



Biza Pty Ltd t/a Biza.io
ABN: 54 624 797 655
Level 6, 25 King Street
Bowen Hills QLD 4006
Tel: +61 1300 MY BANK
www.biza.io

6 October 2023

Aidan Storer
Assistant Secretary
Consumer Data Right Division
The Treasury
Langton Crescent
PARKS ACT 2600
by email: CDRRules@treasury.gov.au

Dear Mr. Storer,

Consumer Data Right rules – Consent Review

Thank you for the opportunity to comment on the Consumer Data Right rules – Consent Review.

Biza.io (Biza) are the market leaders in Data Holder solutions to the Consumer Data Right and are the only pure-play CDR vendor in Australia providing these solutions. Biza.io has been involved in the Data Standards setting process since the very beginning and its personnel remain the largest non-government contributors to consultations. By November 2023, Biza will be responsible for providing the Data Holder infrastructure for more than 50% of the mandated Energy Retailers as recently published by the ACCC¹ accounting for more than 75% of the entire Australian Consumer market within the Energy sector. In addition, Biza delivers the Data Holder obligations for approximately 20% of the Data Holders within the Banking sector.

Fundamentally, we believe Biza is one of the strongest proponents of the CDR and its success. Our business has been built from the ground up on achieving the vision of the CDR and our success is implicitly tied to the success of the ecosystem.

The responses provided are the outputs of the Biza Industry Advisory Committee, an internal group of Biza personnel.

Question 1: Do you support the bundling of CDR consents that are reasonably required for the provision of the service requested by the consumer? Do you consider the proposal strikes the right balance to reduce cognitive load while maintaining informed consumer consent?

At a high level, we are supportive of the concept of bundling CDR consents to optimise the experience for Consumers. We note that Australia has taken a very different path to essentially all other jurisdictions with its approach to individual consent types rather than the grouping into a single consent type.

Whilst we support bundling of CDR consents, it is our opinion the design paper does not sufficiently consider the flow-on impacts of doing so.

¹ <https://cdr-support.zendesk.com/hc/en-us/articles/7975868764431-Energy-Data-Holders-with-Consumer-Data-Sharing-Obligations-Commencing-1-November>



Biza Pty Ltd t/a Biza.io
ABN: 54 624 797 655
Level 6, 25 King Street
Bowen Hills QLD 4006
Tel: +61 1300 MY BANK
www.biza.io

Firstly, options and impacts regarding hybrid bundling whereby some consent types are bundled, whilst others are not, needs significant evaluation. An example of this would be to consider bundling Collection and Use together, but keep Marketing separate. There are many permutations to this proposal, and each will have a variable impact on a Consumers cognitive load, willingness to proceed, and implied agreement. To give an example, a Consumer is likely to use the CDR to establish facts with a lender regarding their ability to repay. If a Recipient required an approval of marketing consent in order to achieve this goal, the user may find themselves in a situation where they are caught between a need to achieve an outcome (i.e., lending approval) versus a willingness to receive marketing material from a finance provider. It is our opinion that this could lead to dangerous consequences potentially colliding with the hawking provisions outlined in Regulatory Guideline 38.

Secondly, the behaviour of a withdrawal, particularly one initiated from a Data Holder, does not appear to be appropriately considered. If a Consumer chooses to withdraw their consent from the Data Holder (currently only impacting the Collection consent) it is unclear what the intention is regarding other consent types which were bundled in the original establishment of the arrangement. If this was to trigger only the Collection Consent withdrawal (as would be the case now), the Consumer perception of a consent would be different between a Holder and a Recipient, and the presentation of the bundle would be incorrect. Conversely, the splitting of a bundled consent on event trigger would in essence alter the original parameters of the arrangement in such a way it would need to be dynamically unbundled.

Finally, we question the veracity of statements regarding Recipient behaviour to be aligned with what is “reasonably required” to achieve the objectives of a use case. Our observations in the live ecosystem are that many Recipients have an extremely broad view of “reasonable”, and resolving this could only be done using a high stakes regulatory enforcement approach. Regardless of the outcome of such an approach, this could cause significant damage to the broader trust of the entire ecosystem.

Question 2: Should disclosure consents be able to be bundled where the service requested by the consumer is for their data to be collected and disclosed (e.g. as an insight or to a trusted adviser)?

We refer to our response to Question 1 as the problem space is similar. With regard to the example posed our view is that there is consequential liability impacts of doing so whereby a Data Recipient Software Product, which was responsible for bundling, now has a potentially vicarious liability with regards to misuse by a Trusted Advisor. It is unclear how this could be reasonably resolved in a way that is accessible to a Consumer without forcibly making the Data Recipient complicit and responsible for the behaviours of a rogue Trusted Advisor.

Question 3: Do you consider clarification is required with respect to how CDR consents may be requested where non-CDR permissions, consents or agreements are requested for the same service? If so, what changes should be considered?

Clarification would be helpful with respect to providing clear visual cues as to which parts of data disclosure etc. are covered by the CDR framework and which parts are not. With that said Biza, sees



Biza Pty Ltd t/a Biza.io
ABN: 54 624 797 655
Level 6, 25 King Street
Bowen Hills QLD 4006
Tel: +61 1300 MY BANK
www.biza.io

significant value and innovation opportunity in the ability for a Recipient, and potentially a Holder, to incorporate permissions outside of the boundaries of the CDR into a single consent flow.

Question 4: What are the key opportunities associated with combining or integrating CDR and non-CDR consents within a single consent flow? Are there any barriers or risks associated with these opportunities?

A key opportunity provided by this capability is for a service provider with access to multiple ecosystems (for instance, CDR, NPP² and ConnectID³) to provide a service of significant value while alleviating cognitive load through a unified consent workflow.

Question 5: Do you support the ability for ADRs to pre-select or clearly indicate datasets, specified uses and consent durations where their selection is essential for the service? Do you consider the proposal strikes the right balance to reduce cognitive load while maintaining informed consumer consent?

Biza is supportive of this proposal but believes it should be informed by sufficient research that assesses interactions patterns of both data clusters and consent types. Our view at this stage is that Consumer research has been conducted on an individual basis for these two different problems spaces and more research is therefore needed.

Question 6: Are there specific design patterns or approaches that you support to ensure that the data types and consent duration are clear to the consumer in the consent?

We support design patterns that are sufficiently supported by Consumer research. At a high level, preselection of duration and minimum required datasets while communicating purpose seems reasonable, but we note that the scope of this consultation appears to have arbitrarily excluded (and in fact made almost entirely invisible) the Holder component of the arrangement establishment.

We note that existing consumer research and promotions by representatives of the Australian Government at industry events, has included patterns which are not technically possible. We implore Treasury to avoid research more akin to marketing assessment than tangible, implementable and real-world evaluation.

Question 7: Do you support the proposal to remove withdrawal of consent instructions from the consent flow and instead provide them in the CDR receipt?

While the research presented suggested that Consumer feedback wasn't negative it was unclear as to whether the removal of the content resulted in a positive decrease of cognitive load, a key reasoning specified as conducting the research to begin with.

Nonetheless we don't oppose making this content optional and support making it mandatory in the CDR Receipt.

² <https://www.rba.gov.au/payments-and-infrastructure/new-payments-platform/>

³ <https://connectid.com.au/>



Question 8: Do you support the proposal to remove information about the consequences of withdrawing consent from the consent flow?

We are generally supportive of this proposal but there is currently no mechanism for the Holder to provide this information to a Consumer within the Holder side dashboard. We note that while a reference could be given to the relevant CDR Policy, these policies are often hard to find and are not generally Consumer friendly (i.e., the CDR Policy of all Recipients we are aware of is an extremely high cognitive load).

Question 9: Do you agree with the proposal to align the consent information requirements for OSPs, sponsors, and principals?

Biza supports the idea that information should be aligned, irrespective of the Recipient's delivery and enablement approach.

Question 10: Do you consider ADRs should notify consumers if the list of supporting parties that may access a consumer's CDR data changes? If so, how should this notification be made?

Biza is supportive of notifying consumers of changes to supporting parties. Methods for doing this are worthy of consideration but we assume this would be via existing digital channels or contained with the regular 90-day consent notifications.

Question 11: Are there any further issues that should be considered in relation to supporting parties?

Biza believes it is critical that the visibility of supporting parties at a Data Holder level is resolved. Data Holders are currently being exposed to significant third and fourth party liability for which they have no means of appropriately assessment. The impacts of this with respect to risk management and insurance coverage are significant and have not been properly considered to date.

Question 12: Do you support the proposal to clarify the rules on CDR receipts by explicitly specifying the content of CDR receipts?

Resolving the significant amount of ambiguity in the CDR Rules in general should be considered a first order priority of Treasury. As such we are supportive of any Rules clarification that reduces ambiguity.

Question 13: Do you support the proposed information required to be contained in a CDR receipt?

Biza is supportive of specifying a minimum amount of information to be included in the CDR Receipt. We recommend allowing for information beyond the minimum to be reasonably included in the same receipt (i.e., set a minimum, not an absolute).

Question 14: Do you support the proposal to allow 90-day notifications to be consolidated?

Biza is supportive of notification consolidation wherever possible. We note that a vast number of Consumers *do not read* information-dense emails thoroughly and consideration should be given to providing alternate notification methods such as in-app notifications.



Biza Pty Ltd t/a Biza.io
ABN: 54 624 797 655
Level 6, 25 King Street
Bowen Hills QLD 4006
Tel: +61 1300 MY BANK
www.biza.io

Question 15: Do you support the proposal to allow consumers to tailor the frequency and delivery of 90-day notifications?

Biza supports the proposal to allow for tailored notification frequency and delivery mechanisms. We note this would align with the generally accepted expectations on Data Holder implementations and believe that rather than allowing such tailoring, consideration should be given as to whether it is mandated.

We are unclear if a customisable frequency would include “Off” as it exists in Data Holder environments but believe this is a valid option to be offered to a Consumer. Additionally, there is little elaboration provided on variability of delivery mechanisms (e.g., email, sms, push notification etc). We note that delivering the quantity of proposed information via SMS would likely be impractical, and we have observed these adverse outcomes on the Data Holder’s side as a result, which we consider unreasonable in the context of Consumer comprehension.

Question 16: Do you support the inclusion of additional information within the 90-day notification, including specific details about all active consents? Are the proposed information requirements appropriate?

We are generally supportive of this proposal but are concerned about the length of the notification in email form. A very large email will have both cognitive and technical transmission limits and which may actually result in the opposite outcome than that intended. We believe it would be more suitable to define a summarisation format .

Question 17: Do you support a ‘deletion by default’ approach to redundant data handling?

Biza is strongly supportive of deletion by default. We have observed existing Recipients in market *deliberately* obfuscating the option to turn this functionality off, presumably for their own commercial reasons we suspect relate to a desire to use the information to optimise transaction classification engines.

Question 18: Do you consider this approach will have a positive impact on consumer experience with the CDR, and on the privacy and security of a consumer’s CDR data?

Biza agrees this will have a positive impact on consumer experience. In the context of data breaches, providing clear and unambiguous information on when an organisation can no longer access Consumer data, helps Consumers self-assess their vulnerability to a data breach.

Question 19: Do you consider this approach will have a negative impact on ADRs that seek to derive value from de-identified CDR data?

Biza does believe this will have a negative impact on ADRs. While it is understood such data is useful for activities such as training classification capabilities our opinion is that this should not override the importance of a Consumer’s ability to provide explicit and informed consent.

Our current market observations are that certain ADRs are placing their commercial priorities above the best interests of Consumers in this respect.



Biza Pty Ltd t/a Biza.io
 ABN: 54 624 797 655
 Level 6, 25 King Street
 Bowen Hills QLD 4006
 Tel: +61 1300 MY BANK
 www.biza.io

Question 20: Do you consider the standard of de-identification in the CDR Rules is appropriate for the intended uses of data by ADRs?

The existing de-identification process is extremely vague, non-prescriptive and likely easily worked around by recipients using market adoption as leverage with the regulatory body expected to validate the method used. Put another way, we do not believe the existing regulatory capacity has the technical capability nor research experience to quantify if a proposed mechanism for de-identification is appropriate.

Our view is that for the known use case (transaction training engine optimisation) *any* de-identification method used would be insufficient as, by definition, the training of an engine to classify transactions would require the location information of the transaction (i.e., the vendor from which goods were being purchased) which, by definition, would fail to meet the bar for having consideration for “*any person to be once more identifiable, or reasonably identifiable*” (CDR Rules 1.17(2)(c)).

Question 21: Do you consider the inclusion of new rules or standards on dark patterns could be effective in mitigating the risk of ADRs designing consents that undermine informed consent and consumer control?

Biza supports the inclusion of rules or standards to ensure dark patterns do not diminish the trust being established in the nascent CDR ecosystem. We note that while the Rules and CX Guidelines are extensive with regards to Data Recipients, the Data Standards themselves are heavily weighted towards Holder implementations. On this basis our view is that Data Recipients are regularly ignoring the *intent* of the Guidelines in the absence of prescribed Standards.

Question 22: Are there specific dark patterns that you consider should be addressed within CX standards or guidelines?

Based on real-world experience of active use cases Biza notes the following specific dark patterns are already present and actively being utilised by Data Recipients:

1. Toggles for de-identification consent being hidden behind accordions with no relevance to de-identification
2. “Optimised” consent flows providing zero pre-amble or consent priming to the Consumer
3. CDR Policy documents which *cannot be found* within Consumer experiences
4. Representatives linking to the CDR Policy document for the Unrestricted Recipient, confusing Consumers on what it is they are agreeing to

We strongly support adding principals-based requirements to the CDR Rules to make it unambiguously clear that Dark Patterns are prohibited in the CDR. Given the prevalence of their use in existing solutions we are of the opinion the Government should seek to make this subject to a civil penalty.



Biza Pty Ltd t/a Biza.io
ABN: 54 624 797 655
Level 6, 25 King Street
Bowen Hills QLD 4006
Tel: +61 1300 MY BANK
www.biza.io

Question 23: Are there any further issues that should be considered in prohibiting the use of dark patterns?

Introducing an explicit ban on unwarranted friction within Recipient solutions should be introduced. This would be aligned with the existing Standards obligation Holders have.

Question 24: Do you support further work in relation to the above areas? Are there areas that should be prioritised?

While we are supportive of continued work on user interaction patterns, we continue to be concerned that this is often done in isolation of the technical reality of authentication, authorisation and generalised identity management. Without appropriately informed technical assessment, further consent review stands the risk of creating visually attractive but technically worthless outcomes.

Question 25: Are there other issues, areas, or improvements that should be considered to improve CDR consents?

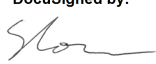
Biza is of the opinion that by constraining this consultation to Data Recipient interactions it has missed an opportunity to holistically assess the Consumer experience across both Recipient and Holder.

We are wary of a situation where Rules and Standards development will be constrained because the existing technical implementation is inflexible and brittle in nature. We strongly recommend that Treasury consider broader changes to how information between Recipients and Holders can be exchanged to provide a more consistent consent experience between both parties.

Conclusion

We thank you once again for the opportunity to comment on these proposals. If you have any questions or concerns regarding this submission, please do not hesitate to contact Stuart Low, Founder & CEO on 1300 692 265 or at industry@biza.io.

Kind Regards

DocuSigned by:

18F97178F0E740B...

Stuart Low on behalf of Biza Industry Advisory Committee
Founder & CEO
Biza.io