9 September 2024

Treasury
Langton Cres
Parkes ACT 2600
by email: CDRRules@treasury.gov.au
cc: michael.palmyre@consumerdatastandards.gov.au and
amy.nussbaumer@consumerdatastandards.gov.au

CDR rules: consent and operational enhancement amendments - Consultation paper and Decision Proposal 350

Thank you for the opportunity to comment on Treasury's consultation on Consumer Data Right (**CDR**) Rules: consent and operational enhancement amendments consultation and the Data Standards Body Decision Proposal 350: August 2024 Rules and Standards Impacts paper. This submission has been drafted by the Financial Rights Legal Centre (**Financial Rights**) with input and support from the Consumer Policy Research Centre (**CPRC**) and Financial Counselling Australia (**FCA**).

This submission will provide comment on the series of proposals for amendments to the rules, and provide comment on the standards' changes, where relevant or needed.

Key points

While jurisdictions around the world are introducing strong, pro-consumer privacy measures to unbundle consent and prohibit pre-selection at the point of consent, several of the enhancements suggested in this proposal are contrary to this trend and will only exacerbate existing flaws in the CDR regime and poor privacy protections that Australians currently endure within the digital economy.

CDR as it stands and based on some of the proposals within this consultation is creating a situation where it disproportionately places on individuals the burden of their own safety online.

In addition to considering compliance costs of industry to meet stronger regulations, the Treasury must also consider the cost impost on individuals being placed with the additional mental load of navigating their privacy protections in a complex environment.

We recommend that the Government does not proceed with the first two proposals with respect to the bundling of consents and pre-selection of data. In the event these two proposals move forward they must be amended by:

- establishing an objective standard with respect to when bundling and pre-selection can occur;
- resourcing the monitoring and enforcement of these rules needs to be appropriately boosted to ensure compliance;
- removing disclosure consents from the bundling proposal;
- introducing a right to object to bundling;
- enabling the ability to toggle off pre-selections;
- enabling the ability for a consumer to notify a data holder (**DH**) of their extra needs and experience of vulnerability within the consent process; and
- establishing a duty of care or best-interests duty to ensure data is collected, shared and used in a way that does not leave consumers worse-off.

Furthermore, this submission recommends that:

- with respect to **proposal 1.3,** Accredited Persons should be required to provide a link to further information about withdrawing and consequences of withdrawing that consent at the point the consent is being requested, if the CDR consumer so chooses to find more information;
- with respect to **proposals 1.4** and **1.6**, all proposed "SHOULD" and "MAY" standards be "MUST" standards
- with respect to **proposal 1.7**, the option to retain de-identification of data should be removed altogether
- before proceeding with **proposal 2.2** regarding expanding the circumstances in which accredited ADIs can hold CDR data as a data holder, that the Government examine ways to build the appropriate protections and frameworks in the use of CDR data for non-CDR purposes; and
- the government introduce a principle-based prohibition of the use of **dark patterns** with a clear taxonomy in the rules themselves, with the practical application of this prohibition addressed in the standards.

Approach to the Privacy Impact Assessment

We do not believe that Treasury are meeting best practice privacy impact assessment (**PIA**) processes to better inform the development of the CDR regime.

It is not clear whether the independent assessor was provided the ability to undertake stakeholder engagement outside of being provided a synopsis of submissions on the rule changes. Consumer groups were definitely not provided with an opportunity to speak with the independent assessor to discuss any potential privacy implications of the proposed rules. Direct stakeholder engagement has taken place in previous privacy impact assessment processes.

To be clear we are not criticising the quality of the work Mills Oakley undertook in producing the Privacy Impact Assessment, which has delivered very reasonable recommendations to further mitigate against legitimate risks identified. Our issue centres on the PIA process established by Treasury and the lack of ability for consumer groups to directly engage with the assessor, provide significant input into their considerations and have their recommendations genuinely impact upon the development of the CDR early enough to ensure that it is embedding a privacy-by-design and privacy-by-default approach in a meaningful way.

1. Consent Review

1.1. Allowing a data recipient to bundle CDR consents, so that consumers can give multiple consents with a single action.

We do not support the proposed rule change to allow a data recipient to bundle CDR consent. The proposal:

- is out of step with global and national best practice
- embeds a dark pattern into the CDR that undermines consumer choice, autonomy and confidence in the CDR, and
- even with the risk mitigants proposed, will not address the problems with bundling consent.

Bundling is out of step with global and national best practice

The proposal to introduce the ability to bundle CDR consents is fundamentally out of step with global and Australian best practice data consent practices and will undermine consumer confidence in the CDR.

Guidance from the European Data Protection Board in relation to the GDPR's requirement notes that voluntary, freely given consent implies '*real choice and control*' for individuals, and that if '*consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given*'.[1]

It is also out of step with best practice Australian consent practices. The OAIC advises consumers the following:

Avoid giving bundled consent unless the request:

- gives you the choice not to consent to one or more proposed collections, uses and/or disclosures of your personal information

- gives you enough information about each proposed collection, use and/or disclosure

[1] European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 (4 May 2020)

- tells you the consequences, if any, of not consenting to one or more of the proposed collections, uses and/or disclosures of your personal information.[2]

The Information and Privacy Commission (NSW) provides advice that:

By bundling consents … , digital platforms are not giving individuals the opportunity to choose which collections, uses and disclosures they agree to and which they do not[3]

The proposal is also contrary to the intentions behind the introduction of open banking in the first place. The Farrell Report states that:

This Review considers that the use of implied and bundled consent for the data provided through Open Banking could undermine the key elements of customer control, namely that: the consent is not informed; voluntarily given; current and specific; and that the individual has the capacity to understand and communicate their consent.[4]

The proposal embeds a dark pattern into the CDR undermining consumer choice, autonomy and confidence

Treasury's Data Standards Body Chair commissioned research into deceptive patterns by the Uni of SA[5] endorses the definition of deceptive patterns used by the EU:

Deceptive patterns on online interfaces of online platforms are practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions. Those practices can be used to persuade the recipients of the service to engage in unwanted behaviours or into undesired decisions which have negative consequences for them.[6]

This research explicitly references the bundling of consents in its Deceptive Patterns Typology and defines it as:

[2] OAIC, Consent to the handling of personal information
[3] IPC, Consent Fact Sheet
[4] Treasury, Open Banking customers, choice convenience confidence, December 2017.
[5] Australian Research Centre for Interactive and Virtual Environments, University of South Australia, Patterns in the Dark, Deceptive Practices in online interactions
[6] (2022) Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive, 2000/31/EC (Digital Services Act)

The user is automatically marked as consenting to multiple settings when consenting to only a single setting.

It then explains the issues with bundled consent being "*free choice repression*", "*undesirable imposition*" and "*forced acceptance*".[7]

Consumers in the digital space currently face serious privacy and security issues arising from the fact that that they do not engage with the use of consents and take part in a tick and flick process. Allowing the bundling of consent embeds this lack of engagement and places the purported problem of "consent fatigue" over the issue of "free choice repression."

This would be less of an issue if consumers could genuinely trust that their best interests are being prioritised and looked after but this is not the case, as outlined below.

The risk mitigants proposed will not address the problems with bundling consent

The only risk mitigant put forward by the Government to limit the impact of bundling consents is that the bundling of collection, use and/or disclosure consents only be allowed where they are "reasonably needed" for the provision of the requested good or service, and linking this to the data minimisation principle (**DMP**) at Rule 1.8.

There are several problems with this approach.

First "reasonably needed" is a subjective test that is in the eye of the beholder – in this case the data recipient who, in most cases, will have a financial interest in obtaining consent to the collection and use of as much data as possible. What may be "reasonable" to them will likely be very different to what is "reasonable" to the consumer who has an interest in ensuring that their personal data sharing is kept to a minimum to lower the risk of breaches and subsequent scamming and fraud risks.

This issue is not ameliorated by Treasury's proposal to link the concept to the DMP since it is similarly a subjective test using the same "reasonable" standard.

There is also little if any oversight, monitoring or enforcement in place currently, and no additional monitoring proposed, to ensure that when a data recipient asserts that collection is "reasonably needed" it is in fact needed. Under the proposal, it is likely that these will only

[7] Kerstin Bongard-Blanchy, Arianna Rossi, Salvador Rivas, Sophie Doublet, Vincent Koenig, and Gabriele Lenzini. 2021. "I am Definitely Manipulated, Even When I am Aware of it. It's Ridiculous!" - Dark Patterns from the End-User Perspective. In *Designing Interactive Systems Conference 2021 (DIS '21), June 28– July 2, 2021, Virtual Event, USA.* ACM, New York, NY, USA 14 Pages. https://doi.org/10.1145/3461778.3462086

be looked at if, and more likely when, something goes wrong, and a consumer is harmed and complains. This is not a foundation upon which trust and confidence is built.

Cost to consumers through increased risk, decreased trust and loss of autonomy

If CDR is to maintain any integrity with the public, and genuinely place the consumer at the heart of the regime, the costs of consumer harms arising out of the introduction of a dark pattern such as bundling into the regime must outweigh any cost to business. Measuring the cost of the loss of consumer autonomy, choice and willingness is fundamentally a more difficult quantifiable exercise to that of measuring the costs to business to add a little more friction. Consumer groups are also not in the position, nor have the resources to engage consultant economic modellers to quantify the expected costs to consumers.

However, we do know that consumers have experienced harm arising out of deceptive patterns. In Australia, 83% of consumers have experienced negative consequences as a result of dark patterns.[8] We are also aware that given the preponderance of deceptive patterns and scams, consumers are more wary of sharing their data and do not hold confidence in the current data holding regimes. CPRC's consumer research in 2023 found that only 7% of Australians feel companies give them real choices to protect their privacy online. It also found that only 15% of Australians feel businesses are doing enough to protect their privacy.[9]

This has been confirmed in the ongoing FCA pilot project into using the CDR in the development of statements of position. This project has so far found that only 1 in 5 clients are willing to consent to use open banking. The key barriers for clients noted are concerns around privacy, data safety and scams.

The Government must consider the potential costs arising from:

- the harms that will take place when consumers agree to a bundled consent including use cases that they did not expect or want;
- the loss of confidence in a regime that is meant to be the gold standard in terms of data handling safety and security.

In the event the proposal moves forward it must be amended to become an objective standard

If this bundling proposal is to go ahead against the objection of consumer groups, a more objective standard is at the very least warranted. We support the proposal expressed in the

[8] CPRC, Duped by Design, Manipulative Online design: Dark Patterns in Australia, June 2022
[9] CPRC, Not a Fair Trade. Consumer Views on how Businesses use their Data March 2023

PIA to only permit bundling where the consents are "strictly essential" to provide the product or service.[10] At a minimum the word "reasonably" should be removed here to at the very least shift the subjective standard to a more objective standard, one that is more in line with the approach taken in Europe regarding consent.

Resource and monitor compliance with the rules

Further, if this proposal is to go ahead the regulators of the CDR – both the OAIC and ACCC should be explicitly empowered and resourced to monitor the assertions at the heart of this proposal and ensure compliance with the rules.

Remove disclosure consents from the proposal

If this proposal is to go ahead, disclosure consents must also be excluded from the ability to bundle.

We agree with the position expressed in the PIA that an additional way to manage the risks associated with the dilution of consumer autonomy over their own data is to also exclude disclosure consents – especially those regarding disclosure to third parties including Trusted Advisors under 1.10A and insight.[11] These disclosures should also have clear definitions of what each of the parties does. This would at the very least remove some of the key risks and enhance transparency.

If the proposal were to be amended in this way, consumers would have a greater ability to understand and consent to all the different types of disclosure, providing them with the explicit information they need and the choice where relevant.

Alternatively, a right to object to bundled consent, should be introduced.

Introduce a right to object to bundling

In line with the views expressed in the PIA, consumer groups support providing CDR consumers with 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.

---

[10] Page 8, Mills Oakley, 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

[11] Rule 1.10A(1)(a), (b) and (c), Competition and Consumer (Consumer Data Right) Rules 2020

A right to object would be both in line with the GPDR and the recommendation 18.2 of the *Privacy Act Review* Final Report.

Introduce a duty of care

Finally, there is a critical need for the CDR framework to introduce a broader duty of care or a best-interests duty to ensure data is being used in way that does not leave consumers worse-off. The Federal Government should introduce more positive obligations on businesses in the collection, sharing and use of consumer data.[12]

CPRC research has confirmed that 84% of Australians agree that companies should act in the best interests of a consumer when using their data.[13] To ensure the effective implementation and uptake of CDR, the Federal Government must create an environment that meets consumer expectations and adequately holds businesses accountable. Without this, consumers will have little trust that the regime will genuinely work for their interests over the interests of for-profit participants in the CDR regime.

1.2. Allowing a data recipient to pre-select the elements of an individual consent that would be reasonably necessary for the data recipient to provide the good or service

Consumer groups do not support the proposed rule change to allow a data recipient to pre-select the elements of an individual consent that would be reasonably necessary.

As with bundling, pre-selection:

- is out of step with global and national best practice;
- embeds a dark pattern into the CDR that undermines consumer choice, autonomy and confidence in the CDR; and
- even with the risk mitigants proposed, will not address the problems with bundling consent.

Embedding pre-selection is a backward step

Under Article 7 of the GPDR, consent must include a clear affirmative act. The European Data Protection Board (**EDPB**) requires that consent must be provided through a 'positive action' that is, the user must do *something* to indicate their consent, rather than silence and passivity. Consequently within the EU, pre-ticked or pre-selected options have been deemed

[12] CPRC, *In whose interest – Why businesses need to keep consumers safe and treat their data with care*, 2023.
[13] CPRC, *Not a fair trade – Consumer views on how businesses use their data*, 202.3

as an invalid way to obtain consent from individuals. This current proposal runs counter to this best practice standard.

The Privacy Act review has also recommended that:

Recommendation 11.4: Online privacy settings should reflect the privacy by default framework of the Act.[14]

Australia should be embedding good practices that have already been implemented in other jurisdictions, instead of placing Australian consumers in situations where they are less protected and have less agency over their data sharing choices.

The proposal embeds a dark pattern into the CDR undermining consumer choice, autonomy and confidence

Pre-selected options and consents undermine consumer autonomy and choice – recognised by the recent Privacy Act Review.

Pre-selection (also known as default sharing or bad defaults) are identified as deceptive patterns in the recent Uni of SA report to the Data Standards Chair.[15] Pre-selection or "default settings" involve making one option the standard or default option, whereby encouraging the sharing of information and either requiring active intervention to switch to another option – for example, by pre-ticking certain boxes, or not even providing the option at all, which seems to be case with the current proposal.

Pre-selection can open UX design to integrate dark patterns such as false hierarchy and data-grab to steer consumer choices that may not be in the best interest of the consumer.[16]

CPRC's consumer research continues to confirm that Australians are not comfortable with providing businesses with more data than necessary with 64% finding it unfair when companies require them to supply more personal information than is necessary to deliver the product or service.

CPRC's most recent research into the cost of managing privacy found that it would take Australians an average of 30 minutes to adjust privacy settings for digital services used in just a single day. The research confirms that what's needed is privacy protections that utilise an opt-in approach to data sharing as opposed to an opt-out model through pre-ticked

[14] Page 109, Attorney General's Department Privacy Act Review Final Report
[15] Australian Research Centre for Interactive and Virtual Environments, University of South Australia, Patterns in the Dark, Deceptive Practices in online interactions
[16] CPRC, Duped by Design, Manipulative Online design: Dark Patterns in Australia, June 2022

selections that takes away choice and control away from Australians, the exact opposite of CDR's objective.

The risk mitigants proposed will not address the problems with pre-selection and there will be little to no monitoring and enforcement

"Reasonably necessary" to function falls into the same subjective traps described above. As with oversight of future bundling of consent practices, there will be little to no enforcement or monitoring of compliance with data recipient practices with respect to pre-selection.

Indeed, on this point we understand that Treasury and the DSB have been made aware that there are data recipients who currently do pre-select elements of consumer consent against the spirit and letter of the rules. Instead of enforcing the rules, no enforcement action has taken place to ensure that that the CDR participants doing this are compliant with current laws.

With a continued limited capacity for regulators to enforce and unclear guidelines for businesses, the onus will unfairly remain on the individual to manage their data.

In the event the proposal moves forward it must be amended to become an objective standard

Rather than "reasonably necessary," the proposal should be amended to meet an objective "strictly essential" standard, or at the very least "necessary" standard.

Introduce a right to object

In line with the recommendation of the PIA - 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.

Require a toggle-off standard

Consumers should be able to untick "essential" boxes to be alerted to their essential nature i.e. 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.

Introduce a requirement to allow consumer to notify a DH of their extra needs and experience of vulnerability

The Consent UI needs to allow for a consumer to notify their institutions of their vulnerability so that their CDR request can be handled appropriately. Currently this can only be done by contacting the bank separately. For example, the consent should include words to the effect "If you are in need of extra support and are concerned about data sharing because it may result in physical or financial harm, or you wish to prevent data sharing from ever happening on your accounts, please contact and alert your institution here."

Resource and monitor compliance with the rules

Both the OAIC and ACCC should be explicitly empowered and resourced to monitor the assertions made under these proposed new pre-selection rules and ensure compliance with the rules.

Finally, as with the above, a duty of care or best-interests duty is required to ensure that consumer can have trust that their interests will be prioritised.

1.3. Simplifying the information a data recipient is required to provide to the consumer at the time of consent

While we are not necessarily opposed to simplifying information being provided to consumers for comprehension purposes, we do not want the Government to take away the *ability* for a consumer to seek out more information on how to withdraw their consent and the consequences of dong so *before* they consent to the collection and use of their data.

The current proposal forces the consumer to have to consent first and only then read the information later – information that may (or may not) have swayed their views in consenting in first place.

In our view it does not have to be a binary choice between only providing information before or after consent.

A middle ground is clear: require an Accredited Person to provide a link for further information about withdrawing and consequences of withdrawing that consent at the point the consent is being requested, if the CDR consumer so chooses to find more information. In this way the consent process is not necessarily overwhelming for consumers at the point consent is requested – but also serves those who do need further information to reassure themselves and make a fully informed choice.

This would ensure that everyone is provided with the right amount of information they wish to engage with both before and after consent.

Providing a link to a page that details straightforward information about withdrawing consent would in no way be a burden to an Accredited Party, nor involve any costs.

This would also mean making amendments to the proposed standards to ensure that the information that must be provided by a data recipient in a CDR receipt[17] (or alternatively the list of information provided in the original design paper, see 1.5 below) should also be provided via a link at the point of consent.

1.4. Allowing a data recipient to consolidate the delivery of 90-day notifications to reduce consumer notification fatigue

As with the bundling proposal above – consideration must be given to balancing the risks of bundling up all the information in one notice, and the information being ignored through complexity and length, versus providing too many notifications and they being ignored.

In the situation seeking redress in this proposal, the consumer needs to be provided with the appropriate information at the right time. It is key that in any consolidation of this information that it does not lead to a *reduction* of the information that is required to the point that it is ineffective and empty. The aim should be to remove redundancy and repetition.

We note that the proposed standards' changes outlined in Proposal 350 includes elements that *must* be included (the name of the person the CDR gave consent to, the purpose etc) and "should" elements that do not strictly have to be provided including (the names of each CDR participant and expiry dates). This provides too much ability for ADRs to obfuscate and hide important information that consumer may find useful. We recommend that these "SHOULD" statements be made "MUST" statements.

1.5. Simplifying the obligations in relation to CDR receipts

We support the list of information being included in a receipt in line with that of the design paper rather than that found at page 5 of the Standard proposal. That is, CDR receipts should include:

- the purpose of the consent(s);
- what data the consumer gave consent for the ADR to collect, use, or disclose;
- if any direct marketing or de-identification consents apply;
- when each consent was given, along with its duration and/or date of expiry;

[17] Page 5, Data Standards Body, Consumer Experience and Technical Working Groups, Decision Proposal 350: August 2024 Rules | Standards Impacts

- the name of the CDR participant from whom data was collected under a collection consent and the name of the recipient of data under any disclosure consents;
- for an insight disclosure consent — a description of the CDR insight;
- the details of any supporting parties that may access the consumer's CDR data at the time of the event that triggered the CDR receipt, be it consent, amendment, or withdrawal;
- a link to the CDR policies of any ADRs involved in the consent;
- instructions for dashboard access to review the most up to date information;
- if the consent is ongoing, the fact that the consent(s) can be withdrawn, and instructions for how to withdraw consent(s);
- information on redundant data handling and, if the consent has expired or been withdrawn, when redundant data is expected to be deleted or de-identified; and
- clear information on dispute resolution and making a complaint.

1.6. Requiring a data recipient to provide consumers information about all supporting parties who may access the consumer's data at the time a consumer gives a consent

While we agree with the additional information and consistency proposed here, we do not agree with the proposed standard that:

> *Data recipients **MAY** apply this standard to other changing attributes where the attribute in the amending consent request differs to that of the previous consent. How a changed attribute is signified is at the data recipient's discretion*

All changing attributes should be highlighted to the consumer. This allows Accredited Persons to not provide this information even where it may be relevant to the consumer continued consent. A consumer in this situation has not been informed nor consented to these changes and they cannot be implied in the situation where the CDR consumer does not withdraw their consent when notified. The "MAY" should be "MUST".

1.7. Requiring data recipients to delete redundant CDR data unless a consumer has given a de-identification consent

We support requiring data recipients to delete redundant CDR data by default. This is a positive step towards data minimisation and developing a more privacy-by-default approach that has been sorely missing in the development of the CDR, including in a number of the proposals in this package of reforms.

While the proposal is that deletion would occur unless a consumer has given a de-identification consent measure, we would argue that de-identification as an option should be

removed altogether based on the evidence re: re-identification and whether de-identification is ever in fact possible. Maintaining the ability to agree to de-identification can also lead to difficulties for consumers to withdraw this agreement and for industry to implement. Consumers would need to find their way to ability to do this which is currently confusing and difficult for consumers to navigate and know what they are agreeing to.

1.8. Requiring a data recipient to advise consumers of the marketing activities they will undertake because of a direct marketing consent

We support this proposal as a positive step to greater transparency.

2. Operational enhancements

2.1. Nominated representatives

We support this proposal.

Requiring that data holders provide CDR consumers with a process that is simple and straightforward to undertake a potentially complex but needed action (i.e. appointing representatives) is an important precedent to establish.

This should also be the case for establishing a simple and straightforward process to enable CDR consumers to alert a data holder of their experiencing (or fear of) financial abuse or domestic and/or family violence. to enliven the protections under Rule 4.7 re: refusing to disclose required consumer data if the data holder considers this to be necessary to prevent physical, psychological or financial harm or abuse.

2.2 Expanding the circumstances in which accredited ADIs can hold CDR data as a data holder

This proposal demonstrates one of the key flaws of the CDR regime – the over-reliance on disclosure and consent as the core protections in a regime that is incredibly complex and confusing.

The proposal assumes a theoretically rational CDR user will not just understand that providing a consent to undertake the actions foreseen will mean that that their data and privacy rights will be subject to different regimes and protections, but will understand what that means, how that will impact upon them if or when something goes wrong and integrate this into their decision-making.

In the real world – very few people will know what it will mean to be protected by the CDR Privacy Safeguards versus the APPs.

Placing the onus on the consumer to understand and integrate this into their decision-making process is unrealistic and overly burdensome.

Consumers want to know that their privacy will be a priority and that the data handling regime that they are engaging with will provide protections from anything going wrong and remedies when something does go wrong.

The weakness of disclosure as a consumer protection has been long identified by regulators as a tool that while still needed, cannot be relied upon to genuinely inform decision-making.[18]

We agree too with the PIA that a more practical result for the over-reliance on disclosure here will result in consumer being less inclined to exercise their CDR data rights – especially where there are "unintended or unwelcome uses of the consumer CDR data."[19]

A corollary of this issue is the situation is one that has currently come to prominence in the FCA pilot. Potential CDR consumers are legitimately concerned with the sharing of information with their DH ADI when considering consenting to sharing that data. Many CDR consumers are understandably refusing to consent to the sharing of their CDR data with a financial counsellor where they fear their ADI will learn of the fact that they are engaging with a financial counsellor. They are concerned that their engagement may be used as a red flag or in any way misused by the bank to deny further credit or other negative consequences. It is our understanding that the CDR framework does not have any restrictions on DHs use of information about who a consumer is interacting with for non-CDR purposes. In other words, there are no rules providing appropriate guardrails on the use of this information. This is a problem.

Similarly, there are no guardrails on DH ADI's advertising competing products in the circumstance where a CDR consumer is seeking information on potentially switching products.

[18] ASIC REP 632 Disclosure: Why it shouldn't be the default; Malbon, J & H Oppewal. (2018), "(In)effective disclosure: An experimental study of consumers purchasing home contents insurance, Monash Business School and Monash Faculty of Law, commissioned by Financial Rights Legal Centre

[19] Page 32, Mills Oakley, 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

This is an issue that will need to be thought through as more and more consumers are presented with the decision as to whether to consent to the sharing of data.

And in FCA's experience, consumers will default to *not* sharing their data and financial counsellors will default to advising certain more vulnerable cohorts of consumers *not to share* given the safety, privacy and security consequences of a decision in a realm that provides no certainty regarding the use by ADI DHs of that information.

We recommend that before this proposal is enacted, that Treasury examine ways to build the appropriate protections and frameworks in the use of CDR data for non-CDR purposes.

2.3. CDR representative arrangements

We support this proposal on the basis that it supports consistency of liability and protections.

2.4. Simplifying data holder requirements – secondary users

We support this proposal on the basis that the primary user still has control over the any potential use or misuse by a secondary user.

2.5. Exempting energy trial products from the CDR

The core concern with respect to these trial or pilot products being exempted from the protections of the CDR is that consumers continue to have to rely on the weak protections of the Privacy Act.

At a minimum, there needs to be privacy notices under APP 5 provided and express customer consent needs to be obtained to participate in a trial plan.

2.6. Codifying the prohibition of dark patterns into CDR

We note that Treasury had originally proposed a principles-based prohibition of dark patterns but has not progressed it because it is "not needed for the Data Standards Chair to set out principles-based requirements within the Standards."

Our view is that a principle-based prohibition of the use of dark patterns with a clear taxonomy should be provided in both the rules and their practical application addressed in the standards. The taxonomy should be developed in a way that it can be updated over time as the use of dark patterns evolve or further harms are identified.

Dark patterns should be adequately defined to ensure there are no loopholes that place intent over impact (even foreseeable impact) to consumers.

Below is some terminology from other jurisdictions that should be taken into account when developing the rules and standards:

- **EU Digital Services Act** specifically uses terminology such as, "*presenting non-neural, biases choices*" and refers to opt-out processes being more difficult than opting-in.[20]
- **California Consumer Privacy Act** has banned dark patterns, using language in its legislation that notes the practice as "*the substantial effect of subverting or impairing a consumer's choice…*".[21]
- **EU Unfair Commercial Practices Directive** does not specifically define dark patterns but instead provides examples of practices, in particular prohibiting practices, "w*ith the intention of inducing the consumer to buy the product at less favourable conditions*".[22]

The following two dark patterns should also be added to the list of dark patterns noted in the original consultation paper for ultimate inclusion in a prohibition list:

- Activity notifications that specifically exploit the bias of social norming by notifying a consumer about how other consumers engage or use a CDR-enabled product with the view to influence actions towards a particular product or service.[23]
- Confirmshaming where specific language is used to suggest that a particular choice is shameful or inappropriate. This will be pertinent especially if information is being provided on why certain data is being selected for sharing over others.[24]

Kind Regards,

Drew MacRae

[20] European Commission, *The Digital Services Act*,.
[21] State of California Department of Justice – Office of the Attorney General, 2021, *Attorney General Becerra Announces Approval of Additional Regulations That Empower Data Privacy Under the California Consumer Privacy Act*,
[22] European Commission, *Unfair commercial practices directive*,
[23] Gupta, C., 2022, *The choice mirage: how Australian consumers are being duped online via dark patterns*, Australian Journal of Competition and Consumer Law, 30(3), 241-245,.
[24] CPRC, Duped by Design, Manipulative Online design: Dark Patterns in Australia, June 2022

Senior Policy and Advocacy Officer
Financial Rights Legal Centre