of the year, which is the appropriate place to introduce economy-wide privacy protections. We see an opportunity for the CDR to lead the way in upholding the economy-wide protections resulting from this review, and we look forward to participating in Privacy Act reform consultation conversations in the very near future.

We thank the Treasury for the opportunity to provide feedback on the draft CDR Rules, and commend the CDR team on the inclusion of the BCDC and seven year consents, which reflect existing market operations while upholding sensible and

necessary protections. DSPs look forward to these initiatives being included in the Rules, which will enable the benefits of the CDR to flow to millions of Australia's small businesses.

Yours sincerely,

Danielle Smith
Xero GM Partnerships - APAC (A/g)

Andrew Baines
MYOB General Manager - Financial Services

Steve Kemp
Intuit Head of Financial Institution Partnerships - Australia and Emerging Markets

Introduction

Small businesses are the lifeblood of the economy employing more than 7.6 million Australians. Their future growth, success and prosperity lies in improving their productivity. In this context, there is a clear opportunity for the Government to design and prioritise policy frameworks that, in practice, help them to work smarter.

Xero, Intuit QuickBooks and MYOB are encouraged to see the Government's recognition , through this consultation, of the economic and societal value the CDR regime can create for small businesses, when designed in a way that encourages participation and reflects the realities of doing business..

The Australian Government announced the ambitious Consumer Data Right (CDR) in 2018 leading comparable economies to pursue a strategy to create an open data economy. With four years passing since CDR was announced, participation remains low. In contrast, the Open Banking regime in the United Kingdom has over 5 million regular users and 231 active TPPs[1]. Momentum continues to accelerate in the UK Open Banking regime with an additional 1 million new regular active users joining every 6 months.[2] The OBIE also found that business penetration (11%) is slightly higher than consumer use (10%) indicating that small businesses were early adopters of open banking technology with consumer offerings following behind.[3]

We are encouraged by the release of these exposure draft rules, which we consider to be a critical development and a significant step forward in addressing the existing low level of participation by business consumers in the CDR.

[1]https://www.openbanking.org.uk/regulated-providers/?query=directories&filter-search=&filter-provider-type=third-party-providers&filter-sort=0
[2]https://www.openbanking.org.uk/news/uk-open-banking-marks-fourth-year-milestone-with-over-4-million-users/
[3]https://www.openbanking.org.uk/news/obie-new-impact-report-shows-cloud-accounting-allowing-smes-to-run-businesses-more-efficiently/

Removing friction from the current framework through introducing the BCDC and seven year consents means DSPs will be able to map pathways to participation in the CDR, to the benefit of our small business customers. We expect DSP participation will deliver increased productivity across the economy, from the broad base of the small business sector.

Heightened awareness of data security

It is appropriate that security is front of mind following recent high-profile cyber-attacks, which have exposed millions of customers' personal information. It is our shared view that data security is our most important customer obligation, and one we take extremely seriously. Security is upheld by complying with privacy laws, Australian Taxation Office (ATO) regulations, applicable international laws (including the EU's General Data Protection Regulation) and continually working towards industry best practice, which in many cases exceeds existing regulatory requirements. These actions are appropriate for our organisations to ensure customer data is safe.

DSPs enjoy strong and trusted relationships with Australia's financial institutions (FIs), which underpin the permissioned two-way sharing of customer transaction data necessary for service delivery. Many small businesses request DSPs to incorporate FI transaction data to inform their financial accounts. This is currently primarily agreed through DSP/FI bilateral contracts and is facilitated via APIs or secure batch file provision. Australian banks have been providing this data for up to a decade, and this arrangement works well for the mutual DSP/FI customers that are supported by this data sharing. DSPs work continuously with government regulatory security teams to ensure customer data is appropriately protected. Securely accessing up to date financial data directly within software, which is longstanding, is one of our customers' most valued features, due to its significant utility and innovation potential.

Small business customers of DSPs have also been able to securely share financial information directly from software with advisers and business apps connected with DSPs via API. This capability is an important point of digitisation for Australia's small businesses, resulting in innovation and productivity. DSPs have worked closely with the ATO and the business-to-business (B2B) software-as-a-service (SaaS) industry to develop the Security Standard for Add-on Marketplaces (SSAM) to ensure this data sharing channel is appropriately protected. DSPs are confident in the security frameworks under which we comply, which we consider fit for purpose for protecting Australia's small businesses while enabling digitisation, innovation and productivity.

Data security standards

ASPs acutely understand the critical need for the growing data sharing economy to adhere to the highest security standards protecting the information of consumers and businesses.

As global cloud based software businesses DSPs adhere to the highest global data protection standard, the European Union's General Data Protection Regulation (GDPR). This means adhering to strict processes in relation to the handling, transparency and storage of data.

The core of our business models is dependent on the protections incorporated into this standard which exceeds Australian regulations. Privacy reform in Australia is overdue and we are collectively encouraged that the Government is prioritising reform in this area. The distinct difference between Open Banking in Australia and the United Kingdom stems from regulators in the United Kingdom having the confidence to develop an effective and innovative open data sharing regime underpinned by the GDPR.

One of the reasons for the slow uptake of CDR in Australia to date stems from the bespoke privacy regime that has been created within its framework as opposed to relying on existing laws and regulations to oversee privacy. This has created an inconsistency between this framework and other privacy obligations that cannot be operationalised while adhering to the innovative services our customers rely on.

As Digital Service Providers, we comply with the Australian Tax Office DSP Operational Framework for businesses which integrate with the ATO via API. We also comply with the Security Standard for Add-on Marketplaces (SSAM), an extension of the DSP Operational Framework, for businesses that integrate via API with a DSP which in turn integrates with the ATO via API.

The Business Consumer Disclosure Consent (BCDC)

We strongly support the inclusion of the BCDC in the CDR Rules, and note that as currently drafted the rules accommodate existing business operations, creating a regulatory regime that strives for best practice while accommodating participation through minimal operational disruption. In effect, the BCDC brings CDR capability in line with the UK's Open Banking Regime, which presents significant opportunities for Australia's small businesses while also reflecting best practice.

In addition, and as previously conveyed through Submissions to the CDR process, a core part of existing operations for many small businesses is the ability to share business data with business advisors, including bookkeepers. Interrupting this business flow would present a significant disruption to small business operations. As currently drafted, the BCDC reflects this crucial business process, and we recommend this expansion to the CDR regime be upheld.

Further, we note a non-individual consumer utilising the BCDC will remain protected, despite data leaving the CDR environment. The ATO DSP Operational Framework, associated SSAM, the Privacy Act and contractual obligations are complemented by existing global privacy protections to ensure business consumers can continue sharing data with confidence. We think this is an important landscape for the BCDC to operate within, and welcome the Government's efforts to create a streamlined, high-reaching approach to Privacy.

How a business authorises a disclosure under the BCDC

DSPs appreciate the flexibility the Rules create by requiring ADRs to take reasonable steps instead of mandating a stipulated process to facilitate a transfer of data under the BCDC. As per the nominated representative guidance for Data Holders[4]. DSPs welcome the ability to utilise existing ADR systems to manage appropriate persons sharing data on behalf of a business. For example, a DSP subscriber today proactively allocates permission to a user (likely a partner or employee) to enable data sharing to third parties. DSPs confidently assert this process is working as intended, complies with our regulatory obligations and is sufficient for managing BCDC disclosures under the CDR.

Keeping track of BCDC consents with dashboards

DSPs note the requirement for ADRs to update consumer dashboards with details about the BCDCs under which CDR data is disclosed. However, we would welcome clarity about the obligations of the ADH and the ADR, along with non-individual dashboard expectations.

[4]https://www.cdr.gov.au/sites/default/files/2022-07/CDR-FAQs-Nominated-representatives-non-individuals-and-partnerships-in-the-CDR-published-21-April-2022-updated-29-07-2022.pdf

DSPs support flexibility to provide business dashboards to non-individuals similar to that in nominated representative Rules. This would give DSPs the flexibility to present to business consumers with appropriate permission: BCDC consents, specified persons receiving data, data being shared and date of consent in a compelling way. This information is already available within a DSP subscription and we think appropriate to satisfy our obligations, as it is in the UK Open Banking regime.

The ADH should only be required to maintain dashboards for data directly leaving its system. For example, an ADH should not be expected to update their consumer dashboard with details of a BCDC. This would create unreasonable complexity for ADHs and would generate enormous network traffic, to ensure dashboards remain current. The ADR is the natural place for this business consumer dashboard to be maintained.

Paper forms in the age of CDR are contra to the intent

We note the manual nature of nominated representative processes for Data Holders. In particular, we note paper forms are common to nominate authorised representatives to consent to non-individuals sharing data from ADHs. While, in time, innovation will likely render paper forms redundant, manual paper forms are contrary to the CDR intent and drastically limit the scalability of the regime. **We recommend the Government assess whether paper forms have a home in CDR**.

Seven-year consents

We welcome the inclusion of the seven-year consent period, and appreciate the intent to better reflect the reality of business requirements.

In practical terms, the way this would work is that the CDR consumer would advise the ADR, for example MYOB, that they intend to share their CDR data with MYOB and that they are a business entity. MYOB manages the required confirmations of business status and business purpose statement. Then, MYOB refers the request to the relevant ADH by means of a message that this CDR consumer is a non-individual CDR data sharer. This enables the ADH to issue an appropriately dated, ie 7 year, token, rather than the normal 1 year CDR token. This information is sufficient to enable the ADH to create or update the customer's CDR dashboard.

However, we would welcome clarity on the business security benefit of introducing time limited consents in the CDR at all. The inability to offer ongoing consents is a notable hurdle blocking DSPs becoming ADRs in the CDR. **We recommend the Government consider alternatives to the time-based consent requirement that minimise data retention while maximising consumer control and protections, including having consents expire when a consumer ends a subscription or contract with a provider**. We look forward to continuing conversations with the Government to ensure the Rules support and encourage secure participation.

The option for business consumers to consent for up to seven years is an improvement on the current Rules but not a solution. There are a number of ways a business could still experience the consequences of a use consent lapsing, both inadvertent and deliberate. Should DSPs become ADRs in the regime, the negative customer experience of a lapsed use consent may outweigh the benefits of participating in the CDR at all.

Data deletion upon expiration of a use consent

One issue in the application of time-limited consents for DSPs is the requirement to delete all CDR data in the event of a 'use' consent lapsing. This requirement would result in the deletion of all data within an DSP subscription. A data deletion

requirement would present significant disruptions for small businesses, and risks undermining their existing compliance and audit requirements.

Businesses rely on cloud accounting for record keeping. Increasing rates of digitisation means few businesses will have hard copy records of the multitude of business records required by law, (for example evidence of all sales and purchases, all documents about GST, tax invoices, wage and salary records, and all records relating to tax returns, activity statements, FBT returns and super contributions) to be submitted and retained for a specified time period. The deletion of these records would render affected businesses noncompliant, and severely challenged in the event of an audit or dispute. **We recommend the Government consider existing auditing and compliance obligations, and enable access to business record keeping information for the period of time required by law as a minimum.**

Recommendations for use consent timeframes:

We recommend the Rules provide the option for an ongoing use consent for business consumers. This inclusion would allow business consumers to run their business with the certainty that data interactions and business reports are secure within software. Business consumers would be able to withdraw consent from dashboards at any time and instruct ASPs to delete data, as per the current capability.

An alternate approach could be to introduce a safe harbour for data deletion, however this presents complexity through build, design and compliance monitoring. The complexity makes this option non-preferred, but would see DSPs given the ability to "freeze" accounts for an amount of time without deleting data to allow a nominated representative to redo a consent to allow a DSP to continue using the data.

Privacy Act reform

We note the introduction of the BCDC aligns with the UK Open Banking downstream protection and restriction limitations. For example, a DSP in the UK is not required to meet any Open Banking obligations when releasing permissioned data to third parties. In part, this is due to both the DSP and the third party being required to comply with GDPR.

We suggest the CDR be cognisant of the Government's commitment to circulating Privacy Act reforms by the end of the year. As DSPs have long argued for, economy-wide privacy protections under the Privacy Act will be a better way to manage security than specific inclusions in the CDR. While businesses are protected by a number of security frameworks, if confidence is drawn from a fit for purpose Privacy Act the CDR may benefit from enhanced participation.

Conclusion

We thank the Government for its ongoing commitment to advancing the CDR in a way that reflects and facilitates modern business operations. We see significant opportunity for CDR to lead the way for upholding Privacy, and see the BCDC as a way to maximise participation in a secure regime.

We look forward to continuing to support the Treasury and the Government in its expansion of CDR, and to help ensure the regime is rolled out in a way that creates the best future operating environment and opportunities for the 2.4 million Australian small businesses and the 7.6 million people they employ.