Australian Banking Association

Consumer Data Right Rules: Consent and operational enhancements amendments

Consultation Paper

9 September 2024

Australian Banking Association

Consultation response

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

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

Proposals 1.1 and 1.2 have been bundled and answered thematically.

The ABA in principle supports consideration of changes to improve the functionality and user experience of CDR. However, we are concerned that well intentioned changes may risk embedding dark patterns in user interfaces that diminish consumer agency, do not align with proposed reforms to the Privacy Act and shift Australia away from global best practice.

Dark patterns

Dark patterns generally refer to practices in online user interfaces (particularly UX/UI design) that lead consumers to make choices that are not in their best interests. Dark patterns are diverse but often seek to separate a user from active decision making.[1] In the case of data collection and sharing processes, dark patterns have the practical effect of consumers unintentionally sharing more data than they mean to or needed to.

The ABA supports the proactive focus both the DSB and Treasury have placed on identifying and prohibiting dark patterns – also noted in the Privacy Impact Assessment for this consultation. However, we are concerned that the proposals – bundling consents and preselected data fields are dark pattern designs – incongruent with informed, in-control consumers.

These concerns are supported by significant evidence from global governments and regulators that online interfaces where significant consumer decisions are presented as defaults, preselected, or grouped so as to minimise conscious decision-making are dark patterns. For example:

- The US Federal Trade Commission[2] sees preselected defaults as likely to be harmful to users and lead to less informed consumers.
- The UK Competition & Markets Authority[3] identifies predefined, business preferred settings that require active steps to change as a 'choice structure' – a practice that strongly effects consumer behaviour and reduces their autonomy.
- Research from the European Commission[4] argues preselection and defaults are dark patterns that diminishes trust in digital markets and expose consumers to exploitation.
- European Data Protection Board guidelines on dark patterns note that preselecting defaults and grouping key customer approvals and acknowledgements prevents consumers giving informed consent – i.e. likely to represent deceptive snugness.[5]
- The OECD views preselected defaults for data collection consents as an interface interference technique that steers consumers towards more privacy-invasive settings.[6]

[1]. 'Dark Commercial Patterns' OECD Digital Economy Papers. October 2022
[2] 'Bringing Dark Patterns to Light' Staff Report, FTC, September 2022
[3] 'Online Choice Architecture. How digital design can harm competition and consumers' CMA. April 2022.
[4] 'Behavioural study on unfair commercial practices in the digital environment' European Commission. April 2022.
[5] 'Guidelines 3/2022 on dark patterns in social media platform interfaces.' European Data Protection Board. March 2022.
[6] 'Dark Commercial Patterns' OECD Digital Economy Papers, October 2022.

Australian Banking Association

Locally, the NSW Information and Privacy Commission notes *'bundled authorisations may not meet the criteria for valid consent'*[7], while the OAIC recognises consent bundling has the potential to undermine the voluntary nature of consent.[8]

It is also noted that the Privacy Impact Assessment undertaken for these proposals also identified concerns with both consent bundling and preselection:

- *"Bundling of consents maybe out of step with best practice and emerging trends in Australian and global privacy law."*[9]
- *"Generally speaking, pre-selected options and consents undermine consumer autonomy and choice."*[10]

Alignment with global best practice

As EU regulations regarding privacy are typically considered best practice, EU specific approaches to consents and dark patterns are important reference points. The General Data Protection Regulation (GDPR) – the EU wide information privacy regime – provides a clear definition of consumer consent regarding data collection in Article 4(11): consent must be *'specific, informed, unambiguous'*[11]

This understanding of consent is reflected elsewhere in the EU Digital Services Act which prohibits online platforms from designing any interface that *'distorts or impairs the ability of the recipients of their service to make free and informed decisions.'*[12] EU compliance guidance for industry is unambiguous*:*

> *"The Digital Services Act (DSA) contains an obligation that equates to a ban on using so-called dark patterns on online platforms. Under this obligation, online platforms will have to design their services in a way that does not deceive, manipulate, or otherwise materially distort or impair the ability of users to make free and informed decisions."*[13]

This example highlights how global best practice approaches see active decisions by consumers as key to informed consumers exercising agency and not being left in the dark.[14]

'Reasonably required'

The ABA acknowledges that the 'reasonably required' test, linked to a data minimisation principle is intended to safeguard consumers from sharing superfluous data. However, we are concerned that the current proposal – while a good start – does not provide sufficient protections to consumers. The key concerns include:

- The rules are broad, with the decision entirely at the ADR's discretion. With significant grey space, there is a risk that certain data recipients will be able to easily justify obtaining data is not essential to the purpose.
- It is unclear how the ADR's judgment of 'reasonably required' will be properly verified.

[7] 'Fact Sheet – Consent' Information and Privacy Commissioner NSW
[8] Australian Privacy Principle Guidelines – Key Concepts. OAIC 2022.
[9] See Privacy Impact Assessment page 7
[10] See Privacy Impact Assessment page 12
[11] See: https://gdpr-info.eu/art-4-gdpr/
[12] 'Article 25, Digital Services Act. See: https://www.eu-digital-services-act.com/Digital_Services_Act_Article_25.html
[13] See: https://digital-strategy.ec.europa.eu/en/faqs/digital-services-act-questions-and-answers
[14] See item 4.6: https://www.edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf

- The DMP link is important, however is unlikely to address these concerns. The fundamental assessment of what the minimum amount of data reasonably required would still rest entirely with the ADR, with no auditing of decisions.

Alignment to Privacy Act review[15]

While reforms to the Privacy Act are still being determined, there is sufficient evidence to suggest the proposed changes may not align with reformed privacy law. For example, the Government's response to the findings of the Privacy Act Review Report endorsed:

- Amending the meaning of consent to be defined as '*voluntary, informed, current, specific, and unambiguous.*' Overseas, governments and regulators have found similar definitions of consent to be incompatible with bundled consents and default data collection practices.
- Online privacy settings that reflect the '*privacy by default framework of the Act*.' This principle will have significant implications on the design of online services.

The Government's response also flagged increased responsibilities for the OAIC. These include a greater focus on enforcement, as well as responsibility for developing guidance for how online services design compliant consent requests. In this context, the previously expressed positions of the OAIC should be carefully considered:

> *"The OAIC considers that the requirement for an unambiguous indication through clear action would ensure that consent can still be implied by entities in appropriate circumstances. In contrast, consent that is given* ***through the use of preselected settings or opt-outs will not be sufficient to meet this requirement*** *as it is ambiguous as to whether the individual did in fact consent or simply did not engage with an opt-out mechanism."*[16]

Additionally, while not necessarily indicative of the requirements of the finalised reforms, the ACCC's response to the Privacy Act demonstrates their clear opposition to consent bundling and preselected data collection.

> *"Valid consent should require a clear affirmative act that is freely given, specific, unambiguous and informed (including about the consequences of providing or withholding consent). This means that any settings for data practices relying on consent must be preselected to 'off' and that different purposes of data collection, use or disclosure* ***must not be bundled****."*[17]

General comments

- While the ABA welcomes discussion on improving customer experience in the consent flow, we have concerns with any proposal to embed dark patterns in the consent flow, or other changes that shift consumer privacy protections away from global best practice.
- Notwithstanding our concerns outlined above, were the changes to be implemented as proposed, we would strongly urge introducing a stronger standard to the reasonably required test. For example, a requirement that preselected data be 'strictly essential only' would be a higher threshold than reasonably required.
- We support exclusion of direct marketing and de-identification consents.

[15] Privacy Act Review Report. See: Government response to the Privacy Act Review Report | Attorney-General's Department (ag.gov.au)
[16] Privacy Act Review Discussion Paper, OAIC submission, December 2021
[17] Privacy Act Review Report, ACCC submission, March 2023

- Given the focus, it is not anticipated that costs would be prohibitive for ABA members.
- While the intent of the changes is understood, it is unclear how the proposed changes would lead to greater consumer uptake or support the Minister's stated high priority use cases. Where the intent is either of these, we would welcome discussion on how these objectives can be best influenced.

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

In principle, the ABA supports consumers being empowered with all the relevant information required to support specific, informed and unambiguous consents.

We agree that the provision of specific and detailed withdrawal instructions is unlikely to be necessary when giving consent. We support the position that an accredited person be required to tell consumers during the consent flow that consents can be withdrawn and where further information can be found.

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

Consolidating 90-day notifications appears to be pragmatic, provided consumers continue to receive the appropriate information.

However, the ABA has reservations with the change being moved into the standards. With standards driven change already the primary driver of change, this move risks adding furthering the existing challenges in standards formation. We welcome discussion on whether this move is necessary.

1.5. Simplifying the obligations in relation to CDR receipts

The inclusions contained in the design paper standards appear appropriate.

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

No concerns with the proposed change. The ABA agrees with increased consistency and additional information.

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

No concerns with the proposed change.

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

The ABA supports this proposal.

2.1. Nominated representatives

On basis of our interpretation of the proposals and rationale outlined below, the ABA **is strongly opposed to the proposed change.** The key concerns have been outlined below.

Ambiguity of requirements – addition of (iii) and (iv) to paragraphs 1.13(1)(c) and (d) and subrule 1.13(1A)

The exposure draft proposes to add additional obligations on data holders to ensure specific consent management processes are "simple and straightforward to use" and "prominently displayed and readily accessible to the CDR consumer." We note these proposals are intended to improve customer experience; however, it is unclear what the incremental requirements would be – for example:

- What is the standard required by simple and straightforward to use? While it is critical that these requirements are not overly prescriptive, it remains unclear what changes would be required and what comparable processes would be referred to for determining simple and straightforward.
- What is expected by 'prominently displayed and readily accessible'? Non-individual customers engage with their bank differently to individuals, often outside a bank's primary digital channels or not via digital channels at all. Reflecting this, it is unclear what the proposed obligation would require from banks in practice.
- What is expectation behind 'must be online' in subrule **1.13(1)(1A)(a)**? Would making existing forms available for completion online suffice? How would this requirement be met if a bank required manual processes to accompany this (e.g. identification)?
- How would the requirements of **paragraphs 1.13(1)(c) and (d)** be implemented versus those under **subrule 1.13(1A)**? While it's noted that subrule 1.13(1A) applies only where there is an existing administrator with online account access, it is unclear whether the requirements of **paragraphs 1.13(1)(c) and (d)** could be satisfied in an offline process.

Congruency of the proposal to existing bank processes and channels.

The types of clients and products that would have access to nominated representative data sharing are typically complex, bespoke, and relationship managed. Processes for these clients are often manual – in part due to inability for straight-through-processing (and other scalable processes available for mass market consumers), while also subject to very different regulatory obligations. The convergence of these (and other) factors means that across the industry, the policies, processes and supporting infrastructure/core banking systems for non-individual customers varies greatly.

Business customers and products are complex, bespoke and relationship managed typically (i.e. they have one or more specialist bankers that support them with any needs). The effect of these factors is a business model that is highly reliant on manual processes and forms, which business customers are accustomed to. Where scalable and/or automated processes exist for individuals (e.g. identification), they often do not for non-individual customers (e.g. identifying non-individual account owners is a manual, non-standardised process).

It is critical that CDR requirements for non-individuals reflect the reality of standard industry practices. Given that the process for authorising administrators on non-individual accounts is universally a manual process, it is unclear how the proposed requirements could avoid creating divergence between these commensurate processes. For non-individual administrators with online

account access, the proposal under **subrule 1.13(1A)** would create disjointed and confusing customer experiences – a manual process for opening an account and appointing an administrator, but an online process for appointing the administrator as a nominated representative.

As a matter of principle, the CDR's requirements should not seek to change or influence commercial decisions outside the core requirements to enable data sharing. Therefore, CDR requirements have generally required data sharing functionality and CX to be of commensurate convenience to non-CDR processes only (i.e. no discrimination). This would also risk creating a situation contrary to the intent of **paragraph 1.13(1)(a)(ii)** by an online process for requests where there is not an existing online one.

While we are grateful for Treasury's consideration of these issues to date, this proposal represents a further incursion of CDR policy into territory that dictates **how** banks provide services to customers. In the case of mandating online forms, for most banks this will require a digital process to be developed, where comparable customer processes are manual.

Subrule 1.13(1A)

In addition to the issues raised already, the proposal to require the services under **rule 1.13** be made available online for authorised administrators with online banking access is deeply concerning.

- The proposed changes ostensibly seek to impose an online requirement only on administrators with online access to a CDR consumer's account. Practically speaking, it is difficult to see how this differentiation would be meaningful given the limited scenarios where an administrator would not have any form of online access.
- The compliance burden of maintaining different obligations for different non-individual customers based on their access status to non-CDR channels would be likely be impractical.
- Non-individual customer products often reside in entirely distinct and separate technology architectures to other core banking systems. Building an online flow for nominated representatives would be prohibitively expensive (discussed below).

There is no clear benefit from the proposed changes.

The ABA acknowledges the preference of some data recipients for an online process for nominated representatives and recognises in principle the advantages of a streamlined, online processes when compared to manual ones.

However, CDR engagement by non-individuals is extraordinarily low – some banks have seen less than 10 non-individuals share their data. Given nominated representatives are a subset category of non-individuals, the proposed changes will be ineffective in driving Treasury's stated objective *'to improve business adoption of the CDR'.*[18] Additionally, a change of this magnitude would misdirect resources, shifting investment and focus away from where almost all CDR usage is currently occurring.

Business banking is relationship based with customers have dedicated bankers to support them with any banking need or process. The relationship banking model is integral to the customer value proposition of business banking, hence it cannot be assumed that the existence of manual

[18] Consultation paper, page 10.

processes for highly complex needs is a problem to be solved, whereas it could be in mass-market retail banking models. As it has not been explained how the proposed changes would support high priority CDR cases, it is unclear whether this proposal is addressing a core customer opportunity, or whether it is responding to the existence of a manual process only.

Implementation costs will be prohibitive.

- Generally, where proposed changes require new digital capability to be built, the costs will be significant.
- The ABA has worked with several members to assess initial high-level costs for delivering the proposed changes. Indicatively we estimate implementation costs would be **at least ~$2 - $3 million** per bank.
- Conservatively, this would suggest costs to the banking sector of at least **$50 million**.
- These costs have the potential to be far higher than this however, given the precedent of CDR costs to date.
- It is not anticipated that the simpler requirements of **paragraph 1.13(1)(a)(ii)** would have a cost benefit given the significant costs for compliance with the online requirement of **subrule 1.13(1A)** would be primarily incurred in implementation – hence little expected marginal cost benefit between the two.

The Treasury's independent review into CDR compliance costs found CDR rules changes have often been considered without a full understanding of use cases and business practices. Given this conclusion and the concerns raised regarding the change proposal's commercial rationale, cost/benefit profile, and feasibility, the ABA strongly urges that the proposed changes to nominated representatives are reconsidered.

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

The ABA appreciates Treasury's consideration of changes to reduce barriers data holders experience when seeking to use data as a recipient. This proposal is in-principle supported, noting the comments provided below and requests for additional context.

- It is unclear precisely what problem is being addressed by the proposal, and how the proposed changes would lead to greater use of CDR data by banks. Further detail and examples of current issues experienced and how the proposed changes would address them would be helpful for consideration.
    - Detail on envisaged use cases that these changes would support would also be of value in assessing their utility.
- Clarity on what the regulatory obligations of holding CDR data as a data holder would be. Is it intended that were congruent to the requirements, CDR data received would in-effect leave CDR regulations and become subject to a bank's normal practices? For example, data received would be subject to a bank's obligations under the Privacy Act vs the CDR Privacy Safeguards.
    - As banks would receive the same types of data that they generate in their normal operations, there is a risk that the proposal may inadvertently introduce further complexity.
- The prescriptive requirements on when and how banks could hold CDR data as data holders in practice have the potential of introducing complexity. Managing this complexity

may be too risky or resource intensive for some, potentially limiting the efficacy of the changes.

While it is unclear how significant this proposal would be for CDR ecosystem growth, expanding the proposal to include services in addition to products could potentially increase its utility.

2.3. CDR representative arrangements

The ABA supports these changes.

2.4. Simplifying data holder requirements – secondary users

The ABA appreciates the intent of the proposed change and does not have a strong position either way. For rules and standards regarding secondary users, we urge sufficient consideration be given to financial abuse implications given the potential for misuse by perpetrators.

2.5. Exempting energy trial products from the CDR

N/A.

Policy Director contact: Maxwell Pryor
Policy Director
maxwell.pryor@ausbanking.org.au

About the ABA

The Australian Banking Association advocates for a strong, competitive, and innovative banking industry that delivers excellent and equitable outcomes for customers. We promote and encourage policies that improve banking services for all Australians, through advocacy, research, policy expertise and thought leadership.