BIZA·IO

Submission to the consultation for

Consumer Data Right rules - expansion to the telecommunications sector and other operational enhancements

14 October 2022

Executive Summary

Introduction

Biza.io welcomes the opportunity to provide feedback on the proposed exposure draft amendments to the Consumer Data Right (CDR) Rules.

Biza.io is an established Australian fintech and the market leading provider of cross-sector CDR Data Holder solutions. Founded by the former Engineering Lead of the Data Standards Body (DSB), Biza.io has been involved in the Data Standards creation process since the very beginning and its personnel remain the largest non-government contributors to the consultations.

In addition to participation within the CDR, Biza.io is also a contributing member of the Financial-grade API (FAPI) Working Group, a contributor to the FAPI 1.0 information security profile, and a co-author of the Grant Management for OAuth 2.0 specification.

Beyond just a contractual engagement Biza.io considers all its customers as partners in the journey towards the shared vision of open data. At the date of this submission, Biza.io is currently responsible for delivery of CDR data for approximately 20 Banking and Energy Data Holders.

Format of this response

The responses in this document reference numbered items contained within Attachment A of the published Exposure Draft Explanatory Materials as provided on the Australian Government's Treasury website.

Responses have been provided for selected numbered items.

A range of additional, broader comments have also been provided for consideration

Extending CDR to telecommunications

Item 3 – 30K services de minimis threshold

The idea of a hard limit has merit however we should consider the *types* of products offered by the carrier. If these are predominantly old technologies such as ISDN or Frame Relay, imposing an obligation to invest in publication of end-of-life products represents low value.

We note the use of *de minimis* as a term in the rules. While appealing in an academic sense, it is at odds with the Government's stated desire to encourage the use of plain language in legislation - https://www.opc.gov.au/drafting-resources/plain-language

There are already many thresholds in CDR and if implemented, we suggest referring to this as the Active Services Threshold instead.

Biza.io recognises the need for parliamentary oversight of threshold definition, yet inclusion of hard values within rules may drive more frequent updates. Where possible, consider abstracting actual values, instead referring to a threshold that can be maintained independently and more readily as CDR evolves and operational evidence requires.

Item 5 – Meaning of Relevant Product - Fixed Internet v Mobile Services

We have already commented publicly on GitHub regarding a potential issue here. To briefly summarise, it is recognised that the rules proposal of fixed Internet services is deliberately ambiguous. While this is no doubt well intentioned, it will inevitably result in varied interpretation by data holders, impacting data quality and consistency for ADRs.

https://github.com/ConsumerDataStandardsAustralia/standards/issues/265#issuecomment-1269810740

Item 10 – Eligibility – Account Size

This is another threshold definition issue requiring further discussion and once again it would be desirable to abstract this hard measure from the rules as it will inevitably date.

We challenge the proposed figure of $40K as an annual Enterprise customer price point, suggesting $500K may be a more realistic figure. Biza.io recognises an attempt to align with the existing Telecommunications (Consumer Complaints Handling) Industry Standard 2018 which also uses a figure of $40K, but this defines the threshold for *consumer protection* which we consider very different to a data sharing ineligibility point.

Some of the greatest potential value in CDR could be associated with a comparison service for small businesses. This threshold must be appropriately set if we are to enable this.

Item 11 – Secondary Users

The rules propose that (unlike Energy) the concept of Secondary Users does not apply to this sector. Biza.io recognises authentication of anyone other than the account holder may be challenging but, contrary to the guidance notes, we believe Energy and Telecommunications both share this challenge, and it is only the banking sector that has a direct relationship with an individual consumer.

Biza.io suggests there is potential value in a secondary user being able to share business account data with a trusted advisor via an ADR, for instance, a managed solutions provider performing an assessment of a small business with a mix of technology services.

Item 14 – Product Data and Bundles

We note and support the desire to identify any type of data consumed as part of the service delivery, viewing this as critical to support any volume-based analysis, however it is not clear how usage data relating to bundled services will be identifiable and made available as such. Schedule 5, clause 1.3 indicates it may be hidden within a category of *product specific data.*

Items 20- 21 - Closed Accounts

Schedule 5, 3.2(5)(a) indicates closed accounts are **in** scope when another *account* is open with the same data holder. Presumably the intent is to retain access to historical data with a provider where there is still a method with which to authenticate the consumer. In banking, the account is typically the lowest element in the product hierarchy. This is not the same in telecommunications. Should the term therefore be *services*, or *products*? Both are lightly defined in Schedule 5, 1.2 but *account* is not. What is the guidance in respect of closed or cancelled services or products and how they relate to accounts? What is the expected behaviour in respect of customers who churn to new accounts/services/products with the same holder?

Items 27- 28 – Phased Delivery Obligations

This approach is understandable and mirrors that taken in Banking, however it does create an initial coverage challenge for ADRs. In banking this was material for certain use cases and was cited as the primary reason for retaining screen scraping. We should be mindful that a similar 2-phase implementation will result in the primary holders heavily influencing evolution of the standards. Data holders that follow may find themselves adapting to what they may view as over-engineered requirements with increased cost of compliance. The current NFR debate is an example of this in the banking sector.

Telstra, Optus and TPG are referenced as initial CSPs. There is no indication of whether non-primary brands (eg. Vodafone) and/or white-label offerings (eg. Aldi) are to be included. 5.4 imposes the obligation to respond to product data requests for initial and large CSPs yet it doesn't include the clarification present in 5.6(3) to cover the scenario where a small CSP later passes the materiality threshold and becomes a large CSP. This should be added.

Item 29 – Large CSP Definition (also refer to Item 3 comments above)

There will inevitably be a level of debate surrounding the definition of the Large CSP threshold. At present the rules suggest 30K services. Biza.io notes the use of the term *services* rather than products or accounts and refers to comments for items 14 and 20.

Item 35 – Direct-to-Consumer data sharing

Biza.io recognises that this is a pre-existing capability originally intended to be launched in the banking sector in 2020. Two years on, we are unaware of strong support for this service. Part 3 of the rules covers the direct request service and Schedule 4, 8.5 and Schedule 5, 5.5 state it does not apply to the Energy or Telecommunications sectors respectively. Rather than continuing to carry this unimplemented legislation within the rules, perhaps now is the time to retire it. It can always be reinstated at a future date if required.

Operational Enhancements to CDR Rules

Item 42-44 – Business Consumer Disclosure Consent and Statement

Introducing a business disclosure *statement* to further certify the sharing of business data will add to pre-existing consent complexity – an area already flagged for reconsideration. It is not clear why such a statement (on top of the BCDC) is necessary and indeed whether it will apply in all business data sharing contexts. For example, a sole trader operating bank accounts as an individual would possess an ABN and can be classed as either, at the Holders discretion, an Individual Consumer or Non-Individual Consumer. At a recipient level would they be sharing data as an individual, or as a business?

Item 45 – ABN Verification

Requiring an accredited person to undertake a search of the Australian Business Register to confirm the consumer has an active ABN is an onerous obligation that does not effectively scale. The current WSDL API offered is not fit for this purpose nor aligned with the technical Standards that govern the CDR. Biza.io suggests the rules should mandate that the Business Register provide a contemporary API-based verification service specifically for CDR and similar to the secondary data holder obligations applied on AEMO and AER.

Item 48 – 7 Year business consents

The selection of the permitted maximum period for authorised use of data may require adjustment if the 7-year period has legal significance. The scenario where a business consumer consents to 12 months collection and 7 years use of data will result in the last piece of collected data only being permitted to be retained for 6 years. If 7 years is significant as a term, then the rules may need to be adjusted to permit use (and other consent types) for a period of 7 years from the *point of collection* rather than the *point of consent to collect.*

That aside, extending the authorised duration of *use* from the current 12 month maximum appears to be a useful enhancement. 1.10A(7) states the types of consents that can be approved via a business consumer statement and rule 4.12 permits an extended duration of up to 7 years to apply to consents incorporating this statement. This change would enable a bookkeeper to unambiguously retain and use CDR data for up to 7 years via a *use consent.* This makes sense, yet enabling an ADR to retain aging data to support subsequent *disclosure* a number of years after that data was originally collected seems less useful.

Item 50 – Record Keeping Obligations

Under this new proposed arrangement, a bookkeeper could potentially be provided with ongoing access to their client data via an amended collection consent obtained through an ADR. Consequently they now have multiple and potentially variable data retention (for use) timeframe obligations to manage. This could be impractical for smaller bookkeepers with many clients and limited systems with which to manage this.

57 – Principals

Biza.io notes multiple uses of the term ‘principal’ in the legislation. The ADR-Rep arrangement makes the ADR a principal; the Rep-OSP makes the Rep a principal; The OSP-

OSP relationship makes the OSP a principal. It is suggested that the rule text qualifies the term in each case to avoid confusion - ie Chain Principal, OSP Principal, ADR Principal etc

Item 64 – CDR Policy

The requirement to list all direct and indirect OSPs of the ADR and any representative seems onerous and will likely create a policy change management burden, particularly for intermediaries who have many representatives, each potentially with many OSPs. It should be permitted to refer to a dynamic register of this information, rather than require it to be embedded in the policy itself. There are also potential ramifications of a highly dynamic policy if an ADR is required to notify clients (and potentially consumers) of any change.

Item 68 – ADR Dashboards

It would be helpful to clarify if this requirement just applies to ADRs and that Data Holders are not required to augment existing dashboard functionality with this information. If Data Holders are required to provide this information, how are they to be advised of it and has consideration been given to implementation impact?

Items 86-89 – Trial Products

Biza.io supports the concept of trial products but questions why this is the exclusive domain of data holders. Arguably there is more consumer value to be gained from permitting an ADR to trial a streamlined software product activation process for a low-volume PoC in order to assess market viability. Software product activation is a material undertaking involving CTS and a more streamlined approach could encourage innovation within CDR.

By contrast, data holders already have PRD and consumer data publication systems in place and administering these to add a new product or service would not seem to be a material undertaking. Clarification is required in terms of whether this proposal applies to PRD as well as consumer data.

If this rule is implemented, Biza.io suggests the proposed 1,000 limit should be abstracted as a volume materiality threshold that can be adjusted outside of the rules. We are also interested to understand how the proposed limits are to be policed and enforced.

To provide at least some level of ACCC and OAIC oversight, it is suggested that the number and status of trial products be included in 6-monthly data holder reporting obligations.

Items 94-95 – Data Holder Dashboard Amendments

The proposed changes to data holder dashboards to reflect amendment to authorisations have been done to align with existing ADR obligations. This will create workload for existing data holders within the banking sector. To ensure the associated work can be appropriately managed, it is imperative that the rules confirm a data standard will be made clarifying how the amendment disclosure will operate. We also suggest retrospective disclosure of amendments be considered out of scope for any such change.

Item 96 – Treasury Feedback – Privacy Safeguard 13

Biza.io suspects there will be low appetite from data holders at this time to implement a capability that allows consumers to request data correction via their dashboard. This could represent a significant build and while optional we would like to understand validation Treasury has done to indicate this is a regularly requested activity.

It is suggested that rather than further complicating the existing dashboard architecture, Treasury consider creating a rule that states a data standard will be made to provide a technical mechanism through which holders could notify recipients of a data correction. Recipients could then re-collect this data in line with provision of their consumer service.

Item 102 – Reporting

We already note that under 9.2(3)(ee) the number of business consumer disclosure consents should be reported. It may also be helpful to report on the volume of newly proposed disclosure consents over 12 months duration. Potentially the move to a maximum of 7 years may result in interim periods being adopted by ADRs. This can only be revealed by those parties. Sharing the term of any such authorisations may be beneficial for data holders and go some way to help them better understand and manage the boundaries and parameters of their customer data risk which will inevitably increase as a consequence.

103 – Non-ADI Reciprocity obligations

The wording in Items 5 of clause 6.2 in Schedule 3 states “at least 12 months”. This might be better reworded to impose the obligation commencing from “12 months onwards”. Consideration might be given to rewording so data holders have the option to publish prior to this date if they wish.

104 – Thresholds for non-ADI Data Holders

Have we considered introducing a threshold for participation for non-ADI data holders? This could be similar to the proposed 30K telecommunications ‘large CSP’ threshold. Absolving smaller non-ADI data holders who are ADRs from reciprocal obligations may serve to stimulate competition and innovation in the regime. Once they reach the materiality threshold obligations should commence. This could be a cross-sector change as under the proposed rules, reciprocal obligations commence for small CSPs in the telecommunications sector once they become accredited persons (albeit with a 12 month grace period).

Additional Feedback

Item A – Rules Complexity and Rules Rationalisation

The existing CDR rules are already complex and with these new changes they become even more so. Is there a point at which we should consider pausing and reviewing whether the highly prescriptive nature of the existing rules is still appropriate? It seems the rules are encroaching into unnecessary territory - telling businesses *how to meet* their obligations rather than what they are via clear high-level principle-based statements.

An example of the prescriptive 'rules built on top of rules' issue is apparent in detailed clauses stating what an ADR's representative and their direct and indirect OSPs must do. Section 7.6 already clearly states what an ADR must do and that it is responsible for the conduct of all downstream parties. All liability ultimately sits with the ADR and the ADR will take appropriate measures to protect itself. It is already very clear yet there are large sections of the rules that state the expected conduct of representatives and OSPs.

Item B – Asynchronous Rulemaking

CDR is a highly dynamic piece of legislation. Government agencies have undergone rapid growth and adaptation of late and there is now an inevitable corporate memory issue. Those who have inherited the rulemaking and enforcement function are largely different to those involved in the creation of them and may be unfamiliar with many of the practical implementation issues of the v0-4 rules. Similarly high churn within the CDR private sector is compounding this issue with topics re-emerging and old debates resurfacing.

Unfortunately, the nature of the rulemaking at present does not provide public visibility of these historical debates, dialogue or thinking behind the decisions. The process for setting data standards is not perfect but it certainly exposes the thinking publicly on GitHub, something widely recognised as a great resource, particularly several years on.

In April 2021 a design paper on joint accounts was published under a GitHub issue: https://github.com/ConsumerDataStandardsAustralia/standards/issues/176

This resulted in rule changes which, at the time, were quite contentious. The matter of joint account capability has recently surfaced again in the Statutory Review[1] so it is helpful that we are today still able to access the thinking behind those earlier changes and resurface and reconsider if original arguments hold true.

Biza.io believes it would be beneficial to the broader ecosystem if the design paper concept could be re-established. We suspect the quality of submissions to the current consultation would be elevated and refined with the benefit of pre-debate.

Item C – Prototype Staged Rulemaking

Following on from Item B above, even once rules are largely settled, they could exist in beta or pilot mode to be proven or to evolve and be refined to the point where they are ready for broader industry adoption at scale.

[1] https://treasury.gov.au/sites/default/files/2022-09/p2022-314513-report.pdf - (Page 75)

Consultation, rulemaking, and data standards setting currently operate on independent timelines. We see value in thinking through what a properly coordinated implementation schedule might look like, and how legislation change and associated implementation might work. To support this direction, Biza.io suggests consideration be given to an experimentation sandbox to result in more successful merging of technical standards with the rules framework.

Item D – Insights

We note 1.10A(3) references *CDR insights* that are largely associated with the banking sector. Are there plans to extend insights to Energy and Telecommunications or to reword existing rules so they are applicable to other sectors, or are entirely sector agnostic? If not, perhaps the insight rules belong in Schedule 3 (banking).

Biza.io believes insights could and should be truly cross-sectoral. We would like to see an automated process established whereby ADRs can make an application to the ACCC or Treasury for approval of an insight use. This might require broad principles or parameters to be established in the rules but would again abstract a more dynamic and variable element from the rules, easing maintenance and enhancing flexibility for the regulator.

Item E – Business Disclosure Consent

Rather than create a new consent duration for specific consent types associated with business data, should we instead consider extending the duration of all business consent types? It seems that extension of a business data collection consent for banking purposes beyond the 12-month current term is really what is required.

Whatever the duration, with the current model there is always still an end date. While the move to 7 years for use of data seems 7 years sounds good it introduces other challenges. Only the ADR has visibility of the arrangement with the business consumer. The data holder has no visibility of where their customer data resides. Recent data breach events illustrate the risks associated with large scale and wholesale distribution of copies of data.

Furthermore, the ACCC is also unable to determine if the data is permitted to be retained. Auditors and other regulators such as APRA would be unable to readily view the chain of authority to see if parties are entitled to retain data. It is not clear how we anticipate this obligation could be policed or enforced?

Potentially the ADR dashboard needs to reflect more details of business consumer disclosure consents and that information may need to be pushed to the data holder to promote visibility and enable the data holder to have some level of awareness for risk management purposes.