Data Standards Body | The Treasury

Noting Paper 273 – Consent Review

Consultation
16 November 2022 – 09 December 2022

Contacts
Michael Palmyre, Consumer Experience Lead, Data Standards Body
Nathan Sargent, Senior Adviser, Treasury

Overview

The Data Standards Body (DSB) and Treasury are exploring opportunities to simplify the Consumer Data Right (CDR) consent rules and standards to support a better consumer experience while maintaining key consumer protections. The mission statement of the review is to help organisations provide intuitive, informed, and trustworthy consent experiences that enable positive outcomes for CDR consumers.

The purpose of this noting paper is to accompany the workshop on 22 November to gather CDR community views on preliminary change proposals and the priority of items that may be considered for future amendments to rules and standards. The noting paper will be open for feedback until 9 December 2022. Anyone unable to attend the workshop may provide written feedback via the DSB GitHub page by this date.

Outcomes from the workshop will inform proposals for a joint Treasury/DSB rules and standards design paper in early 2023. This will provide an opportunity for interested stakeholders to make submissions on proposed amendments prior to formal consultation on rules and standards.

The initial scope of this review will examine options to improve the consumer experience that minimise impacts on existing implementations. This will focus on 'non-breaking' Accredited Data Recipient (ADR)-side changes, including consent steps, ADR dashboards and notifications, and related ADR requirements. A review of the authentication flow is being conducted separately.

A subsequent review will consider Data Holder (DH)-side changes, including the authorisation flow, DH dashboards and notifications, amending consent, and other recommendations to support future developments for the CDR, such as action initiation. For example, the interaction between the CDR consent framework and existing consent mechanisms for specific actions may require further consideration. Feedback on these and other priority change candidates is also welcome.

This paper covers:

- Background
- Consent principles
- Consumer Experience (CX) research
- Content and Interactions
- Separation of consents (bundling)
- De-identification and consent

Background

Consumer consent plays a central role in the CDR. Consent-driven data sharing provides consumers with control over their data. The rules require consent to be voluntary, express, informed, specific as to purpose, time limited, and easily withdrawn. To enliven these objects of consent, various requirements are articulated in the CDR rules and standards.

The performance of the rules and standards for consumer consent has been a consistent focus for stakeholders. The independent Statutory Review of the CDR highlighted issues experienced by participants and consumers in engaging with the CDR consent process.[1] The Review recognised the importance of revisiting consumer consent journeys as the CDR evolves to ensure the initiative continues to deliver consumer benefit, especially as it evolves to include action initiation.

Consent Principles

The object statement in the CDR consent rules provides a strong foundation for giving and amending CDR consents. The elements of the object statement can be described as follows:

- **Voluntary** refers to consumers' having genuine choice about whether they give their consent. The requirement for consent to be informed, time limited and easily withdrawn is critical to consent being voluntary.
- **Express** refers to consumers actively expressing their consent, which cannot be implied.
- **Informed** refers to information provided to consumers on the implications of providing consent. The currency of consent is maintained through ongoing engagement, such as appropriate notifications and re-consents.
- **Specific as to purpose** refers to consent being requested for targeted reasons rather than broad, generic, or ambiguous uses.
- **Time limited** refers to consent being requested in relation to a specific and finite period. The period can only be extended with a consumer's consent.
- **Easily withdrawn** refers to the ability to stop data being shared and used in a way that is accessible to the consumer.

Based on these objects, Treasury and the DSB have developed consent principles to guide and assist the assessment of proposed amendments to the rules and standards. The consent principles incorporate each of the elements described in the object statement and reframes them to centre on consumer experience and desired consumer outcomes – including, for example, that CDR consents are intuitive and trustworthy for consumers.

The consent principles are as follows:

1. Consent is inclusive, empowering and creates positive outcomes
2. Consent is given freely and enthusiastically
3. Consent is specific, current, and reversible
4. The consent process is intuitive and comprehensible
5. The CDR is trustworthy and meets expectations

[1] See: https://treasury.gov.au/publication/p2022-314513

CX Research

To support this work, the DSB's CX team has engaged over 300 consumer participants in three rounds of research from September to October 2022. This section provides an overview of this research. The primary research question was:

How might we simplify the consent model while maintaining intuitive, informed, and trustworthy consent experiences?

To answer this question, the CX research focused on the following areas:

- **Content presentation**, including existing requirements relating to withdrawal instructions, notifications, supporting parties, data handling, CDR receipts, and descriptions of datasets
- **Consent separation**, including the current treatment of certain consents as 'separate', particularly collection, use, and disclosure consents
- **Interaction requirements**, such as the active selection of each dataset, use, duration, and the right to delete functionality.

The CX team applies design thinking for research and development using the 'Double Diamond' process. Qualitative approaches are used to help answer 'why' consumer behaviours and sentiments exist, and quantitative approaches are used to help answer 'what' is occurring at scale. Methods include in-depth interviews, moderated and unmoderated prototype testing, and surveys. The consent review research tested iterations of the change proposals outlined in this paper, but the analysis also considered CX research conducted to date with over 600 consumer participants.

The change proposals in this paper were tested using a prototype that consumer participants interacted with, followed by accompanying questions to gauge how intuitive, empowering, trustworthy, and comprehensible the experience was. In general, design changes were considered based on how they might reduce unnecessary content, minimise the level of required interactions, and provide lower levels of friction while still upholding the consent principles and the objects of consent in the rules.

Round 1

The first round of research focused on the current state consent flow to establish a benchmark using key metrics aligned to the consent principles. This round used surveys to capture data sharing attitudes and preferences in response to different value propositions – including scenarios that may be perceived as high/low risk and benefit. It also tested an unmoderated prototype of the current state consent flow to capture metrics on task completion, participant engagement and ability, comprehension, and trustworthiness.

Round 2

The second round of research used the same metrics to test a simplified consent flow prototype. The development of this prototype was guided by the consent principles and in response to issues identified by CDR agencies, the community, past research, and heuristic analysis.

Round 3

The third round of research iterated on the change proposals tested in round 2 using the same approach and metrics to aid ongoing comparisons. This round focused on design changes rather than alternative policy settings.

Preliminary findings

A final report will be published to outline the findings of this research, which will include the artefacts used in the research, and more comprehensive details on methodology and analysis. To support transparent consultation in the interim, the below statements provide preliminary insights from the research:

The consent flow can be simplified without undermining consumer protections and expectations.
The research suggested that, taking margins of error and broader variables into account, levels of intuitive use, empowerment and trustworthiness were generally similar for the current state of the consent flow and a simplified version. That is, simplifying the consent flow did not have a significant impact on the experiences, sentiments, and confidence levels of consumer participants.

Attitudes towards CDR are shaped by broader data safety contexts.
The research also suggested that events beyond CDR notably shaped perceptions and attitudes towards CDR data sharing in general. Research spanned from early September to late October 2022, with some rounds taking place before multiple high-profile corporate data breaches in Australia, and some at the height of these breaches. While not all participants were directly affected by these data breaches, many cited these recent events as reasons for viewing data sharing, including through CDR, as risky.

More information and control may not equate to higher comprehension and empowerment.
Research indicated that some participants struggled to understand various date ranges presented throughout the consent model (such as the sharing period, use period and historical data periods). While a simplified consent flow attempted to improve the ability to comprehend these differing periods, consumer participants' recollection of the duration of their consent actually decreased when compared to the current state. Conversely, the removal of elements of control in the simplified consent flow – such as the ability to actively select certain options – had a negligible impact on consumer perceptions of empowerment and ability and, based on previous research, may have also supported higher levels of comprehension.

The CDR consent flow meets and exceeds consumer expectations.
Overall, the majority of participants rated the simplified flow as very fast and extremely easy to complete, very easy to understand and much easier than existing data sharing methods.

Content and Interactions

This section outlines various areas of the rules and standards relating to consent and interaction requirements that may warrant revision. The current consent flow requirements include that ADRs must make specified information and interactions available to CDR consumers. This includes, for example, that consumers be able to expressly agree to specific elements of a consent request, which cannot be pre-selected, by actively selecting them, and that specific information be provided about various operations. The proposals in this section seek to consolidate some of these requirements and reduce the extent of unnecessary interactions and information.

Pre-selected and actively selected options

The 4.11 rules include requirements for consumers to actively select or otherwise clearly indicate:

- the particular types of CDR data they consent to being collected;
- the specific uses of collected data;
- if the consent is to apply on a single occasion or over a specified period of time; and
- the period of the collection, use, or disclosure consent.

The rules also prohibit the pre-selection of these options and suggest that un-filled checkboxes for certain options, such as each type of data, could be presented to the consumer for selection. Live implementations of these requirements include checkboxes next to each dataset, as well as interactions that require the selection of the consent duration. Community feedback and heuristic analysis has suggested that while these requirements imply a higher level of consumer control, it also introduces a false choice where the options are required for the service to function. In such a scenario, if a consumer were to continue without actively selecting the options presented, they would not be able to receive the good or service they were attempting to acquire.

The requirement to actively select these options, and to prohibit their pre-selection, could be revised to address these issues. This could, for example, allow options to be pre-selected and clearly indicated provided they are essential to the provision of the good or service. Conversely, if the requested options or terms are not essential, the existing requirements to actively select the option(s) could still apply. This may look like required datasets being listed without checkboxes, and optional datasets being listed with checkboxes. It could also manifest in pre-set but editable durations for a consent where the provision of the good or services affords that flexibility. With this approach, ADRs could still invite a consumer to opt-in to additional terms or options that are not essential to the provision of the service, but these would not be on by default.

Evidence from CX research to date supports this approach. The research suggests that allowing consent to be provided for all essential options at once, provided they are clearly indicated and essential to the service, can be done without negatively impacting informed consent.

Data language standards

The data language standards must be used to describe CDR data to consumers. These include ‘data cluster language’, which constitutes the ‘primary’ heading for a grouping of datasets, and ‘permission language’, which lists more specific information that may be shared as part of the data cluster. To provide additional flexibility and to support any changes to the pre-selection and actively select requirements, these standards could also be revisited.

In CX research to date, a range of design patterns have been tested to understand how datasets could be presented to consumers in a way that limits cognitive load yet facilitates informed consent. A 'details' design pattern was tested in 2021 disclosure consent research and 2022 consent review research rounds. This research suggested that consistent and standardised language assisted informed consent and comprehension and met consumer expectations. This was especially important when it came to describing data clusters. It was possible, however, to maintain consumer comprehension by applying the more granular permission language in a more conversational way than is currently being done in the CX Guidelines and live implementations.

The data language standards could be revised to make clear that ADRs and DHs to apply certain aspects of the data language standards more conversationally. This could include, for example, that CDR participants are not required to 'list' permissions in a rigid manner. Such changes could also introduce greater flexibility for future developments, such as action-initiation, where the complexity of term(s) being consented to may be impractical to comprehensibly explain with concise and prescriptive language.

Withdrawal of consent information

As part of the consent flow, ADRs are required to provide consent withdrawal details. These details include that consents can be withdrawn at any time, instructions for how to withdraw a consent after it is given, and the consequences of withdrawing a consent. To reduce cognitive load, the amount of content provided in the consent flow could be revisited.

CX research indicated that the absence of specific withdrawal instructions did not negatively impact trustworthiness or informed consent. Providing these instructions in the CDR receipt instead was seen as sufficient for the purposes of engagement, recall, and comprehension. Research also suggested that displaying the consequences of consent withdrawal on-screen may be unnecessary. Over 90% of consumer participants understood the consequences of not consenting without being presented with such information because the consequences of not proceeding were implied.

If a consumer did attempt to exit the consent process, an ADR using best practice design patterns would still need to consider communicating the consequences of cancelling the process, but this should be done in a way that is non-coercive and does not constitute a dark pattern. Being notified during the consent flow that consent can be withdrawn at any time, however, improves trustworthiness and the propensity to willingly consent as it clarifies that the action can effectively be reversed if desired.

Authentication information

The authentication standards focus on DH requirements, but also outline specifications for ADRs. This includes a statement that CDR participants do not need to access consumer passwords for the purposes of sharing CDR data, and that a 'One Time Password' will be used instead – which must be explicitly referenced in the statement as per the standards. These requirements were developed to provide consistent messaging between ADRs and DHs regarding the sole approach to authentication in CDR, and to help mitigate phishing risks by establishing an awareness around the absence of password sharing in CDR.

In research to date, consumer participants concerned about the security of authentication have generally focused on the sharing of passwords. The statement that passwords will not be shared was viewed as sufficient for assuaging these concerns and increased confidence in the process. ADRs specifying 'One Time Password' to consumers may be an unnecessary technical detail to include. Further, the DSB is reviewing the existing approach to CDR authentication as a separate stream of work, which may result in alternative authentication methods being used. As such, future approaches may not be reliant on a 'One Time Password', making this requirement in the authentication standards redundant.

Ahead of the broader work on authentication uplift, the current authentication standards could be amended so that ADRs no longer need to reference a 'One Time Password' and only need to state that passwords do not need to be shared.

Supporting parties

The rules requirements are inconsistent between the displaying of the names of sponsors, principals, and outsourced service providers (OSPs). The names of sponsors and principals must be displayed, while ADRs need only note that OSPs are involved and to see the CDR policy for more details. Up-front information is required regardless (unless the ADR is unrestricted and does not use any OSPs), but what should be displayed is inconsistent. The CX Guidelines suggest consistency in this regard, but the rules requirements for displaying sponsors, principals, and OSPs could also be reconciled for consistency.

In CX research to date, consumer participants have consistently articulated the importance of outlining all parties involved in the process who may access the data. A revision of these rules may result in this content being consistent regardless of the access arrangement, such that the entity is listed regardless of whether they are an OSP, principal, sponsor, or perform another role. Noting that the involvement of certain parties may change over time, this content could be based on an ADR's supporting parties at the point of consent, and the CDR policy could be referenced for an up-to-date list.

90-day notifications

ADRs are required by the rules to provide a notification to a consumer every 90 days to remind them that a collection or a use consent is still current. Based on this requirement, if a consumer provides 5 consents to an ADR over the course of 5 days, the consumer may receive 5 separate notifications over 5 consecutive days, every 90 days. These rules only require that a consumer be reminded, and they do not outline any other content that the reminder should contain.

CX research has explored the frequency of notifications from various angles. In general, contextual notifications delivered in a timely way are considered useful and necessary, but an excessive number of notifications – particularly where the content is not tailored, informative, or actionable – may be unwelcome. The concept of 'notification fatigue' is widely recognised and a heuristic analysis suggests that amendments to this requirement would result in operational and consumer experience improvements.

The 90-day notification requirements could be amended to allow such notifications to be consolidated and tailored according to consumer preferences. For example, a consumer could be reminded of *all* current consents with an ADR every 90 days or could choose to receive these notifications in line with their existing preferences – which may be to receive them less often, or in response to a specific trigger. The 90-day notification could also be made more useful and actionable with the inclusion of specific details, such as instructions for how to review and withdraw consents.

Dark patterns

Removing prescription from the rules and standards provides greater implementation flexibility. This should be done in a way that manages the potential for unintended consequences and undesirable behaviours that may undermine the consumer protections currently articulated as required. To do

this, alternative principle-based measures and additional guidance may need to be considered to discourage undesirable behaviours. The use of 'dark patterns' is one such example.

'Dark patterns' are a relatively new and emerging concept in privacy law and the field of human-computer interaction. The ACCC's Digital Platform Services Inquiry defines dark patterns as '[t]he design of user interfaces intended to confuse users, make it difficult for users to express their actual preferences, or manipulate users into taking certain actions.'

Dark patterns have not been defined or prohibited in the context of CDR. However, dark patterns have been explicitly considered and prohibited in various other jurisdictions, including the California Privacy Rights Act (CPRA), the Colorado Privacy Act (CPA), the Virginia Consumer Data Protection Act (VCDPA), and the European Data Protection Board.

To date, CX research and CX Guidelines have explicitly avoided the use of dark patterns, but live CDR implementations exhibit designs that would be considered dark patterns. In the context of CDR, this might include emphasising certain actions or settings over others to enable more data collection or the granting of additional permissions when seeking consumer consent, or by making consent withdrawal more difficult than the process of granting consent in the first place.

There is a growing body of evidence highlighting the need to deal with the practice of 'dark patterns' online, particularly in relation to consent. A public report developed by the Consumer Policy Research Centre (CPRC) for the DSB recommended that CX standards for dark patterns be made. This could manifest as a principle-based requirement prohibiting dark patterns to strike an appropriate balance between the removal of prescription in the rules and standards and the usefulness of parameters to maintain consumer protections. A principle-based requirement could simply prohibit interfaces, choice architecture, and design patterns that undermine, impair, or subvert user autonomy, choice, and decision making, and the CX Guidelines and other guidance could then provide relevant visual and theoretical examples to guide implementations.

Dashboards for once-off consents

Consumer dashboards provide an important mechanism for consent withdrawal and the ongoing management of consents. The rules require that ADRs and DHs provide dashboards, wherein a consumer can review the terms of consents and authorisations they have given, withdraw those consents or authorisations, review and manage various settings related to their data and, among other things, request records relating to the sharing of their data.

Insights from preliminary research and heuristic analysis suggest that where a consent is given to collect CDR data once but not use that data for an ongoing period, ADR dashboards may not be necessary. The absence of this requirement for such a scenario could lower the cost and complexity of implementation for ADRs that only intend to support once-off consents.

The rules could be reviewed to facilitate this particular use case and would need to consider interrelating requirements, such as how dashboard requirements remain intact where a consumer also has an ongoing consent with the ADR and how relevant records can be requested. The equivalent requirement for DHs could also be reviewed, but further considerations would need to be made for how various online services would be provided, including the disclosure option management service, secondary user instruction service, and potentially the nominated representative service.

CDR receipts

The 4.18 rules require that ADRs provide a CDR receipt after a consent has been given, amended, or withdrawn. The details to be included in this receipt include the names of the parties to whom the consent relates, details such as the period of the consent and the associated data, and any other information provided to the consumer when obtaining the consent.

CX research has shown that the CDR receipt provides a critical record of consents for later reference, but also to maintain informed consent and comprehension after a consent has been given. This is because the current approach to informed consent relies on the ability for a consumer to comprehend and recall the extensive detail they are presented with during a critical and time-constrained decision-making process. While certain information should be shown prior to granting consent, other information is better contextualised after consent has been provided, such as dashboard access and withdrawal instructions. The CDR receipt is an important artefact that can provide relevant information contextually while also serving as a record of what was agreed to that can be accessed later as necessary. The CDR receipt will play a more fundamental role in maintaining consumer comprehension and control if a revision of the rules and standards results in less information being provided in the consent flow itself.

The CDR receipt rules could be made more explicit about what to include, and when to provide a CDR receipt. Currently, the CDR receipt rules broadly require the inclusion of any information that was presented to the consumer in the consent flow. This could be refined to specify key and meaningful details; avoid extraneous information; and specify the inclusion of other information that may not currently be present or that may be removed from the consent flow to support simplification.

Separation of consents (bundling)

The CDR rules restrict CDR consents from being bundled with other directions, agreements, consents, or permissions. However, for an ADR to provide services using CDR data, the consumer would generally be required to agree to multiple ‘consents’ to collect, use and/or disclose their CDR data. Separating CDR consents can result in more complex and duplicative consent flows than is necessary. It also presents a false choice to the consumer where each consent is necessary for the service to function.

CX research has suggested that duplication of consent actions for the one good or service (for example, multiple checkboxes and durations) may cause confusion and reduce comprehension and informed consent. However, presenting ‘separate’ consents together in the same request has consistently matched consumer mental models in CX research to date, provided the consent requests were related and necessary for the service.

The bundling restriction could be clarified to allow ‘bundling’ of CDR collection, use and/or disclosure consents where these consent types are necessary for the provision of the requested good or service. That is, a consumer could be asked to agree to multiple consent types with a single action provided each consent is necessary for the provision of the service. The consumer would still be presented with all necessary information about the consents they are agreeing to in order to receive the good or service. Consents that are not necessary for the provision of the good or service

should not be 'bundled' – for example, consents for optional or 'add-on' goods or services, direct marketing consents, and de-identification consents.

De-identification and Consent

The CDR rules allow an ADR to de-identify consumers' CDR data in several ways, including where a consumer has provided a de-identification consent, or if the CDR data becomes redundant and a consumer has not elected that their data be deleted instead.

CDR data becomes redundant when an ADR no longer needs it for a purpose permitted under the CDR rules. The ADR may either delete the redundant CDR data, or de-identify it in accordance with the de-identification process in the CDR rules. If an ADR intends to de-identify redundant data, then the ADR must allow the consumer to elect that their redundant data be deleted (instead of de-identified), in the consent flow, in writing, or through their consumer dashboard.

Consumers can separately provide a de-identification consent to an ADR. If a de-identification consent is sought, then the 4.15 rules require the ADR to state to the consumer that the data could be disclosed and sold to other persons; the classes of persons who might access that data; why the data would be disclosed; and, if the ADR intends to use it for general research purposes, the kind of research to be conducted. If an ADR intends to de-identify data when it becomes redundant, the 4.17 rules require the ADR to state similar but fewer details to the consumer.

The potential interactions between consumer elections to have their redundant data deleted and consumers separately granting de-identification consents are complex and likely to lead to confusion. For example, if a consumer provides a de-identification consent and subsequently elects to have their redundant data deleted, they may not understand that their data can continue to be de-identified prior to it becoming redundant, and that any de-identified data would not be deleted.

Stakeholders have cited concerns and difficulties with the approach to de-identification in CDR. This includes that the rules on de-identification are complex and overlapping; that de-identifying consumer data is difficult to achieve in practice and, as such, may represent a risk to informed consent and consumer privacy. CX research has shown that consumer participants have a poor understanding of de-identification and the processes for electing that their data be deleted instead. An analysis of live implementations suggests that the de-identification of CDR data may be an existing aspect of some ADR business models, while other ADRs are deleting redundant data by default.

While we are not proposing specific changes at this time, community feedback is invited on the requirements and processes relating to de-identification and deletion in CDR, including if revisions should be considered.

Feedback

We welcome feedback on the following questions:

1. Do you agree with the preliminary proposals in this paper? If not, what changes or revisions should be considered?
2. Do you agree with the initial scope of the consent review? If not, what might an alternative scope be, or what other changes should be considered as a priority?
3. If the proposed changes were made, are there any implementation or consumer impacts that need to be assessed?
4. If the proposed changes were implemented, how might their success be measured? What mechanisms in CDR exist, or should be proposed, to measure a consumer's experience of the consent model?
5. Do you have any views on what consent issues may need to be considered to support the CDR's expansion into action and payment initiation?