Consumer Data Right

Proposed amendments to the CDR rules: Consent Review rule changes and operational enhancements

Privacy Impact Assessment

Prepared for

The Department of the Treasury

7 June 2024

Table of Contents

1 Executive Summary

About the Operational Enhancements and Consent Amendments

1.1 The Department of the Treasury (the **Treasury**) is reviewing the *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) (the **CDR Rules**) to ensure the CDR Rules are 'fit-for-purpose' and support the policy aims of the Consumer Data Right (**CDR**).[1]

1.2 This PIA has been progressed as an iterative project in parallel with:

(a) Treasury's development of design papers, for public consultation, which outlined a series of proposed amendments to the CDR Rules about consent and operational matters;

(b) A public consultation process where stakeholders were invited to give feedback about the proposals outlined in the design papers; and

(c) Treasury's refinements to its proposals to amend the CDR Rules to achieve the objectives referred to above.

Summary of Privacy Impacts, Risks and Recommendations

1.3 This privacy impact assessment (**PIA**) report sets out Mills Oakley's independent review of the proposed amendments to the CDR Rules. The following recommendations have been made to eliminate, or to mitigate, potentially negative privacy impacts on CDR consumers.

Recommendations	Page Reference
Recommendation [1]: The Treasury consider whether 'reasonably needed' is sufficiently narrow to avoid function creep and the inadvertent expansion of consent requests. If the term will be interpreted narrowly and supports an inference that the consent request must be essential to provide the product or service, this could be addressed in guidelines that Treasury has indicated it intends to explore with OAIC and the ACCC.	9
Recommendation [2]: Treasury consider whether excluding disclosure consents from consent bundling usefully reinforces transparency requirements about the parties with whom a CDR consumers' data is shared.	10
Recommendation [3]: As an alternative to Recommendation 2, Treasury consider a measure that gives CDR consumers the right to object to bundled consents which would trigger an obligation for the accredited person or ADR to explain the basis for the conclusion that the consents are essential to provide the product or service. A right to object, in this context, could conceivably be aligned with Privacy Act reforms, in the event a right to object to certain privacy practices is progressed by the Australian Government.	10
Recommendation [4]: Subject to Recommendation 3, Treasury consider whether guidelines and CX Standards would be an appropriate vehicle to clarify (a) whether a consumer can override pre-selected options and (b) the level of detail necessary to explain why a pre-selected option is necessary to deliver the product or service.	13

[1] The Australian Government, The Treasury, *Operational Enhancements – CDR Rules Design Paper* ([August] 2023) pg 3 para [1].

Recommendations	Page Reference
Recommendation [5]: Treasury consider whether guidance, such as in CX Standards, might encourage an Accredited Person to tell consumers, as part of a consent flow, where to find further information about withdrawing consent.	15
Recommendation [6]: Treasury's regulatory response (if any) to mitigate the risk of dark patterns being used in CDR user experience design patterns and consent/authorisation architecture should be informed by the Privacy Act reforms on this issue.	22
Recommendation [7]: Treasury consider supporting any regulatory response or guidance material about avoiding dark patterns with visual examples of what is not permitted (i.e. an illustrative example of a dark pattern in a CDR context).	23
Recommendation [8]: Noting that the Treasury has narrowed the scope of the proposal such that the data in question has been obtained in connection with an application to acquire a product or service, Treasury may wish to consider whether the CDR consumer's decision (and autonomy over the CDR data) would be assisted by an explanation by the ADI about the *practical consequences* of consenting to the ADI holding the data as a data holder.	32
Recommendation [9]: Treasury consider the feasibility of a regulatory and enforcement strategy that is calibrated to support small retailers meet their CDR obligations rather than defer the application of those obligations.	37
Recommendation [10]: Treasury consider the combined and sequential operation of: • the deferred application of CDR Rules for certain cohorts; and • the exemption for trial products/plans; on an individual customer whose CDR experience is that their CDR data is not protected by the full suite of CDR rights and protections. One way this risk might be avoided is to ensure that a small energy retailer cannot offer only trial plans.	38

2 About this Privacy Impact Assessment

Focus of this PIA

2.1 Mills Oakley was engaged by the Treasury to prepare a PIA on proposed amendments to consent procedures and further operational enhancements to the *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) (**CDR Rules**). The Treasury is exploring options to:

(a) simplify the CDR Rules to support better consumer experiences while maintaining key consumer protections; and

(b) support the development of CDR Rules to ensure they are 'fit for purpose' and appropriately calibrated to the policy intent of the CDR.

2.2 This PIA identifies and assesses the potential privacy impacts (perceived or otherwise) of the Treasury's proposals. The assessment is informed by:

(a) contextual references to relevant CDR Rules;

(b) the Australian Privacy Principles (**APPs**) set out in Schedule 1 to the *Privacy Act 1988* (Cth) (**Privacy Act**), where relevant and applicable to CDR stakeholders; and

(c) the CDR privacy safeguards in Part 7 of the CDR Rules.

How did we get here?

2.3 Mills Oakley was engaged by the Treasury in March 2023 to undertake a PIA in relation to the suite of proposals outlined in the following documents:

(a) *CDR Consent Review – CDR Rules and data standards* design paper (**CDR Consent Design Paper**); and

(b) *Operational Enhancements – Consumer Data Right Rules* design paper (**Operational Enhancements Design Paper**);

together, referred to as the ('**Design Papers**').

2.4 On 21 April 2023, Mills Oakley provided two [2] PIA Issue Papers that identified and discussed *potential* privacy impacts and risks in relation to the proposals outlined in the Design Papers. The intention of the Issues Papers was to share Mills Oakley's *preliminary* views about the privacy issues, risks and factors raised by each of the proposals canvassed in the Design Papers. The PIA Issue Papers were considered by Treasury in developing the Design Papers but were not published alongside these documents.

2.5 On 25 August 2023, the Treasury published the CDR Consent Design Paper and the Operational Enhancements Design Paper and undertook a public consultation exercise in relation to the proposals outlined in the Design Papers. The Treasury invited stakeholders to provide input about the change proposals with a view to informing the development of amendments to the CDR Rules concerning consent and operational enhancement measures.

2.6 The consultation period closed on 6 October 2023, with 49 stakeholders making written submissions to the Treasury on various issues canvassed in the Design Papers. The Treasury has, with the benefit of reviewing those submissions, revisited its proposals and, in some cases, further refined, clarified and changed its proposals to address feedback from stakeholders. In doing so it has balanced varied, and at times competing, considerations and firmed up its proposals for reform.

2.7 In addition to the information referred to above, Treasury has provided Mills Oakley with the following documents to inform this PIA:

(a) a summary of each of the proposed changes to the CDR Rules, flagging the iterative development and evolution of some proposals;

(b) preliminary and confidential versions of drafting instructions for proposed changes to the CDR Rules; and

(c) a synopsis of stakeholder submissions which draws out the privacy-related comments and feedback about the proposals outlined in the Design Papers. With the agreement of the Treasury, Mills Oakley's assessment has primarily leveraged the synopsis of stakeholder submissions and where relevant or necessary to obtain a deeper understanding of stakeholder views, we have then referred to the relevant submission, which has also been provided to us.

2.8 The scope of the PIA has been refined to reflect the proposals that the Treasury intends to progress to public consultation. Not all of the proposals set out in the Design Papers are being progressed at this time and there are some additional proposals.

2.9 Mills Oakley is instructed that this PIA report will be published along with a consultation draft of the proposed amendments to the CDR Rules as part of the public consultation process. The consultation process also includes the requirement for Treasury to consult with the Information Commissioner about the likely effect of new or amended rules on the privacy and confidentiality of consumers' information[2].

Our Methodology

2.10 The PIA has been undertaken having regard to the Office of the Australian Information Commissioner's (**OAIC**) *10 steps to undertaking a privacy impact assessment*[3] and industry PIA practices, modified and adapted to an iterative policy development and legislative reform project.

2.11 The PIA process has included:

(a) extensive consultation with the Treasury's policy advisers and analysts;

(b) preparation of two PIA Issue Papers which sets out Mills Oakley's preliminary observations, analysis and recommendations based on our review of the draft Design Papers;

(c) consideration of a synopsis of stakeholder submissions about the proposal outlined in the Design Papers and, where necessary for a deeper understanding of stakeholder views, reference to the submission;

(d) an assessment of each individual policy proposal, including whether the proposal has changed over the course of our engagement;

(e) contextual and high level assessment of each proposal by reference to:

(i) relevant parts of the CDR legislative framework including the CDR Rules, CDR Privacy Safeguards and OAIC's *CDR Privacy Safeguard Guidelines*[4];

(ii) the APPs (where relevant); and

(iii) the Department of the Attorney General's *Review of the Privacy Act Report*, 2022[5] (**Privacy Act Review Report**) and the Government response to the Privacy Act Review Report.[6]

(f) preparation of a draft and final PIA report (including recommendations).

2 See ss 56BQ and 56BR of the Competition and Consumer Act

3 See < https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/privacy-impact-assessments/10-steps-to-undertaking-a-privacy-impact-assessment >

4 https://www.oaic.gov.au/consumer-data-right/consumer-data-right-guidance-for-business/consumer-data-right-privacy-safeguard-guidelines.

5 www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf.

6 https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report

3 Privacy Impacts, Risks and Recommendations: Consent related amendments

Bundling of Consents

3.1 The bundling of consents is currently prohibited by the CDR Rules.[7] The Treasury is proposing a change to the CDR Rules to permit Accredited Data Recipients (**ADRs**) and CDR representatives to ask a consumer to give consent, *in a single action*, to:

(a) multiple CDR consents that address a combination of collection, use and disclosure of CDR consumer data; and

(b) the duration or longevity of the consent.

3.2 However, this measure is subject to the limitation that CDR and non-CDR consents must not be combined into a single consent flow.

3.3 Initially, Treasury proposed that bundled consents be permitted where 'reasonably needed for the provision of the requested service'.[8] With the benefit of feedback following public consultation on the Consent Design Paper, Treasury proposes that bundled consents be allowed where 'reasonably needed' to provide a CDR-related product or service.

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
Broadly, there was qualified support for bundling CDR consents. However stakeholders have indicated further detail or guidance is necessary about the meaning of 'reasonably required'. Stakeholder comments and feedback included: • combining CDR consents with non-CDR permissions in a single consent flow may confuse or mislead CDR consumers,	The Treasury intends to progress the proposal to amend the CDR Rules to permit, in certain circumstances, the bundling of consents. *Note: There will be corresponding changes to the consent provisions for CDR representatives.* Following stakeholder feedback, the Treasury has refined its proposal to *minimise* the potential privacy impacts identified by stakeholders by combining	r 1.8 r 4.10(1)(b)(ii) r 4.11(1) r 4.20E r 4.11(2) PS 3	Mills Oakley observes that shifting the CDR regime to a position that expressly permits (rather than expressly prohibits) the bundling of consents may be out of step with best practice and emerging trends in Australian and global privacy law. This may have the unintended consequence of undermining trust and confidence in the CDR regime, especially for those stakeholders actively managing their engagement with multiple privacy regimes, including the Privacy Act and the General Data Protection Regulation (**GDPR**).

7 *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth), r 4.10(1)(b)(ii).

8 The Australian Government, The Treasury, *CDR Consent Review – CDR rules and data standards design paper* (August 2023) page 8 section [1].

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
particularly in relation to the applicability of CDR protections. Additionally, it reduces or obfuscates transparency; • combining CDR and non-CDR consents within a single consent flow increases the risk of dark patterns being part of the consent experience. • bundling consent carries risks and, in some circumstances, has the potential to undermine the voluntary nature of consent. • disclosure consents should not be bundled, especially since disclosures may be made to trusted advisers and other unaccredited entities that are not subject to CDR privacy and security obligations and may also not be subject to the Privacy Act 1988 (Cth). Bundling of disclosure consents therefore poses an increased risk to CDR consumers. • the bundling of 'reasonably required' consents may erode a	CDR and non-CDR consents. The proposal to allow consent bundling will be limited to CDR consents. Bundling CDR and non-CDR consents will not be permitted. Treasury's proposal contemplates bundling a combination of various consent types (i.e. collection, use and disclosure) 'reasonably needed' to provide a product or service. The threshold or precondition of 'reasonably needed' is aligned with the data minimisation principle[9] which also uses this language. However bundling CDR and non-CDR consent will not be permitted. The period for which the consent is valid can also be combined into the single data flow, subject to the limitation on maximum periods for which consent can be requested[10]. The prohibition on combining consents in rule 4.10(1)(b)(ii) will be removed and the rules recalibrated to accommodate the limitations discussed above.		Mills Oakley agrees with stakeholder suggestions that there would be value in exploring how the breadth of phrases such as 'reasonably required' or 'reasonably needed' might be tightened. The inclusion of the word 'reasonably' may accommodate a greater range of consent bundling than, for example, a precondition, or threshold test, which permits consent bundling only where the consents are *'strictly essential'* to provide a product or service. Mills Oakley is of the view that a precondition grounded in the practical necessity and essential nature of the *combination* of collection, use and disclosure consents to successfully provide the product or service will mitigate many of the privacy impacts that have been identified by stakeholders. We acknowledge that the language proposed by the Treasury is purposely aligned with the data minimisation principle[11] to address, in part, the risk that consent bundling inadvertently broadens the scope of consent that consumers are asked to provide. While the ordinary meaning of 'reasonably needed' would tend to support the view that the consent sought must not merely be highly desirable, but must be required or essential, whether this phrase

9 Rule 1.8.
10 Rule 4.12.
11 See rule 1.8.

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
consumer's fundamental right to choose how their information is shared and limits a consumer's ability to control the way in which they engage with ADRs. This may result in consumers inadvertently sharing data or otherwise being pressured to share more data than is preferred or strictly necessary. • consent bundling is a significant deviation from the existing consent framework. Additionally, the Rich Authorisation Requests within FAPI 2.0 will facilitate purpose built consents and ultimately negate the need for consent bundling. • organisations ingesting CDR and non-CDR data to provide services may find it burdensome to maintain compliance with multiple privacy standards across various regimes. This may present competition barriers. Stakeholders suggested the following mitigation strategies: • Treasury clearly explain the distinction between 'reasonably required' and 'essential' noting the	Treasury has also indicated an intention to work with OIAC and the ACCC on additional guidance to support these amendments.		is sufficiently narrow to achieve the policy objective is ultimately a matter for the Treasury to explore with the drafters. ***Recommendation [1]:*** The Treasury consider whether 'reasonably needed' is sufficiently narrow to avoid function creep and the inadvertent expansion of consent requests. If the term will be interpreted narrowly and supports an inference that the consent request must be *essential* to provide the product or service, this could be addressed in guidelines that Treasury has indicated it intends to explore with OAIC and the ACCC.[12] Mills Oakley agrees that Treasury's proposal to exclude de-identification and direct marketing consents from bundling practices preserves a degree of consumer autonomy in respect of activities that tend to be of particular interest and concern to consumers. An additional way to manage the risk that consent bundling dilutes CDR consumers' autonomy over the management of their own CDR data is to *also exclude disclosure consents* from bundling. Disclosures tend to have a higher risk profile by virtue of the data being shared with additional participants in the data supply chain. The rationale for exploring this approach is that it is often the business practices and the architecture of data flows between parties to deliver a product or service

[12] See discussion at 3.3.

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
need to navigate two [2] different standards increases risk. Similarly, the phrase 'reasonably required' should be replaced with 'strictly necessary' which is a narrower test and would permit less bundling. • consider Privacy Act reforms to avoid potential re-work for the industry. Stakeholders observed that proposal 11 of the Attorney General's Privacy Act Review Report 2022 suggests amending the definition of 'consent' in a way that is likely to impact UX and design for many online services. • further consultation following implementation of FAPI 2.0 would be desirable.			(and over which CDR consumers have no control) that will render a disclosure consent 'reasonably needed' to provide a product or service in question. By quarantining disclosure consents from bundled consents, consumers will have better visibility about the number of stakeholders within a single data supply chain and the manner in which parties collaborate to deliver products and services. Consumers may want to select products and services that minimise the number of parties interacting with their data. The following recommendation complements existing requirements and proposals concerning transparency about data recipients. Mills Oakley appreciates that this approach will not necessarily streamline the consent process to the extent that has been proposed. However, preserving some degree of consent friction may be a compromise to ensure consent bundling practices do not move too far away from best practice and global trends. ***Recommendation [2]:*** Treasury consider whether excluding disclosure consents from consent bundling usefully reinforces transparency requirements about the parties with whom a CDR consumers' data is shared. ***Recommendation [3]***: As an alternative to Recommendation 2, Treasury consider a measure that gives CDR consumers the *right to object to bundled consents* which would trigger an obligation for the accredited person or ADR to explain the

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
			basis for the conclusion that the consents are essential to provide the product or service. A right to object, in this context, could conceivably be aligned with Privacy Act reforms, in the event a right to object to certain privacy practices is progressed by the Australian Government. Mills Oakley acknowledges this may be an extension of the kinds of information handling to which a right to object is presently associated. Treasury may wish to consider limiting a right to object (and the consequential obligation for an accredited person or ADR to explain the basis for the conclusion that the consent is reasonably needed to deliver the product and service) to certain types or combinations of consents. Mills Oakley has formed the view that relying on a consumer's ability to exercise choice and select other products/services that do not present consumers with bundled consents is likely to underestimate the degree to which bundle consents will be taken up by the market, and become standard practice, if allowed.

Pre-selection of consent options

3.4 Treasury is proposing a change to the prohibition on presenting consumers with pre-selected consent options, whether as separate or bundled consents.[13]

[13] The Australian Government, The Treasury, *CDR Consent Review – CDR rules and data standards design paper* (August 2023) page 12 section [2].

3.5 The Treasury's proposal would permit an accredited person or CDR representative, when seeking a consumer's consent, to present the precise combination of data types, uses, disclosures and consent durations considered reasonably necessary to provide the good or service that has been requested by the consumer.

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
The synopsis of stakeholder submissions suggests the benefits of a streamlined consumer experience (**CX**) is generally accepted but needs to be balanced against the dilution of consumer autonomy and active choice around how a consumers' CDR data is used, and by whom. The synopsis includes the following stakeholder views: • the proposal strikes a good balance, enabling more effective communication with the consumer (i.e. through the use of preselected data clusters, consent durations, and disclosures). • consumer privacy will be eroded, which could result in inadvertent sharing of non-necessary data. • pre-selection functionality and design options give the appearance	As noted above, the Treasury proposes a change to amend the CDR Rules[14] to remove the requirement for consents to involve an active selection requirement while preserving the requirement for there to be a clear indication of the consumer's agreement to the combination of consents that have been preselected for a particular product or service.	r 4.11(1) r 4.11(2) r 4.11(3)(g) r 4.12C(3) PS 3	In our view, a right to object (see ***Recommendation 3***) would mitigate the privacy risks and criticisms that have been levelled at pre-selection options. Generally speaking, pre-selected options and consents undermine consumer autonomy and choice.[15] If the pre-selected option cannot be overridden by the consumer, consistent with the approach that has been explored in the Privacy Act Review Report, an objection about pre-selected choices should trigger a more detailed explanation about why the pre-selected choice is necessary.[16] Noting Treasury's proposal to work with OAIC and the ACCC to progress guidelines about bundled consents, Mills Oakley suggests there is also guidance about whether consumers can override pre-selected consents. If a consumer 'toggles-off' a pre-selected consent (whether a bundled consent or an individual consent) it would be helpful for the consumer to be presented with an explanation about *why* the pre-selected consent is necessary in the circumstances.

14 *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth), r 4.11(1) and r 4.11(2).
15 See Privacy Act Review Report, page 103.
16 See Privacy Act Review Report, page 172-173.

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
of optionality but pushes consumers to endorse data sharing that may be contrary to their preferences. • may encourage practices being promoted as 'reasonably needed' for a product or service and therefore presented as a 'pre-selected' data flow. There were concerns that this may drive the development of 'premium' or 'add-on' services that would require additional data. • functionality and design for preselected options should allow consumers to 'unclick' essential data sets and only then be told the data is essential / required for the product or service. It was suggested this would promote a greater understanding and explanation of necessary data sets. • the data minimisation principle provides sufficient protection to ensure pre-selected options are not broader than they should be. • heavy visual cues are already needed to ensure consumers select options essential for the service.			***Recommendation [4]***: Assuming the pre-selection is limited to only what is necessary to deliver the goods or services and subject to ***recommendation 3***, Treasury consider whether guidelines and CX standards would be an appropriate vehicle to clarify whether a consumer can override a pre-selected option and the level of detail necessary to explain *why* a pre-selected option is necessary to deliver the product or service.

Providing information about the withdrawal of consent

3.6 The Treasury is proposing a change to the CDR Rules to amend the requirement that an Accredited Person must provide CDR consumers with instructions about how to withdraw consent, and the consequences of doing so, when asking a CDR consumer to give consent.

3.7 Rather than provide these details as part of the consent flow, the Treasury proposes that these details are made available to a consumer in a CDR receipt.[17] To simplify the consent flow (and the key messaging) it is proposed that all a CDR consumer needs to be told when asked to provide consent is that they may withdraw the consent at any time.

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
The synopsis of submissions indicates that stakeholders were broadly supportive of the proposal. The few stakeholders that either did not support the proposal, or expressed concerns, flagged the following issues: • withdrawing consent should be as simple as providing consent. • a clear disclosure about the impact of withdrawing consent should be a key element of the consent flow because it avoids misunderstandings about the consequences of withdrawing consent.	The Treasury intends to streamline the information that is provided to CDR consumers about withdrawing consent and the timing of that information in the UX. As indicated above, instructions about how the consent can be withdrawn[18] and a statement about the consequences (if any) to the CDR consumer if consent is withdrawn will be provided 'after the fact' rather than at the point consent is requested.[19] In addition to moving this consent messaging to CDR receipts, Treasury is exploring whether information could be captured as part of consumer dashboard functionality.	r 4.11(3)(g)(ii) and (iii) r 4.13 r 1.14(1)(c) r 7.5(3)	Mills Oakley has formed the view that the proposal balances the need for consent to be informed and not providing consumers with unnecessary or poorly timed additional information. Provided that CDR consumers' expectations are managed up-front and that a consent flow includes express notification to the consumer that they can withdraw consent at any time, the combination of the measures identified by the Treasury mitigates the privacy risks associated with resequencing *when* and *how* the additional details about withdrawing consent are provided. We are of the view that providing instructions about how consent can be withdrawn, and the consequences of doing so, can be sensibly presented as part of a CDR receipt. However, since receipts are issued after consent has been provided

17 The Australian Government, The Treasury, CDR Consent Review – CDR rules and data standards design paper (August 2023) page 14 section [3].
18 *Competition and Consumer (Consumer Data Right) 2020* (Cth), r 4.11(3)(g)(ii).
19 *Competition and Consumer (Consumer Data Right) 2020* (Cth), r 4.11(3)(g)(iii).

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
• consumers are generally more engaged during the on-boarding process, making it a better time to manage expectations about the management of consent. • engagement with instructions about how to withdraw consent and the consequence of doing so is likely to be low. Concerns were expressed that sequencing the provision of this information later in the consent flow is essentially hiding the information, disempowers consumers and may undermine confidence and trust in the CDR regime. • re-sequencing the provision of this information may inadvertently create a 'dark pattern' where the consequences of withdrawing consent are presented in a negative light and operate (or nudge behaviour) in a way that is analogous to a subscription trap.			by a consumer, Mills Oakley is of the view that a brief explanation about how consent can be withdrawn and the consequences of doing so should be readily available and discoverable by those consumers who want to refer to that information *before* providing or confirming their consent. In other words, the consent flow should permit a consumer to click through to that level of detail if they want it before giving consent. ***Recommendation [5]:*** Treasury consider whether guidance, such as in CX standards, might encourage an Accredited Person to tell consumers, as part of a consent flow, where to find further information about withdrawing consent.

Information about supporting parties

3.8 The Treasury is proposing a change to the CDR Rules to ensure that CDR consumers have visibility of supporting parties (of any description) who are permitted to access their CDR data. The transparency requirements for sponsor/affiliates, CDR representatives and outsourced service provider arrangements would be enhanced.

3.9 If a supporting party will not have access to a consumer's CDR data, they need not be listed.[20]

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
The synopsis of submissions indicates that stakeholders were generally supportive of this proposal. Transparency about the identity of supporting parties and when they will engage with consumer CDR data, and the positive impact this has on the quality of informed consent was a consistent theme. One stakeholder proposed an ancillary measure, namely, that ADRs should notify consumers of new supporting parties accessing the consumers' CDR data *after* the consumer has been advised of relevant third parties as part of the consent flow.	Treasury proposes a change to the CDR Rules to require information about any supporting parties (e.g. outsourced service providers, sponsors, CDR representatives) be provided to a CDR consumer when seeking the consumer's consent. The details provided will include: • supporting party name. • the supporting party's accreditation number and a link to their CDR policy. • the country where the supporting party is located. • a brief explanation about why the supporting party will access the consumer's CDR data.	r 4.11(3) r 4.20E(3)	Mills Oakley is of the view that to secure valid and informed consent, the consent flow that is presented to a CDR consumer should meet minimum information requirements about the supporting parties in the data supply chain. It is our understanding that the information provided to the consumer in the context of asking the consumer to provide consent effectively defines the scope of what they are consenting to. The stakeholder proposal to notify consumers about supporting parties engaged by an ADR or CDR representative after the consumer has provided consent is a privacy positive measure because it ensures ongoing transparency about the data supply chain. While the Treasury does not propose to progress this proposal at this time, Mills Oakley is instructed that it would not necessarily involve a new consent, but rather, could involve the consumer being notified and given the opportunity to withdraw the existing consent. If this proposal is progressed, we suggest whether consent can be implied in circumstances where the consumer does not withdraw their consent when notified of the additional supporting consent should be further assessed. This approach appears to conflate notice and consent.

20 The Australian Government, The Treasury, CDR Consent Review – CDR rules and data standards design paper (August 2023) page 16 section [4].

Information required in CDR receipts

3.10 The Treasury proposes a change to the CDR Rules that will streamline the requirements about the details to be included in CDR Receipts. The proposal is that CDR Receipts must comply with the data standards. Those standards will in turn set out the minimum information to be included in a receipt.

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
The Treasury proposes to simplify the regulatory approach to CDR-receipts by imposing a single obligation for CDR receipts to be issued in accordance with the data standards. A stakeholder expressed the view that third party details should be included in CDR receipts, while others were concerned the inclusion of additional details in receipts would mean SMS notifications would not be viable due to character limits.[21]	The Treasury intends to progress the proposal to amend the CDR Rules by imposing a single obligation for CDR receipts to be issued in accordance with the data standards. It is proposed that the standards will provide details about the information that must be included and how they are provided.	r 4.18 r 4.20O	Mills Oakley has formed the view that the proposed change is privacy neutral, on the basis that CDR Receipts *must comply* with the data standards and changes to the standards are ordinarily the subject of public consultation.

Consolidated requirements for dealing with redundant data and deletion by default

3.11 The Treasury is proposing a change to the CDR Rules to introduce a single consent mechanism by which a CDR consumer can agree to the de-identification of their CDR data. In the absence of a de-identification consent, the CDR data will be 'deleted by default' when it becomes redundant.

[21] Teleconference with our instructing officers on 23 April 2024. We were instructed by the Treasury of the views expressed by a stakeholder in respect of this reform.

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
N/A – Stakeholders did not comment on this proposal.	Currently, the CDR rules permit the de-identification of data where: • a consumer has given a de-identification consent (whether or not the data is redundant). • where an accredited person who has a policy or business practice of de-identifying redundant data, and has informed the CDR consumer about those practices, and the consumer has not elected to instead have their data deleted when it becomes redundant. The Treasury's proposal will simplify the management and protection of CDR data, all data would be deleted by default unless a consumer opts to have it de-ID'd, whether redundant or not.	r 4.11(1)(e) r 4.11(3)(h) r 4.13 r 4.15 – 4.17 r 4.18A(2)(b) r 4.20E (1)(f) r 4.20M r 4.20N	Mills Oakley is of the view this proposal is privacy positive. It preserves consumer autonomy over data and allows a consumer to tailor the end of life phase of the data lifecycle by choosing which treatment, i.e. deletion or de-identification, is applied to the data.

Consolidation of Notifications (CDR Receipts and 90 day notifications)

3.12 The Treasury is exploring a proposed change to the CDR Rules that would permit ADRs to consolidate 90-day notifications (i.e. multiple notifications consolidated into a single notification).[22] The Treasury will not be progressing amendments that would enable consumers to completely disable notifications. The proposed Rule change would move minimum information requirements to the data standards.

22 CDR Privacy Safeguard Guidelines, Chapter A, paragraphs [A.45] to [A.47]. The privacy protections that apply to data holders in the CDR context are; privacy safeguards [1], [10], [11] and [13] and APPs [1] – [9] and [11] – [12].

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
The synopsis of submissions indicates there is broad support for this proposal. Stakeholders expressed various views such as: • clarifying receipt rules and adjusting the timing of consent notifications is necessary. However, there was a variety of views about whether sensitive data should continue to be subject to a 90-day notification, while other stakeholders expressed a preference for consumers being able to opt-out entirely of notifications; • bespoke notifications may be preferrable in relation to harmful data, especially where a notification is not received due to an error (e.g. unsuccessful notification due to email delivery failures). • third party details should be included in CDR receipts, however, this may mean SMS notifications would not be viable due to character limits. • an ancillary measure, to notify consumers about OSP access, would provide greater transparency	The Treasury has noted the range of views provided through the stakeholder consultation process. Treasury does not propose to progress the proposal for consumers to tailor their notifications, however, will explore whether an amendment is necessary to permit 90 day notifications to be consolidated into a single consumer notification. The Treasury proposes minimum information requirements for notifications to be included in the data standard.	r 4.20(1)(b)(iii) r 4.20U(1)(b)(iv)	Mills Oakley has formed the view this proposal is privacy neutral, provided that the substance of the notifications is not diluted and consumers are nudged about the operative consents that they have in place. The regularity of notifications can be adjusted without a significant impact on consumer privacy, provided the minimum information requirements to be addressed in the notification are not reduced. Mills Oakley is cognisant that notification fatigue can undermine the effectiveness of notification steps intended to ensure consumers consider whether their consent settings remain fit for purpose.

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
to consumers about who had accessed their data.			

Withdrawal of de-identification & direct marketing consent

3.13 The Treasury was exploring whether a change to the CDR Rules was necessary to permit consumers to withdraw a de-identification or direct marketing consent without withdrawing all consents. The proposal is no longer being progressed on the basis that the Treasury is satisfied the Rules already permit withdrawal of these types of consent without withdrawing all operative consents.

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
Stakeholders were broadly supportive of this proposal and saw it as being privacy positive and aligned with the data minimisation principle. Stakeholders that did not support the proposed change expressed the view that the quality of services may be negatively impacted by selective withdrawal of de-identification and marketing consents.	The Treasury is exploring whether the CDR Rules need to be amended to facilitate consumers withdrawing de-identification or marketing consents only.	r 4.11 r 4.12 r 4.13	Mills Oakley appreciates that this policy position is the corollary of the proposal to quarantine de-identification and direct marketing consents from bundled consents. Because these consents cannot be bundled, they must be separately and specifically withdrawn. Mills Oakley considers this to be a privacy positive position. It gives CDR consumers autonomy over secondary uses of CDR data that, unlike consents for the collection, use and disclosure of CDR data for product and service purposes are transactional specific. Stakeholders that hold the view that de-identified CDR consumer data is an important resource to inform the development of improved products and services should advocate that position when

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
			seeking consumer consent for data to be de-identified rather than destroyed. In the absence of an active choice by the CDR consumer, the deletion by default approach promotes a privacy positive and secure end of data lifecycle process.

Direct marketing activities

3.14 The Treasury is proposing a change to the CDR Rules to ensure CDR consumers have visibility of the direct marketing activities to be conducted in reliance of a consumer direct marketing consent.

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
Nil. This proposal was not addressed in the Consent Design Paper.	Proposal for CDR consumers to have visibility of direct marketing activities that flow from direct marketing consent.	r 4.11.(3) r 4.20E r 7.5(3)	Mills Oakley has formed the view that this is a privacy positive proposal. For the direct marketing consent to be valid and informed, CDR consumers must have an awareness about the *types* of marketing activities to which the CDR data will be applied. Without that degree of awareness and specificity, the consumer response may not meet the legal requirements of valid and informed consent.

Dark patterns

3.15 Treasury is considering how best to prohibit the use of dark patterns in consent and authorisation process flows.

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
Stakeholders were generally supportive of the view that any directions about avoiding the use of dark patterns should be aligned with the Privacy Act reforms.	The Treasury will consider whether data standards or other guidelines are an appropriate vehicle to mitigate the privacy risks associated with the use of dark patterns in CDR consumer consent flows and authorisations.	r 8.11	Mills Oakley is of the view that how the CDR regime deals with dark patterns should be in lockstep with how the Privacy Act will respond to, and mitigate, the privacy risks associated with dark patterns designed to nudge or influence consumer behaviour and choice about the way their CDR data is handled. Treasury should minimise the risk of stakeholders and avoid duplicating effort, for instance, in relation to revisiting user experience designs and architecture patterns to meet CDR requirements and Privacy Act reforms about the use of dark patterns. The characterisation of what is and is not a dark pattern should be consistent across the regulatory regimes. ***Recommendation [6]**:* Treasury's regulatory response (if any) to mitigate the risk of dark patterns being used in CDR user experience design patterns and consent/authorisation architecture should be informed by the Privacy Act reforms on this issue. Mills Oakley anticipates that public awareness about dark patterns, and how design choices and patterns can nudge consumers to make privacy choices that have the practical effect of consumers inadvertently sharing more data than they mean to, is likely to be low. As such, educative materials would be valuable to explain how dark patterns might manifest themselves in a consumer's CDR user experience.

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
			Recommendation [7]: Treasury consider supporting any regulatory response or guidance material about avoiding dark patterns with visual examples of what is not permitted (i.e. an illustrative example of a dark pattern in a CDR context).

4 Privacy Impacts, Risks and Recommendations: Operational Enhancement Amendments

Secondary Users

4.1 The Treasury proposes to remove the requirement for data holders to offer a service that permits account holders to 'block' data sharing that has been authorised by a secondary user in relation to a particular accredited person. Treasury no longer intends to replace this obligation with a requirement that data holders instead offer a service that allows account holders to block data sharing on behalf of a secondary user in relation to a particular authorisation. The Treasury is satisfied that the existing requirement that requires data holders to provide an online functionality that permits an account holder to withdraw a secondary user's permission to give instructions is sufficient.

4.2 To address an anomaly in the operation of the Rules, the Treasury is proposing to clarify that where an account holder ceases to be eligible in respect of a particular account, that any secondary user instructions will cease to have effect.

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
Stakeholder views on the proposals set out in the design paper (particularly to introduce a requirement that data holders offer a service allowing account holders to block data sharing on behalf of a secondary user in relation to a particular authorisation) were mixed and canvassed the following issues: • a withdrawal of a secondary user authorisation by an account holder may remove the authorisation for accounts	The Treasury proposes to remove the requirement that data holders provide an online service that allows an account holder to block data sharing with a particular accredited person that has been authorised by a secondary user. It is not necessary to maintain this requirement since the account holder can simply withdraw the secondary user's authorisation. Treasury proposes a clarification to the Rules that would ensure secondary user instructions would lapse, in the event an account holder is no longer eligible to share CDR data.	APP 6[23] r 1.7 r 1.10(1)(b) r 1.15(5)(b)(ii) r 4.6A(a)(ii) r 4.28	Mills Oakley observes that under the CDR Rules, an account holder has a discretion to permit a secondary user to authorise data sharing in relation to an account (see rule 1.15(5)(b)(ii)). Relevantly, the account holder can withdraw that secondary user authorisation at any time (see rule 4.6A(a)(ii)). Given the practical effect of these rules, the proposals are privacy neutral. Removing the requirement to have an online functionality to block data sharing that has been authorised by the secondary user means data sharing decisions will continue to rest with the primary account holder. The clarification that is proposed for secondary user instructions to lapse, in the event the account holder is no longer eligible to share data, is also consistent with this approach.

[23] CDR Privacy Safeguard Guidelines, Chapter A, paragraphs [A.45] to [A.47]. The privacy protections that apply to data holders in the CDR context are; privacy safeguards [1], [10], [11] and [13] and APPs [1] – [9] and [11] – [12].

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
for which the account holder has no authority. • permitting an account holder to 'block' certain data sharing authorisations (rather than 'blocking' sharing with a particular accredited person) is potentially circular and ineffective. If the 'last in time' authorisation is the effective instruction, a secondary user whose instructions have been blocked by an account holder could simply re-authorise the sharing of data through a further (and refreshed) secondary user instruction. • an account holder may not fully understand the consequences of 'blocking' a particular instance of data sharing or may not successfully tailor the practical consequences of blocking the secondary users' authorisation. • account holders might usefully have the ability to control which of their accounts are the subject of a single			To permit a secondary user to make CDR data sharing decisions, contrary to the wishes of the primary account holder (or in the absence of an eligible account holder), would have an impact on the primary account holder's privacy.

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
authorisation given by a secondary user. • an 'opt-out' process for data sharing on behalf of secondary users might be useful, (provided the primary account holder has not withdrawn the secondary user instructions).			

Nominated Representatives

4.3 The Treasury put forward a number of proposals for changes to the CDR Rules in the Operational Enhancements Design Paper in relation to 'nominated representatives' including:[24]

(a) to require data holders to implement a quick, easy to use and to find process for appointing a nominated representative;

(b) to require data holders to provide an online mechanism for appointing nominated representatives;

(c) to deem account administrators for non-individual and partnership accounts to be the nominated representatives for the account (unless the non-individual or partnership consumer has expressly opted not to have the account administrator as the nominated representative, or the nomination has been revoked).

4.4 Additionally, the Treasury sought to address concerns about the transparency of authorisations given by nominated representatives and consents they have given to ADRs or CDR representatives. Stakeholders were invited to comment on the desirability of:

(a) requiring a data holder to identify, on the consumer's dashboard, the nominated representative that gave, amended or withdrew an authorisation;

(b) data holders using CDR consumer dashboards to inform or remind consumers that the dashboard does not capture consents given to ADRs or CDR representatives and that consents given may be active even after the relevant authorisation has expired and those consents must be managed through the relevant ADR dashboard(s).

24 The Australian Government, The Treasury, *Operational Enhancements – CDR Rules Design Paper* (August 2023) page 29 section [7].

4.5 The Treasury's proposal to change the CDR Rules has been refined and simplified, requiring data holders to provide CDR consumers with a simple and straight forward process to:

(a) appoint a nominated representative, which is prominently displayed to the CDR consumer; and

(b) allow an account administrator to be authorised as a nominated representative with a simple and straightforward online process.

(c) Noting the variety and complexity of the arrangements likely to be necessary to implement these processes, the Treasury proposes data holders have a 12 month deferred commencement period to implement the necessary digital functionality to achieve the above.

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
Some stakeholders expressed concern about the proposal, as it was outlined in the design paper, including: • automatically deeming account administrators of non-individual and partnership accounts as a nominated representative poses practical challenges for large organisations with multiple account administrators with bespoke access and authorisation permissions that are often tied to specific accounts.	The proposed has been refined, as explained above. The Treasury proposes that data holders provide CDR consumers with a process that is simple and straightforward to: • appoint a nominated representative and that it is prominently displayed to the CDR consumer; and • allow an account administrator to be authorised as nominated representatives, via a simple and straight forward online process. The Treasury proposes a 12 month deferred commencement or transitional period for the online functionality.	APP 3 APP 5[25] APP 6 r 1.13(1)(c) r 1.13(1)(d)	Mills Oakley observes that a deeming provision may undermine the value being placed, elsewhere, on requiring positive steps to authorise data sharing and selecting the appropriate person to give relevant instructions. As the deeming provision is no longer a proposal that the Treasury intends to put forward to change the CDR Rules, the privacy impacts of that approach do not need to be further considered. By contrast, a simple, straightforward process to permit CDR consumers to appoint nominated representatives (including by making an account administrator a nominated representative) support CDR consumers' effective engagement with their CDR rights. Noting that data holders would need to offer a simple and straight forward online process, Mills Oakley understands that data holders would each implement

25 The facility to nominate an account administrator as a nominated representative would need to include a collection statement that meets the requirements of APP 5. This is a design and implementation issue for the data holder in due course.

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
• potential misalignment with business consumers' *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* compliance strategies. • nominated representatives should *not* be identified on the consumer dashboard as this would create a new privacy risk. • the cadence at which data sharing can be suspended or ceased (where nominated representative approvals are amended or revoked) since access and sharing can be in next-to-real time. • lack of clarity around who has the authority to withdraw nominated representative authorisations (i.e. to override the deeming mechanism). Other stakeholders were *supportive* of the proposal on the basis that: • identifying nominated representatives on a consumer dashboard is crucial for			processes for appointing nominated representatives that meet their respective legislative obligations, risk posture and business needs. This kind of flexibility is a privacy positive because it enables data holders to leverage existing business and governance processes rather than a one-size-fits-all process being imposed that may require the collection and handling of data that is not needed, or suitable, for the data holder's operating environment. Mills Oakley observes the intention to have a civil penalty provision for non-compliance with the proposed obligation to have a simple and straight forward online process that is prominently displayed, illustrates the level of importance being placed on the ability to easily appoint a nominated representative.

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
traceability and creating an auditable activity log. • there are synergies between permissions given to account administrators and the permissions that fall to a CDR nominated representative.			

Accredited ADI to hold CDR data as a 'data holder'

4.6 In the Operational Enhancements Design Paper, the Treasury sought preliminary comments from stakeholders in respect of whether the circumstances in which an authorised deposit-taking institution (**ADI**) [26] or energy retailer[27] who has collected CDR data as an accredited data recipient (**ADR**) is permitted to handle the data as a data holder (rather than as an ADR) should be expanded. The consequence of this includes disapplying the CDR Privacy Safeguards to the CDR data, which means the data would then be regulated by the ADI's existing and business as usual privacy obligations (e.g. the APPs). In particular, the Treasury invited preliminary comments on whether ADIs should be permitted to hold data received under the CDR Rules *as a data holder* where they have received the data in relation to a CDR consumer who has *sought* (but has not necessarily acquired) a product from the ADI. The proposal has been refined following stakeholder feedback. It is now proposed the ADR can hold the data received under the CDR Rules as a data holder where the consumer has made an application to acquire a product from the ADR, or is in the process of doing so. The proposal is subject to a requirement that the CDR consumer is notified that the ADI will hold the data as a data holder, rather than as a usual ADR, prior to the consumer consenting to the ADI collecting the data. The ADI must also have explained to the CDR consumer the practical implications of that arrangement.

26 *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth), r 1.7. ADI is short for authorised deposit-taking institution, which has the meaning given by the *Banking Act 1959* (Cth).

27 *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth), Sch 4, r 1.4. For the purpose of provisions relevant to the energy sector, a data holder of the energy sector is a 'retailer' if: it retails electricity to connection points in the National Electricity Market; and it is either: the holder of a retailer authorisation issued under the National Energy Retail Law…in respect of the sale of electricity; or a retailer within the meaning of the *Electricity Industry Act 2000* (Vic).

4.7 This will expand the operation of the Rules since an ADI can presently handle CDR data received under the CDR Rules as a data holder only where the CDR consumer has *acquired* a product from the ADI and the CDR consumer has *agreed* to the ADI being a data holder, rather than an ADR, for the relevant CDR data.

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
The Treasury received submissions from ADIs indicating that the CDR rules are preventing them from using the CDR as a source of information about consumers seeking to apply for their products. ADIs have indicated that, ordinarily, they would retain information about consumers who have applied for, but not taken up, a product for the purposes of fraud control and other consumer analytics purposes. ADIs have also indicated they share information (including derived information) with external service providers, lawyers, consultants and auditors and this is stymied by the application of the Privacy Safeguards. Stakeholder feedback suggested that a consumer may provide their CDR data to multiple ADRs as a result of comparing products and testing the market on comparable products.	The Treasury proposes a change to the CDR Rules that will permit an ADI to hold data received under the CDR regime as a data holder, where a consumer has explored the ADI's products but not ultimately acquired a product from them. Consistent with current clause 7.2, the ADI will need to explain to the CDR consumer 1) that the CDR privacy safeguards which apply to ADRs would no longer apply in relation to that data and 2) the manner in which the ADI proposes to treat the relevant CDR data. The ability of the ADI to hold the data as a data holder, rather than as an ADR, will be subject to the consumer being informed of this intention prior to giving consent for the ADI to collect the data.	Sch 3, r 7.2(2)(b) Sch 3, r 7.2(2)(c)(ii) Sch 3, r 7.2(2)(d) S 56AJ (4) CCA APPS, particularly; APPs 1, 3, 6 and 7	We recognise that the Treasury is seeking to strike a balance between the protection of consumer data derived from the CDR regime and enabling an ADI to manage that data (in instances where the consumer has applied for a product or service from the ADI), consistently with its existing, APP compliant, information management practices. Although, under the proposed change, the CDR data would be subject to the APPs, the CDR Privacy Safeguards would continue to apply to the ADI when seeking the consumer's consent to collect the data, and at the time of collection. The following would also apply: • the ADI must reasonably believe the CDR data is relevant to providing the product to the CDR consumer; • the ADI must, when seeking consent from the consumer to collect their data under the CDR Rules (or before this consent is sought), explain to the CDR consumer: ○ the CDR Privacy Safeguards, to the extent that they apply to an ADR, will no longer apply to the person in relation to the relevant CDR data; and

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
Stakeholders suggested the proposal would introduce further complexity and fragmentation of the privacy settings under the CDR regulatory framework for regulated entities, consumers and regulators. If the CDR Rules were amended in the manner proposed, multiple ADIs would obtain a single consumer's CDR data in circumstances where the consumer is not necessarily a customer of the regulated entity. A stakeholder suggested that when a consumer is asked to consent to the ADI receiving the data as a data holder (rather than as an ADR), and told that the APPs (if applicable to the ADIs) would apply rather than the privacy safeguards, the practical impacts of that regulatory shift should be explained.			○ the manner in which the person proposes to treat the relevant CDR data. In circumstances where a consumer has made an application to acquire a product, or is in the process of doing so, the data can be used for a range of secondary purposes beyond the initial CDR-related product enquiry. However, those secondary uses are not unlimited and must meet the requirements of the APPs, where applicable. The ADI should explain the practical consequences of the data being governed by the APPs rather than the CDR Privacy Safeguards. The explanation, though high level, would need to provide sufficient context for the CDR consumer to consent (or not). The likely areas of difference that may be suitable to highlight to a CDR consumer include security, retention, deletion and correction. The explanation should be referrable to the ADI's information handling practices, as shaped by either the Privacy Safeguards or APPs. Stakeholders have referred to legitimate business purposes as the justification for why the CDR derived data should be available to the ADI to use (subject to the ordinary privacy protections applicable outside the CDR regime). Stakeholders have, for instance, referred to bona fide business needs to retain and use the CDR derived data as part of its records about credit decisions and as part of fraud management and mitigation strategies.

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
			Other stakeholders have suggested that the APPs may permit a range of secondary uses by an ADI, after the consumer has exercised their CDR rights and ultimately decided not to take up the ADI's product. This might be after the consumer has made an application to acquire a product or service. Consumers may be less inclined to exercise their CDR data rights if, as a result of exploring alternative and comparable products across the market via the CDR regime, there are unintended or unwelcome uses of the consumer CDR data. This would be contrary to the competition objectives of the CDR and is likely to make it less attractive to consumers if effort is required on their part to understand the practical ramifications of the data being governed by the APPs not the Privacy Safeguards. ***Recommendation [8]:*** Noting that the Treasury has narrowed the scope of the proposal such that the data in question has been obtained in connection with an application to acquire a product or service, Treasury may wish to consider whether the CDR consumer's decision (and autonomy over the CDR data) would be assisted by an explanation by the ADI about the *practical consequences* of consenting to the ADI holding the data as a data holder.

CDR Representative Principals

4.8 The CDR Rules do not expressly require that a CDR representative principal ensure that their CDR representative complies with the consumer experience data standards (**CX Standards**).

4.9 The Treasury proposes a change to the CDR Rules to address this and to expressly require a CDR representative principal to ensure their representatives comply with any 'consumer experience data standards' *as if they were an ADR*. It is proposed that a failure to comply with this obligation would have civil penalty consequences.

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
Not applicable. The proposal was not included in the Operational Enhancements Design Paper.	It is proposed that a CDR representative principal be required to ensure that their representatives comply with any consumer experience data standards as if they were an ADR. The amendment would reinforce through a civil penalty provision.	r 1.10AA r 1.16A(2)(a)	Consistent application and reinforcement of the CX Standards is a privacy positive step because it promotes trust, uniformity and predictability across the CDR regime.

Energy Rules - Deferral of data holder obligations for an ADR who becomes a small energy retailer

4.10 The Treasury proposes a change to the CDR Rules to defer the obligations of data holders set out in Part 4 of the CDR Rules. Accredited persons that become a small retailer[28] will have the benefit of a 12 month deferral of their obligations, and an 18 month deferral period for obligations concerning complex data requests. The intention is to provide those participants with sufficient time to build and operationalise their solution and business practices to comply with data holder obligations.

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
Not applicable. The proposal was not included in the Operational Enhancements Design Paper.	The Treasury is proposing a change to the CDR Rules to defer data holder obligations for an accredited person who transitions to become a small energy retailer. We are instructed that the reverse scenario - small retailers that become accredited persons - have the benefit of:	Sch 4, r 8.1 Sch 4, r 8.6(7) Sch 4, r 8.6(8) PS 11	Mills Oakley recognises that the Treasury is seeking to strike a balance between: • supporting new entrants to the cohort of small retailers operating in the energy market by providing a phased approach to the application of certain statutory obligations under the CDR regime; and

[28] (i.e. by obtaining authorisation from the AER or licence from the ESC (in Vic)).

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
	• a 12 month deferral of the application of Part 4 of the Rules which deal with data holders responding to consumer data requests made by an accredited person. • an 18 month deferral of obligations concerning the management of, and response to, complex data requests. The Treasury proposes to address an inconsistency in the application of deferred obligations by making this change.		• privacy protections for consumers and their CDR data. Treasury is specifically seeking to address the inequity created by the way in which the 12 and 18 month deferrals of certain CDR related obligations affect small energy retailers. Deferring the application of certain CDR requirements inevitably means privacy protections and associated compliance measures lack consistency across the small retailer cohort. Put another way, although all small retailers will have the benefit of the deferred application of certain CDR requirements when they transition to become a small retailer (as part of the phased approach to implementing the CDR regime), not all small retailers will be subject to the same suite of requirements at a single point in time. In our view, deferring the application of statutory protections and guarantees about actioning consumer data requests does not build trust and confidence in a maturing CDR regime. From a data protection perspective, consumer confidence and protection may be negatively impacted because a small retailer is in its first year of operation. Mills Oakley has formed the view that the consistent regulation of CDR stakeholders (i.e. all small energy retailers are treated the same way and are accountable by reference to the same obligations) can reasonably be expected to have privacy positive impact. Also, consumers are likely to be better positioned to:

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
			• make informed choices; and • compare products and retailers *if those retailers are expected to meet the same regulatory requirements*, no matter how long they have been operating in that capacity under the CDR regime. Allowing a 'like for like' comparison is, after all, one of the hallmarks of the CDR regime. Mills Oakley is cognisant that the deferral of certain obligations is *already* a feature of the CDR regime. However, from a privacy impact perspective, it is important to appreciate that the Treasury's proposal will effectively *expand the volume of consumers* whose interaction with the CDR regime will be complicated by: • which small retailer they are dealing with at any given time (i.e. whether the retailer is one that can, at a particular date, take advantage of the deferral of the obligations); and • the regulatory gap in terms of the time remaining before the small retailer must meet the statutory obligations referred to above. By addressing the apparent inequity of the application of statutory deferrals of certain obligations for small retailers, the Treasury will be increasing the number of consumers (up to 9,999 consumers *for each additional small retailer* that has the benefit of the delayed application of certain CDR Rules) whose end-to-end

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
			CDR dealings with a small retailer is not necessarily governed by the full suite of relevant CDR rules. Mills Oakley is not aware whether there is any modelling or forecasts about the number of small retailers (and by inference the number of consumers) whose privacy and data requests are impacted by the current deferral arrangements and the proposed extension of those deferrals. This makes it difficult to assess how the privacy and data access considerations are being balanced and weighted against the competition and market entry factors that we understand underscore the deferred application of certain obligations. Expanding the scope of the small retailer cohort that can leverage the deferral arrangements risks retailers entering the market before they have the procedures and technical capabilities to manage the full suite of obligations under the CDR Rules. One stakeholder has suggested this might create a risk of systemic non-compliance with PS 11. [29] The Treasury has indicated the regulatory approvals and licences that need to be in place for a small retailer to enter the market is likely to mean the impact on consumers is low (i.e. in terms of the number of affected consumers), and temporary, since it can often take months/years to acquire consumers and offer energy products and services.

29 Office of the Australian Information Commissioner, Consumer Data Right Privacy Safeguard Guidelines, page 3, Chapter 11, paragraph [11.6].

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
			Recommendation [9]: Treasury consider the feasibility of a regulatory and enforcement strategy that is calibrated to support small retailers meet their CDR obligations rather than defer the application of those obligations.

Products for the energy sector

4.11 Treasury proposes a change to the CDR Rules to insert an energy sector-specific definition of 'trial products'. We understand that the intention is to mirror the amendments made by the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2023* that inserted a bank sector-specific definition of trial products. The proposed change is about *exempting* trial products in the energy sector from the CDR Rules. The intention is that energy data holders would not need to meet CDR data obligations for these trial products. Stakeholder feedback obtained by the Treasury on the 2023 Rules indicated there was support for extending these amendments to the energy sector.

4.12 The Treasury proposes the definition of 'trial products' is tied to a trial or pilot period of no more than 12 months. Treasury will also explore with the drafters whether 'trial plans' is more appropriate language for the energy sector than, trial products'.

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
The synopsis of submissions indicates that stakeholders were broadly *supportive* of treating 'trial products' in the energy sector in the same way trial products are dealt with in the CDR Rules for the banking sector.	The Treasury proposes a change to the CDR Rules to insert an energy sector-specific definition of 'trial products'[30] to exclude data in relation to those products from the CDR Rules.	Sch 4, r 1.2 APPs (1– 9 and 12) PS 11 and 13	Mills Oakley has formed the view that the privacy impacts of excluding CDR data for trial plans can be effectively managed through pilot-specific privacy notices under APP 5 and obtaining express customer consent to participate in a trial plan (i.e. setting up a consent or authorisation for the collection, use and disclosure of CDR data that is also personal information

30 The Australian Government, The Treasury, *Operational Enhancements – CDR Rules Design Paper* (August 2023) page 17 section [8]. The proposal would seek to replicate the approach taken to authorise CDR data to be shared in connection with trial products in the banking section – see *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2023*, subclause 145.

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
Some stakeholders were supportive of the policy proposal but suggested alternative ways in which to characterise or define a trial. These are technical and industry specific measures but have a privacy impact since they will ultimately define the scope that consumers have chosen trial products.	It is proposed that a trial product is one that is supplied for no longer than a 12 month period.		for the purpose of the trial and that, if it were not for this proposal, would be CDR data). Mills Oakley has considered whether the combined and sequential operation of the proposal regarding the deferred application of certain CDR requirements (see above), together with this proposal to exclude data in connection with trial plans from the CDR regime, may have unintended privacy impacts on consumers. Small retailers might reasonably be expected to be market disruptors and explore a series of innovative plans to secure a customer base. This would effectively mean consumers do not get the benefit of the full suite of CDR-related rights and protections if they elect to stay with the small retailer. ***Recommendation [10]:*** Treasury consider the combined and sequential operation of: • the deferred application of CDR Rules for certain cohorts; and • the exemption for trial products/plans; on an individual customer whose CDR experience is that their CDR data is not protected by the full suite of CDR rights and protections. One way in which this risk might be avoided is to ensure that a small energy retailer cannot offer only trial plans. In other words, the business model cannot seek to avoid the rights and protections afforded to consumers under the CDR Rules by only offering trial plans.

Extending obligation dates for small retailers who become larger retailers

4.13 The Treasury is proposing a rule change to allow small retailers who become larger retailers an additional six months to prepare for their complex data request sharing obligations. This will align data sharing obligations for these new larger retailers with the complex data request sharing obligations applicable to initial retailers and original larger retailers.

Synopsis of stakeholders' privacy comments and submissions	Proposed amendments	Relevant CDR legislative framework	Privacy impacts, risks and recommendations
Not applicable. This proposal was not included in the Operational Enhancements Design Paper.	The Treasury is proposing a rule change to give small retailers who become larger retailers[31] an additional six-months to prepare for their complex data request sharing obligations. The proposal is intended to address an inconsistency in the deferred application of obligations to respond to complex data sharing requests across this cohort of stakeholders. Currently, a small retailer that becomes a larger retailer has less time to comply with the complex data sharing obligations (i.e. 12 months) than a small retailer that becomes an accredited person (18 months). The proposal is intended to standardise the deferral period to facilitate consistent support for the retailer's preparedness.	Sch 4, r 8.3 Sch 4, r 8.6(6) Sch 4, r 8.6(8)	In addition to the comments above in relation to the proposal concerning deferred application of CDR obligations from small retailers, we note the following. As the CDR regime matures, it is conceivable that consumers see diminishing justification to defer the application of CDR obligations, particularly for CDR participants transitioning from a small to a large retailer and therefore acquainted with the CDR regime. However, Mills Oakley acknowledges that this phased implementation of certain CDR requirements is an existing feature of the CDR regime.

31 *Competition and Consumer (Consumer Data Right) Rules 2022* (Cth), r 8.3. A 'large energy retailer' is a retailer that had 10,000 or more small customer on the amendment day is a large retailer; and a retailer that had 10,000 or more small customers at all time during a financial year that begins on or after the amendment say is also a large retailer on and from the day 12 months after the end of that financial year.

Annexure A Glossary

Term / Abbreviation	Meaning / Description
ADI	Authorised deposit-taking institution
Accredited Data Recipient (ADR)	A provider, who has been accredited by the ACCC to receive consumer data to provide a product or service under the CDR. See section 56AK of the CCA.
Accredited Person (AP)	A person granted accreditation by the Data Recipient Accreditor (i.e. the ACCC). See subsection 56CA(1) of the CCA.
ACCC	The Australian Competition and Consumer Commission, an independent Commonwealth statutory authority, who is a co-regulator of the CDR regime along with OAIC.
Australian Privacy Principles (APP)	The Australian Privacy Principles, which are principles-based laws that apply to any organisation or agency the *Privacy Act 1988* covers. See Schedule 1 of the Privacy Act 1988.
CCA (or 'the Act')	The *Competition and Consumer Act 2010* (Cth).
CDR consumer	A person who has the right to access the CDR data held by a data holder and direct that the CDR data be disclosed to an accredited person. See subsection 56AI(3) of the CCA.
CDR data	Data that has been 'wholly or partly' derived from the data set out in the designated instrument, and data derived from any previous data. See subsection 56AI(1) of the CCA.
CDR Participant	A data holder or an accredited data recipient of CDR data. See subsection 56AL(1) of the CCA.
CDR Principal	A person who has been granted unrestricted accreditation and has engaged a CDR Representative under an agreement that complies with the CDR Rules.
CDR Privacy Safeguards	Defence mechanisms used by the CDR designed to keep data secure and protect privacy of individuals, placing 13 strict obligations on businesses collecting and handling data. See Division 5 of Part IVD of the CCA.
CDR Representative	A person who is not accredited that has been engaged by a CDR principal under an agreement that complies with the CDR Rules.
CDR Rules	The *Competition and Consumer (Consumer Data Rights) Rules 2020* (Cth) as in force on 10 February 2022.
Consent Design Paper	The *CDR Consent Review: CDR rules and data standards design paper* drafted by Treasury.
Consumer Dashboard	In relation to an accredited person, an online service that can be used by CDR consumers to manage consumer data requests and associated consents they have given to the accredited person. In relation to a data holder, an online service that can be used by each CDR consumer to manage authorisations to disclose CDR data in response to consumer data requests.

Term / Abbreviation	Meaning / Description
Consumer Experience Standards (CX Standards)	Data standards regarding the obtaining/withdrawal of authorisations and consents, the collection and use of CDR data, authentication of CDR consumers etc.
Data Holder	A business that holds consumer data and must transfer the data to an accredited data recipient at the consumer's requests. See section 56AJ of the CCA.
Data Minimisation Principle	Principles that limit the scope and amount of CDR data an accredited person may collect and use. See CDR Rules (r 1.8).
Design Papers	The below documents together are referred to as the Design Papers: • CDR Consent Review – CDR Rules and data standards design paper (CDR Consent Design Paper); and • Operational Enhancements – Consumer Data Right Rules design paper (Operational Enhancements Design Paper).
OAIC	The Office of the Australian Information Commissioner who is a co-regulator of the CDR regime along with the ACCC.
Outsourced Service Provider (OSP)	A person or corporation to whom an accredited person may disclose CDR data under a CDR outsourcing arrangement.
Personal Information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable: • Whether the information or opinion is true or not; and • Whether the information or opinion is recorded in a material form or not.
Secondary User	A person who is nominated by an account holder to authorise data sharing from their account.
Secondary User Instruction	Instructions made by the account holder for the data holder to treat a person as a secondary user for the purposes of the CDR Rules.