Beautiful business

20 July 2020

By Email: ACCC-CDR@accc.gov.au

Dear CDR Rules team

Re: CDR Rules consultation

Xero welcomes the opportunity to participate in the Consumer Data Right (CDR) Rules consultation that allows for accredited collecting third parties (intermediaries).

We support the highly constructive approach the Australian Competition and Consumer Commission (ACCC) continues to embrace when working through the development of the CDR Rules framework.

Introduction

Xero's submission is from the perspective of a likely accredited data recipient (ADR). Xero will make a final decision on becoming accredited once it is satisfied that the scheme is not so complex as to discourage participation, not just by ourselves but by our partners. An overly complex scheme and a lack of wide participation would lead to increased business cost that exceeds the associated benefits.

At present, we still have questions as to whether this cost benefit analysis will come down in favour of participation in the CDR scheme. This is because we are seeing a high degree of complexity and uncertainty, including in becoming accredited, the scope of CDR data and in how the CDR scheme interacts with and relates to other areas of law and regulation. We are concerned that if this is not resolved, the barriers to entry into the CDR scheme will be too high and in effect discourage participation.

This would mean that Australia misses the opportunities set out by the Productivity Commission in its report into Data Availability and Use. Namely that "improved data access and use can enable new products and services that transform everyday life, drive efficiency and safety, create productivity gains and allow better decision making." In its Response to the Productivity Commission's report, the Government stated that there are significant opportunities to "encourage new business models to unlock the value of consumer data."

We are concerned that these potential benefits will be missed if the complexities and uncertainties currently in play are not resolved. This would result in missed opportunities to improve outcomes for consumers and small businesses at a critical time in Australia's economic response to COVID-19.

Summary of concerns

Areas where we currently see an unnecessary amount of complexity include the ADR accreditation process. FinTech Australia has estimated that the cost of becoming accredited will be in the order of $100,000. Further, the ADR accreditation framework does not leverage or acknowledge relevant existing certification regimes. Finally, Schedule 2 of the CDR Rules introduces a separate framework for assessment of security practices and does not acknowledge internationally recognised security certifications.

Xero Australia Pty Ltd
ABN 89 124 215 247

Registered Office
1/6 Elizabeth Street
Hawthorn
VIC 3122

www.xero.com
0800 GET XERO
T +64 4 819 4800
F +64 4 819 4801
E info@xero.com

We are also concerned that the CDR scheme as currently framed, does not sufficiently make clear the scope of the Authorised Deposit-taking Institution (ADI) Designation Instrument. (Designation Instrument). This is discussed further below.

Lastly, it is not sufficiently clear that the deletion and de-identification requirements are subject to an organisation's record keeping obligations under Australian law.

Xero submits the following recommendations:

> ***Recommendation One*:** ADR accreditation should be streamlined by recognising existing accreditation and certification frameworks. This should include recognition of the Australian Taxation Office (ATO) Digital Service Provider (DSP) Operational Framework accreditation, ISO 27001 and SOC 2.
>
> ***Recommendation Two*:** In regards to the Minimum Information Security Controls, Schedule 2 should be a requirement only for entities that cannot produce appropriate accreditation or certification under existing frameworks.
>
> ***Recommendation Three:*** The CDR Rules should explicitly acknowledge that the information designated under the Designation Instrument does not include Materially Enhanced Information (see the definition in the Designation Instrument). Accounting data should be considered Materially Enhanced Information and be excluded. Whether or not accounting data is a priority CDR dataset should be considered as a policy decision by Government. If Government determines as a matter of policy that accounting data should be part of the CDR scheme, then a specific designation instrument should be made for that dataset following appropriate industry consultation.
>
> ***Recommendation Four:*** Requests to delete or de-identify redundant data should be considered subject to established record keeping laws.

We look forward to working with the ACCC to encourage participation in a robust, effective CDR scheme.

Unnecessary cost and complexity

Accreditation, whether as a Principal or Provider

Xero remains concerned about the creation of unreasonably high barriers to entry through the accreditation process. Accreditation to participate as an ADR in the CDR scheme will be resource intensive. We note that FinTech Australia estimates the cost of accreditation at $100,000.

Xero has advocated in previous submissions for recognition of existing accreditation frameworks. This will contribute to increased ADR participation and the overall success of the CDR scheme.

In Xero's industry, key existing frameworks include the Australian Taxation Office ATO DSP Operational Framework, the related Security Standard for Add-on Marketplaces (SSAM) and Tax and BAS agent requirements. Detail on these frameworks was provided in our submission to the consultation on how best to facilitate participation of third party service providers earlier this year and is attached as an Annexure.

It would be appropriate to recognise and provide streamlined accreditation pathways to reflect:

- The ATO's DSP accreditation as equivalent to unrestricted CDR ADR status.
- The SSAM accreditation as equivalent to third party accreditation under the CDR.
- Tax and BAS agent accreditation as equivalent to third party accreditation under the CDR.

Providing streamlined accreditation pathways in this way would ensure a high level of CDR scheme participation and minimise disruption of existing secure data transfer processes.

If organisations are faced with inconsistent accreditation processes, the cost of participating in numerous schemes will become prohibitive. Multiple inconsistent schemes would exponentially increase barriers to entry of cost, complexity and capital requirements that will in turn reduce competition between service providers, and potentially the overall benefits of the CDR scheme.

Recommendation One: ADR accreditation should be streamlined by recognising existing accreditation and certification frameworks. This should include recognition of the Australian Taxation Office (ATO) Digital Service Provider (DSP) Operational Framework accreditation, ISO 27001 and SOC 2.

Minimum information security controls

Recognising existing robust security certifications will reduce cost and complexity, appropriately lowering barriers to entry and increasing ADR participation. Many organisations hold existing internationally recognised security certifications, namely ISO 27001[1] and SOC 2[2]. These certifications should be recognised as an appropriate way to meet the security requirements of the CDR Rules and Schedule 2 should only apply where such certification cannot be demonstrated.

Many smaller organisations will not have ISO 27001 and/or SOC 2 certification. Therefore it is appropriate that Schedule 2 offer a framework for assessment of those organisations. However it should not become a duplicative framework.

The ATO DSP Operational Framework recognises ISO 27001 certification which gives organisations the opportunity to leverage well accepted international standards.

Appropriately aligning Schedule 2 with international standards and recognising those international standards, will streamline participation for both holders and non-holders of accreditation. In addition, alignment will prepare smaller entities to gain international accreditations in the future, streamlining growth into global markets.

[1] The International Organisation for Standardisation (ISO) is an independent, non-governmental international organisation with a membership of 164 national standards bodies. ISO/IEC 27001 is widely known, providing requirements for an information security management system. Using ISO/IEC 27001 enables organisations of any kind to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties.

[2] Intended to meet the needs of a broad range of users that need detailed information and assurance about the controls at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems.

Beautiful business

Turning to the specifics of Schedule 2, Xero welcomes the new reference to the encryption of data in transit. We note that Schedule 2 does not contain particulars about encryption of data in transit, allowing for interpretation in different ways by different participants. This should extend to recognising the data encryption practices certified as part of ISO 27001 and SOC 2 compliance.

Recommendation Two: In regards to the Minimum Information Security Controls, Schedule 2 should be a requirement only for entities that cannot produce appropriate accreditation or certification under existing frameworks.

The scope of the ADI Designation Instrument

The Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019 sets out the range of information subject to the CDR scheme for the banking sector (Designated Information). A key element of this Designation is the exclusion of Materially Enhanced Information from scope.

Materially Enhanced Information is:

> "(a) … information (that) was wholly or partly derived through the application of insight or analysis to information to which subsection 7(1) applies (***source material***); and
> (b) that insight or analysis:
> (i) was applied by, or on behalf of, the entity that holds the information or on whose behalf the information is held; and
> (ii) rendered the information significantly more valuable than the source material.

Xero is concerned that the current drafting of the CDR Rules does not explicitly acknowledge that the range of data subject to the scheme is limited by the exclusion of Materially Enhanced Information.

Xero considers accounting data to be materially enhanced information. Accounting data is hyper-accurate compliance data created by applying analysis to bank transaction data. Accounting data forms the backbone of compliance activities across the economy, including:

- STP, BAS and annual tax return data to the ATO.
- Payroll tax data to state revenue agencies.
- Child support data to the Department of Human Services.
- Payroll compliance data to the Fair Work Commission.
- Remittance of data to comply with the Corporations Act.

If in the future, the Government decides that accounting data should be Designated Information under the CDR scheme, then it is appropriate that a new designation instrument be put in place and that implementation is reflective of the unique characteristics and needs of accounting data. This would need to be informed by appropriate accounting industry consultation, including relevant industry bodies, for example CPA Australia and the Institute of Certified Bookkeepers.

The lack of clarity and certainty on this point may undermine confidence in participating in the CDR scheme. It is important to be cognisant of the fact that many organisations approach their compliance obligations conservatively. Accountants, bookkeepers and government departments receiving accounting data would likely be concerned with the requirement to become an ADR to continue receiving or working on such data.

Being required to become an ADR would significantly change the cost and process to support businesses with their accounting needs, including compliance.

It is particularly problematic given the ADI Designation Instrument *does not extend* to Materially Enhanced Information - ie in Xero's view, accounting data. Hence this should be explicitly clarified in the CDR Rules. Without this clarification, there is a significant risk that additional barriers to compliance will be inadvertently created, undoing recent red tape gains such as auto-populating compliance reports.

> *Recommendation Three:* The CDR Rules should explicitly acknowledge that the information designated under the Designation Instrument does not include Materially Enhanced Information (see the definition in the Designation Instrument). Accounting data should be considered Materially Enhanced Information and be excluded. Whether or not accounting data is a priority CDR dataset should be considered as a policy decision by Government. If Government determines as a matter of policy that accounting data should be part of the CDR scheme, then a specific designation instrument should be made for that dataset following appropriate industry consultation.

Established record keeping obligations

Xero supports the consumer's ability to elect how redundant data is treated and the notion that decisions about the treatment of redundant data will be made solely by the Principal, with the Provider to treat the data in accordance with the Principal's policy. However, the CDR Rules should be clarified regarding the appropriate treatment of data when there are legislated requirements to keep records.

Business records are required to be kept for at least five years, often seven years. Record keeping obligations are a requirement of section 262A of the Income Tax Assessment Act; the Australian Securities and Investment Commission under section 286 of the Corporations Act; and the Fair Work Ombudsman under sections 535 and 536 of the Fair Work Act. Records are required to help a person explain all transactions and acts that are relevant to the various Acts. Therefore all financial data a small business directs to its Xero account is required to be kept for at least five years.

Records are to be kept from when the business owner prepares or obtains the record, or completes the transaction or acts the record relates to. This requirement extends beyond accounting data, and includes all financial information to explain transactions by a person engaged in business relevant to the Acts.

A Xero subscriber's business record is obtained as the transaction enters the Xero software. The record is most often in the form of an unreconciled transaction, recorded as a line of a bank feed. In the event personal and business data are mixed in a bank feed, for example a sole trader using a personal credit card to purchase business supplies, financial data still cannot be deleted or de-identified without breaching the Acts. Deletion or de-identification is not possible because all transactions are required to be held to verify the nature of the transactions by a person engaged in business in the event of an audit. On the other hand, should Xero on behalf of the customer delete or de-identify data, Xero is facilitating a direct breach of potentially numerous Acts and exposing the customer to administrative penalties.

The CDR Privacy Safeguard Guidelines from the OAIC include the following:

> 12.4 These requirements apply except where:

- the accredited data recipient or designated gateway is required by law or a court/tribunal order to keep the CDR data, or
- the CDR data relates to current or anticipated legal or dispute resolution proceedings to which the accredited data recipient, designated gateway or consumer is a party.

Xero submits that the CDR Rules should reflect the exclusion of deletion and de-identification obligations where there are legal obligations to keep the information.

Recommendation Four: Requests to delete or de-identify redundant data should be considered subject to established record keeping laws.

Third parties update

The treatment of third parties will determine Xero's participation in the CDR scheme. Small businesses rely on connection to third parties. Critical third parties include accountants, bookkeepers, advisers and third party apps. Engagement includes small businesses providing third party access to accounting data. The rules update in August must support this existing data transfer mechanism. While big businesses are better equipped to manage accreditation complexity, in many cases, small businesses are not. If the CDR Rules sever the existing link between small businesses and third parties, Xero will be forced to review its participation.

Xero's proposed solution is to recognise existing accreditations. As outlined above and in our previous submissions, the ATO Digital Services Provider (DSP) Operational Framework is a suitable, risk proportionate accreditation model for ADRs. The DSP Operational Framework accreditation has the flexibility to manage accreditations of third parties which integrate with DSPs, through the Security Standard for Add-on Marketplaces (SSAM). Accountants, bookkeepers and advisers are each accredited to manage sensitive customer data appropriately. In Xero's view, respecting a working accreditation system will help scale the CDR from launch, incentivising participation.

Xero welcomes the opportunity to engage with the ACCC in the lead up to and during the upcoming third party consultation process.

Kind regards

[redacted]

Ian Boyd, Director of Partnerships
Xero

Beautiful business

ANNEXURE

ATO DSP/SSAM Operational Framework

In the 2016-17 financial year, the ATO collaborated with industry to develop the DSP Operational Framework. This framework sets out the minimum technical and security requirements software developers and their products are expected to meet if they wish to consume ATO services via API or from within software.

The DSP Operational Framework requirements include internationally recognised compliance standards including the International Organization for Standardization (ISO) and SOC 2, developed by the American Institute of Certified Public Accountants (CPA). These accreditations are recognised, interoperable and considered global best practice.

All DSPs wanting to consume the ATO's digital services need to meet the requirements which can include, but is not limited to:

- Authentication
- Encryption
- Supply chain visibility
- Certification
- Data hosting
- Personnel security
- Encryption key management
- Security monitoring practices.

Further information on the full suite of DSP requirements is available at: https://softwaredevelopers.ato.gov.au/RequirementsforDSPs

As of October 2019, more than 250 software developers and software products have been reviewed, accredited and certified by the ATO under the DSP Operational Framework.

In 2019, the ATO further engaged with industry to codesign the world-first Security Standard for Add-on Marketplaces (SSAM). The SSAM is likely to be adopted by other Commonwealth jurisdictions within the next 24 months.

The SSAM framework sets out the minimum recommended security and certification requirements for cloud software products (apps) that integrate via API with entities governed by the DSP Operational Framework.

Requirements for third party apps participating in add-on marketplaces to gain SSAM accreditation include:

- Ensure effective key management Ensure effective key management is implemented to protect client data.
- Ensure that sensitive client data in your app is protected during the transport process.
- Ensure that users who access to your app are authenticated.

- Ensure that unauthorised third-parties are unable to access customer data.
- Ensure that your app server is secure.
- Ensure that your app is secure against the common vulnerabilities.
- Ensure that sensitive client data in your app is protected while at rest.
- Ensure appropriate audit logging functionality is implemented and maintained.
- Ensure client data is not hosted in high risk areas
- Ensure you have security monitoring practices in place to detect and manage threats.

Full information for SSAM security requirements third parties can be viewed on the Australian Business Software Industry Association website: https://www.absia.asn.au/industry-standards/addon-security-standard/ABSIA-Security-Standard-for-Add-on-Marketplaces.pdf

The SSAM and the DSP Operational Framework enact a tiered, standardised accreditation process based on risk and is a pragmatic solution to manage customer security in an environment of increasingly connected parties.