Consumer Data Right Draft Operational Enhancement Rules

Supplementary Privacy Impact Assessment for the Department of Treasury

14 December 2022

Notice to Third Parties

This report is solely for the purpose set out in the Scope Section and for The Commonwealth Department of Treasury's information, and is not to be used for any purpose not contemplated in the engagement contract or to be distributed to any third party without KPMG's prior written consent. This report has been prepared at the request of The Commonwealth Department of Treasury in accordance with the terms of KPMG's engagement contract. Other than our responsibility to The Commonwealth Department of Treasury, neither KPMG nor any member or employee of KPMG undertakes responsibility arising in any way from reliance placed by a third party on this report. Any reliance placed is that party's sole responsibility.

The information contained in this report is of a general nature and is not intended to address the specific circumstances of any particular individual or entity. Appropriate professional advice should be obtained before acting on this information.

The views and opinions expressed herein are those of the author and do not necessarily represent the views and opinions of KPMG, an Australian partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International.

Table of Contents

Part 1. Introduction and Structure of this Report

1.1. Overview and context

1.1.1. The Consumer Data Right (**CDR**) was established by the *Treasury Laws Amendment (Consumer Data Right) Bill 2019* (**CDR Bill**) by inserting Part IVD into the *Competition and Consumer Act 2010* (**CCA**). The CDR is designed to enable individual and business consumers in certain (designated) sectors of the economy to have greater control over their data.

1.1.2. This supplementary privacy impact assessment (**SPIA**) follows consultation by Treasury on the expansion of the version 3 rules.[1] The version 3 rules introduced new disclosure options outside the CDR (trusted adviser and insight disclosures) and new access models (sponsorship and representative models). If made, the draft operational enhancement rules the subject of this SPIA would build on these measures by modifying and adding functionality to existing arrangements, data disclosures, and obligations in the current CDR Rules, and provide new mechanisms for consumers to share data with non-accredited entities.

1.1.3. The amendments that are currently proposed to be made through the draft operational enhancement rules are to implement the following measures (**5 Key Measures**):

1) **Measure 1: The introduction of business consumer disclosure consent (BCDC):** This measure would give business consumers (who are eligible CDR consumers) the ability to consent to their CDR data being shared with specified third parties, such as bookkeepers, consultants and other **unaccredited** advisers, who are not classified as 'trusted advisers' under the current CDR Rules. It would also allow for disclosures to the wide range of software providers that offer important services to small businesses in Australia. Prior to disclosing CDR data to an unaccredited person under a business consumer disclosure consent, accredited data recipients (**ADRs**) would need to take reasonable steps to confirm that either the business consumer is not an individual, or that they have an active ABN. The business consumer would also need to declare to the ADR that the data is being shared for a 'business purpose'.

2) **Measure 2: Extending the duration of Business Consumer consents:** Related to Measure 1, it is proposed to extend the maximum duration of certain use and disclosure consents given by a business consumer from a maximum of 12 months to seven years. It would remain possible for a business consumer to select a shorter consent period, or to withdraw their consent at any time. These amendments would address stakeholder feedback that business consumers are better placed to manage how their data is disclosed. It will also allow for business continuity and reduce the risk of inadvertent data loss (for example, ADRs must currently delete or de-identify consumer data when consent expires (within the 12 month period or immediately after), even if the expiry is inadvertent). This change does not apply to collection, AP disclosure, direct marketing and de-identification consents.

3) **Measure 3: Reciprocal data holder (DH) obligations for newly accredited entities that hold designated banking data:** Stakeholders raised concerns that the current reciprocal DH obligations which apply to banking datasets are stopping non-bank lenders (**NBLs**) from becoming ADRs. This measure would delay the imposition of these obligations until 12 months after the entity is becomes an ADR, allowing new entrants more time to build DH capabilities. This would operate similarly to the energy sector rules, which impose DH obligations on small retailers 12 months after they become accredited. It would not affect the timing of any obligations arising from the expansion of the CDR to Open Finance.

4) **Measure 4: Exemptions or deferrals of CDR obligations in respect of data generated as a part of small-scale, publicly offered trial products:**[2] This measure would allow DH in the banking sector to publicly offer small scale trial products, without being subject to data sharing

[1] See Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021. Note v4 of the Rules introduced energy CDR.
[2] This measure is being considered for expansion into other sections.

obligations (for up to 1000 consumers, for no longer than 6 months). If the product exceeds its consumer quantity or duration thresholds, the data becomes subject to data sharing obligations. This would address possible disincentives under the CDR for DHs to introduce innovative new products. This applies particularly to smaller DHs, who do not have the scale to trial products internally.

5) **Measure 5: Enhancements to CDR representative arrangements and CDR outsourcing arrangements:** This measure would remove the prohibition on CDR representatives from engaging outsourced service providers (**OSPs**) in a CDR outsourcing arrangement. This is in response to stakeholder feedback that businesses who rely on third parties to help them manage data currently have difficulty functioning in the CDR, affecting their ability to efficiently provide goods and services to consumers. In addition, it would amend and strengthen the provisions dealing with ADRs' liability for the actions of their CDR representatives and OSPs, including the actions of any OSPs engaged under further CDR outsourcing arrangements, and direct and indirect OSPs of the ADR's CDR representatives.

1.2. Development of the CDR and previous PIAs

1.2.1. Before outlining the scope of our assessment of the changes, it is helpful to summarise the structure of the CDR framework, which includes:

a. **Primary Legislation:** The CCA establishes the CDR framework and builds key protections into the CDR, including the sector designation process and the 13 Privacy Safeguards set out in Division 5 Part IVD.

b. **Privacy Safeguard Guidelines:** The OAIC has published CDR Privacy Safeguard Guidelines (**Guidelines**) in February 2020 under section 56EQ(1)(a) of the CCA. The Guidelines were updated in July 2020 (version 2), June 2021 (version 3) and November 2022 (version 4). The Guidelines outline how the Australian Information Commissioner will interpret and apply the 13 Privacy Safeguards. The purpose of the Guidelines is to ensure that the security and integrity of the CDR regime is maintained.

c. **Consumer Data Standards:** The DSB has published updated Consumer Data Standards (v 1.17.0), and updated CX Standards and supporting CX Guidelines (v 1.19.0) as at 21 June 2022.

1.2.2. A number of Privacy Impact Assessments (**PIAs**) have been undertaken on the CDR to date in relation to the effect of designation of sectors for CDR as well as prior amendments to the CDR Rules. These have included:

a. An initial PIA for the CDR, and a version reflecting feedback was released in March 2019.[3]

b. An independent draft SPIA conducted by Maddocks on the implementation of the CDR regime, Draft Rules (version 1), and the Draft Data Standards (in place at the time) which was finalised on 29 November 2019.[4]

c. An independent SPIA conducted by KPMG on the designation of the Energy sector (which was finalised on 25 May 2020.[5]

d. An independent PIA conducted by Maddocks on proposed CDR Rule amendments that related to access changes, joint account changes and new options to disclose CDR data to unaccredited entities (version 3), and was finalised on 29 September 2021.[6]

[3] The Department of Treasury, Privacy Impact Assessment – Consumer Data Right (March 2019): https://treasury.gov.au/sites/default/files/2019-03/p2019-t361555-pia-final.pdf
[4] Maddocks, PIA - Consumer Data Right Regime (29 November 2019), https://treasury.gov.au/sites/default/files/2019-12/p2019-41016_PIA_final.pdf .
[5] KPMG, Supplementary PIA - Consumer Data Right in the Energy Sector (25 May 2020), https://treasury.gov.au/sites/default/files/2020-06/p2020-89229.pdf
[6] Maddocks, Consumer Data Right Regime - Update 3 to PIA (29 September 2021), https://treasury.gov.au/sites/default/files/2021-10/p2021-213006-pia-maddocks.pdf

e. An independent PIA conducted by Maddocks on proposed CDR Rule amendments that related to the scope of DHs in the Energy sector (version 4) which was finalised on 29 October 2021.[7]

f. PIAs undertaken by Treasury and embedded in the Non-Bank Lending Sectoral Assessment[8] and the Telecommunications Sectoral Assessment.[9]

1.3. Approach

1.3.1. This SPIA builds upon existing PIAs prepared and/or commissioned by Treasury and is a "living document" which may be updated following further review and consultation with relevant stakeholders, including government, industry and customer representatives. In preparing the SPIA, KPMG has:

a. considered stakeholders' feedback received through Treasury's public consultation process regarding the draft operational enhancement rules;

b. assessed the likely effect of the proposed amendments against the broader CDR framework;

c. assessed the privacy impacts (risks and benefits) of the proposed amendments (under the draft operational enhancement rules) on the privacy and confidentiality of consumers' information; and

d. identified and recommended options for avoiding/minimising/mitigating negative privacy impacts caused by the proposed amendments.

1.3.2. KPMG acknowledges the valuable contribution from stakeholders. Stakeholder submissions have helped KPMG prepare this SPIA and have contributed to further the understanding of the privacy impacts and safeguards required for implementing the draft operational enhancement rules.

1.4. Structure of this report

1.4.1. The structure of this report is set out as follows:

a. **Part 2 (Summary of Findings and Recommendations**) explains our key findings and recommendations based on our scope and approach to this SPIA;

b. **Part 3 (Scope, Assumptions and Methodology)** explains why this SPIA is a point-in-time assessment and the assumptions that have been made to inform the breadth and depth of our considerations. It also summarises our approach to conducting this SPIA and outlines the publicly available information that we reviewed, the stakeholders that we consulted and the information received from Treasury;

c. **Part 4 (Key features of the draft operational enhancement rules)** describes the focus of the 5 Key Measures including a discussion about the key features and privacy considerations; and

d. **Part 5 (Analysis of Privacy Impacts and Risks)** analyses the privacy impacts and risks that we identified, having regard to the scope, approach and our assumptions and based on our review of information relevant to the impact of the proposed amendments to the CDR Rules.

[7]Maddocks, Consumer Data Right Regime - Update 4 to PIA (29 October 2021), https://treasury.gov.au/sites/default/files/2021-11/p2021-223520-update-4.pdf
[8] Consumer data right: Non-bank lending sectoral assessment, Final Report (August 2022), https://treasury.gov.au/sites/default/files/2022-08/p2022-300402-finalreport.pdf
[9] Consumer data right: Telecommunications sectoral assessment, Final Report (November 2021), https://treasury.gov.au/sites/default/files/2021-11/p2021-225262.pdf

Part 2. Summary of Findings and Recommendations

In preparing this SPIA, we identified and critically assessed and analysed the potential privacy risks and impacts both positive and negative from the draft operational enhancement rules. We have not attributed a risk level or rating to the privacy risks we have identified. Our recommendations are also developed on this basis.

2.1. Summary of findings

2.1.1. This section includes a summary of the key privacy impacts and risks identified from the draft operational enhancement rules. It is then followed by a summary of key recommendations made from our analysis of the risks and impacts. These privacy risks supplement the risks identified in the existing PIAs and are not intended to repeat those findings.

2.1.2. The key privacy risks that we consider require further mitigation strategies are:

1. A CDR business consumer may not understand the consequences of providing or withdrawing a business consumer disclosure consent allowing disclosure of their data to a third party ('receiving party').
2. The varied consent durations that could create confusion for business consumers, who under the proposed changes could give consent for up to seven years in some circumstances, but only up to 12 months in others.
3. DHs may use multiple trial products to avoid attracting CDR obligations (proposed to apply in banking, but may be extended to other sectors). The risk for potential CDR consumers is that they would not have the benefit of the CDR which has greater protections for consumers in the event their participation is deferred or avoided completely through the use of trial products.
4. OSPs use or disclose CDR data in a manner or for purposes that are not permitted by the CDR Rules. Further, allowing unaccredited CDR representatives and OSPs to outsource to other unaccredited entities may result in increased complexity in the CDR and reduce accountability of entities handling CDR data resulting in an erosion of consumer trust in the CDR framework.
5. A further authentication risk is in relation to business owners or representatives who are under the age of 18. This could occur if someone under the age of 18 ran a small business or was a sole trader and provided a business consumer disclosure consent to an ADR.

2.2. Summary of recommendations

2.2.1. Our corresponding recommendations to these key risks set out above are:

1. We **recommend** that**:**
   a. user testing and/or use case development is completed with CDR business consumers to ensure that the business consumer consent processes designed by the DSB are fit for purpose and ensure the correct consent(s) are provided;
   b. Treasury considers defining 'business purpose' in the CDR Rules. This could focus on the types of 'specified persons' intended to be in scope for these consents, and how the subsequent use of a business consumer's data can be limited for the purpose specified; and
   c. Treasury considers whether additional rules should be imposed on the administration of business consumer statements, such as a requirement to ensure the statements are retained for regulatory oversight.
2. We **recommend** that guidance is issued to business consumers on the available options to provide consent for the specified disclosures proposed under a BCDC, including how and when

the consent could end. It would be open to Treasury to determine the most suitable method to issue business consumers with such guidance.

3. We **recommend** that Treasury consult further with stakeholders on whether placing limits on the number of trial products, or the definition of trial products would prevent or mitigate opportunistic actions of this nature, noting the benefits of the trial and their intended purpose.

4. We **recommend** that guidance materials (such as those issued by the OAIC) are updated to support ADRs in understanding their obligations with respect to OSPs, including but not limited to the circumstances where an OSP must cease use of CDR data.

5. Treasury should consider developing guidance to support DHs (and/or ADRs and business consumers) in understanding how to deal with minors that may attempt to provide consent on behalf of a business. This could highlight that the onus is on DHs to confirm the age of a nominated representative (for a business), and what this means for other parties (i.e. ADRs, and businesses involving minors) in practice.

Part 3. Scope, Assumptions and Methodology

3.1. Scope

3.1.1. In preparing an assessment report for the Minister, Treasury must consider the likely effects of making new CDR rules on the privacy and confidentiality of consumers' information.

3.1.2. Treasury has engaged KPMG[10] to deliver a SPIA relating to the privacy issues (impacts and benefits) associated with amendments that, if made, would modify and add functionality to existing arrangements, data disclosures, and obligations, as well as provide new mechanisms for business consumers to share data with non-accredited entities. These are set out in the draft operational enhancement rules.

3.1.3. This SPIA has been conducted in accordance with the *OAIC's Guide to Undertaking Privacy Impact Assessments* (noting that the Privacy Safeguards replace the APPs for some purposes under the CDR) and reflects the findings of the CDR PIAs to date and stakeholders' responses to the draft operational enhancement rules.

3.1.4. The issues and risks in this SPIA have been considered on an 'exception' basis. That is, this SPIA addresses issues or risks in relation to the 5 Key Measures which have not been mentioned in the previous PIAs. Previous CDR PIAs have provided detailed overview and description of the CDR and its framework, which this SPIA relies on and refers to.

3.1.5. This SPIA is based on and has regard to the following assumptions:

a. **Supplementary PIA**: this SPIA supplements the CDR PIAs that have already been completed. It does not revisit or address certain aspects of the CDR that were the subject of previous CDR PIAs.

b. **Point-in-time analysis**: This SPIA has been prepared based on the issues and risks assessed at a point in time, noting:

   i. the CDR regime developments described in **Section 1.2** of this report; and

   ii. issues raised in this report may be subject to further review and analysis as the draft operational enhancement rules continue to be developed.

c. **Current reforms and reviews**: The Privacy Act, including consumer protections in relation to digital platforms, is currently undergoing review and reform (including the definition of personal information and whether it should include metadata). The scope of this SPIA does not extend to the examination of the proposed reforms.

3.2. Approach

3.2.1. In preparing this SPIA, the following steps were taken:

a. **Initial briefing:** we were briefed by and consulted with Treasury and agreed on the scope of the SPIA and working assumptions, which were refined during the assessment. We also discussed and identified material to be relied on, including Treasury's instructions in relation to the proposed policy intentions for the draft operational enhancement rules, and confirmation of the timeframes for completing the SPIA.

b. **Consultations:** consultation meetings were held with Treasury on a recurring bases to allow updates from both sides and track-keeping of the project. Consultations were also held with the OAIC and DSB.

c. **Stakeholder feedback**: in preparing this SPIA, KPMG has reviewed feedback received from stakeholders to Treasury specific to the draft operational enhancement rules.

[10] Including KPMG Law.

d. **Exposure draft rules**: KPMG has been provided with the exposure draft operational enhancement rules which inform this assessment.

e. **Publicly available information**: this SPIA draws on and reflects on a range of publicly available and relevant submissions, reports, and papers, including applicable research which were reviewed in the time available. A list of key materials that have been considered during the development of this SPIA is included in **Appendix 3** to this SPIA;

f. **CX Standards and Guidelines**: the objective of the CDR is to enable consumers to participate seamlessly in the CDR environment and to access and understand the CDR data that is held about them. We considered the applicable CX Standards and Guidelines that were relevant to formulating our analysis in this SPIA;

g. **Recommendations:** we identified and considered the current CDR framework and potential risk mitigation strategies that could further address the privacy risks. We also considered whether they were feasible at the current time or at some stage in the future before the implementation of the draft operational enhancement rules.

Part 4. Key features of the Measures proposed in the draft operational enhancement rules

The following section details the key features of the draft operational enhancement rules. As noted above, Treasury received public submissions on the exposure draft of the draft operational enhancement rules. The key considerations from those submissions as well as those received during consultations are included in the following discussion to the extent they remain relevant to the current proposed 5 Key Measures.

4.1. Business consumer disclosure consents

4.1.1. Through the creation of a business consumer disclosure consent, businesses would be able to consent to their CDR data being shared with specified persons (such as unaccredited third parties), like bookkeepers, consultants and other advisers who are not classified as trusted advisers under the current CDR rules. The proposed changes would also allow disclosures to the wide range of software providers that offer important services to small businesses in Australia.

4.1.2. The disclosure is to be made by an ADR on behalf of a business consumer in their capacity as a business.[11] To support this, ADRs would be required to take reasonable steps to ensure that the business consumer is not an individual or that the business has an active ABN.[12]

4.1.3. Further, the business consumer would be required to declare to the ADR that the data is being shared for a business purpose, in the form of a statement (business consumer disclosure statement). Stakeholder submissions included suggestions to require these statements to include the name of the receiving party, the scope of the consent, and/or any regulatory or professional standard obligations that the receiving party would be expected to comply with in the course of handling the consumer's data (e.g. accounting bodies). Some stakeholder submissions indicated a preference that the statements be administered online (such as in dashboards) rather than in paper form.

4.1.4. While this is intended to ensure that data is only shared for a business purpose, there is a risk that the business consumer could unintentionally provide consent to disclose data for non-business purposes.[13] This is more likely to occur if the business is a sole trader as the data shared may be more akin to the sole trader's personal information rather than business related data. In addition, there is the potential for an individual to be identified by the business consumer data (this could be a sole trader or an employee for example). Business consumers may not consider that these disclosures may include personal information.[14]

4.1.5. A business consumer may not understand the full range of consequences of providing or withdrawing a business consumer disclosure consent.[15] For example, it may be hard for a sole trader to distinguish whether the information they are agreeing to be disclosed is their personal information or business data of the business. There may also be added complexity for sole traders who are currently CDR consumers and could potentially, and separately, become a business consumer. The OAIC also noted there may be complexity in this situation in circumstances where the sole trader may provide separate consents in their capacity as both a CDR consumer and business consumer. Further, the OAIC noted that information in relation to sole traders and small business owners is often a mix of personal and business-related data. A disclosure of the businesses information for a business purpose may therefore also involve a disclosure of personal information.

4.1.6. There are also authentication risks associated with BCDCs. First, a CDR business consumer may not be properly identified for authentication purposes. Given the maximum duration of certain disclosure consents would be extended from 12 months to seven years (although a shorter period can be selected) there may be situations where the 'nominated representative' within a business has moved on over the

[11] See proposed CDR rule 1.10A.
[12] Note the draft operational enhancement rules do not confirm what is meant by 'reasonable steps' however it is noted the Privacy Safeguard Guidelines provide that the 'reasonable steps' test is an objective test and is to be applied in the same manner as 'reasonable' and 'reasonably'.
[13] This risk was raised in feedback from stakeholders.
[14] This risk was raised in feedback from stakeholders.
[15] This concern was raised by both the OAIC and DSB during consultations.

consent period and the relevant authentication expires for them before the period of consent does. Additionally, if the business consumer did not appropriately manage their nominated representatives with the relevant DH, this could mean the DH is no longer being able to authenticate the business.

4.1.7. The current CDR Rules require an individual CDR consumer to be 18 years of age or older to consent to data sharing. By contrast, non-individuals (i.e. business consumers) do not have an age requirement, however DHs must ensure that a non-individual appoints a nominated representative who is 18 years of age or older.[16] While this scenario may not occur often, it is possible that minors could approach ADRs potentially attempting to represent a business. The ADR may not be aware that the purported representative is a minor, and may not take steps to verify their age.

4.1.8. Feedback from stakeholders on this measure generally was that further guidance is required on how business consumer disclosure consents would operate in practice (such as the types of receiving parties to which the consents should apply, and example use cases on how the consents could operate). Stakeholders sought a clear definition of the term 'business purpose' in conjunction with the measure.[17] Concerns were raised about ensuring the measure is not relied on by third parties to access and use CDR data in circumstances that would otherwise require accreditation.

4.2. Extending business consumer use and disclosure consents from 12 months to seven years

4.2.1. It is proposed to extend the maximum duration of certain use and disclosure consents given by a CDR business consumer from twelve months to seven years (although a shorter consent period can be selected by them if facilitated by an ADR). The consent duration is intended to allow business consumers to choose a period that reflects the ongoing nature of their relationship with a service provider and to prevent undesirable data loss caused by inadvertent failure to renew consents. It would still not be possible to give a collection, AP disclosure, direct marketing or de-identification consent that is longer than 12 months.

4.2.2. Stakeholder feedback has indicated that business consumers are better placed than individuals to make informed decisions about how their data is disclosed. However, as noted above, there is a risk that business consumers do not understand the consequences of providing or withdrawing a business consumer disclosure consent. There is also a risk that the varied consent duration creates confusion for business consumers when providing consents that could otherwise be defined with a consistent limit. Concerns were also raised about whether extended consent could inadvertently allow disclosure of more data than necessary and/or was understood by the business consumer over an extended period.

4.3. Reciprocal data holder obligations for newly accredited entities holding designated banking data

4.3.1. This measure would delay the commencement of reciprocal data sharing obligations for ADRs until 12 months after they become an ADR. This measure is intended to remove the barrier to participation without removing the longer-term benefits of reciprocity in the CDR. Currently, the banking sector rules require newly accredited persons to respond to consumer data requests once they become an ADR.

4.3.2. The intention is to delay the imposition of DH obligations for 12 months to allow newly accredited entities holding designated banking data time to build DH capabilities. However, there is a risk that the 12 month timeframe may not be sufficient time for entities to be ready to comply. It may be prudent to issue guidance to entities on how to plan for compliance within this timeframe (particularly smaller entities) and/or how to seek exemptions in advance.

4.4. Exemptions or deferrals of CDR obligations in respect of data generated as a part of trial products

[16] See CDR rules 1.10B, 1.13(1)(c) and (d).
[17] This is a concern raised by various stakeholders including the Australian Competition and Consumer Commission, and the Joint Submissions of Chartered Accountants and Australia New Zealand, CPA Australia and the Institute of Public Accountants,

4.4.1. DHs in the banking sector[18]would be able to publicly offer small scale trial products (for up to 1,000 customers and for a 6-month maximum duration). Such products would be excluded from data sharing obligations while they are in scope of a trial, preventing ADRs from being able to access the trial data through the CDR.[19]

4.4.2. DHs could attempt to use multiple trial products to avoid attracting CDR obligations. While this is a framework risk, the associated privacy risk for CDR consumers is that data they wish to share that is in scope of a trial (that may otherwise be CDR data) is not handled consistently with the provisions and protections of the CDR, including the Privacy Safeguards.

4.5. Enhancements to CDR representative arrangements and CDR outsourcing arrangements

4.5.1. The amendments make changes to the rules around CDR representative arrangements and CDR outsourcing arrangements:

a. CDR representatives would be able to engage outsourced service providers (**OSPs**) in a CDR outsourcing arrangement, removing the current prohibition on such engagements

b. OSPs would be able to disclose CDR data under such arrangements:

i. to the principal of the CDR outsourcing arrangement,

ii. to the chain principal of that arrangement (that is, the ADR or CDR representative under which the CDR outsourcing arrangements have been set up),

iii. to another OSP of the chain principal, or

iv. in circumstances where the disclosure of the CDR data by the chain principal would be permitted under the CDR rules.

4.5.2. The changes respond to stakeholder feedback in relation to the current OSP and CDR representative rules, including that businesses who rely on third parties to help them manage data currently have difficulty functioning as an ADR or a CDR representative. Under the proposed amendments, ADRs are required to list direct and indirect OSPs in their CDR Policy and those of their CDR representatives.[20]

4.5.3. Proposed Rule 1.10 provides for the meaning of direct OSP, indirect OSP and related terms as follows:

> *For these rules, where a person who is an accredited person or a CDR representative is the principal in one or more CDR outsourcing arrangements:*
> 1. *the provider in each such arrangement is a **direct OSP** (for "direct outsourced service provider") of the person; and*
> 2. *where a direct OSP of the person is also the principal in a further CDR outsourcing arrangement, the provider in the further arrangement is an **indirect OSP** of the person; and*
> 3. *where an indirect OSP of the person is also the principal in a further CDR outsourcing arrangement, the provider in the further arrangement is also an **indirect OSP** of the person; and*
> 4. *the person is the **chain principal** of each direct and indirect OSP.*

4.5.4. Obligations relating to CDR outsourcing arrangements are the responsibility of the ADR;[21] and the ADR must ensure that OSPs that they or their CDR representatives contract with act in a manner that is compliant with the CDR rules (i.e. in an equivalent manner to how the ADR would if acting alone). The content of a CDR outsourcing agreement is a written contract between a person (the **principal**) and another person (the **provider**) under which the provider would either collect CDR data from a CDR participant in accordance with the CDR Rules on behalf of the principal,[22] or use or disclose data to

[18] However this may be expanded to the Telecommunications and Energy Sectors.
[19] See proposed CDR rules 1.10E, 3.1A(2).
[20] See CDR rule 7.2(f).
[21] See proposed CDR rule 1.16.
[22] Only those accredited to the unrestricted level. Treasury has instructed there is an error in the draft rules which will be amended to reflect this.

provide specified goods or services to the principal.[23] The CDR outsourcing agreement must also require the provider to comply with a number of requirements in relation to **service data**.[24]

4.5.5. A CDR representative arrangement[25] is a written contract between a person with unrestricted accreditation (the **CDR principal**) and a person without accreditation (the **CDR representative**) under which the CDR representative will offer goods and services to consumers for which it will need to use and/or disclose CDR data of the consumer. Under the arrangement, the CDR representative can obtain the consent of a CDR consumer to the collection, use and disclosure of CDR data in accordance with CDR rule 4.3A[26] and to use CDR data to provide the relevant goods or services to the CDR consumer.

4.5.6. CDR representative arrangements place a number of requirements on the CDR representatives, including that they must not enter into another CDR representative arrangement[27] and that they must comply with a number of requirements in relation to service data, including complying with Privacy Safeguards 2, 4, 12, 13 and the quality elements of Privacy Safeguard 11.[28]

4.5.7. In addition to the above requirements, the CDR rules relating to Privacy Safeguards 4,[29] 8, 9,[30] and 12[31] broadly state that an ADR breaches the relevant subrules if a direct or indirect OSP of the ADR or a CDR representative of the ADR fails to comply with the relevant provisions in the CDR rules.

4.5.8. Further, it is proposed to amend the CDR Rules relating to CDR data[32] to provide that the collection, use and disclosure of service data by a direct or indirect OSP of an accredited person is taken to have been by the accredited person, and it is irrelevant whether the collection, use or disclosure is in accordance with the relevant CDR outsourcing arrangement.

4.5.9. The onus would be on the ADR to ensure that OSPs and CDR representatives (that they contract with) act in a manner that is compliant with the CDR Rules and the relevant CDR outsourcing arrangement or CDR representative arrangement. If there is non-compliance, there is a risk that the ADR will lose its accreditation or be subject to compliance action. For these reasons, the ADRs should be motivated to monitor and ensure compliance.

4.5.10. In practice however, there may be barriers to this such as the ability to take steps to ensure the OSP or CDR representative is fit and proper prior to entering into an outsourcing arrangement or CDR representative arrangement, as well as the costs associated with actions to ensure that the terms of any agreement/ arrangement are complied with.

4.5.11. Under the CCA, the Australian Information Commissioner may conduct an assessment, in a manner they see fit, of whether a CDR participant is managing and handling CDR data in accordance with the Privacy Safeguards and privacy or confidentiality related CDR Rules.[33]. Some submissions suggested a third party management framework similar to that required for those seeking to sponsor an Affiliate

[23] See proposed CDR rule 1.10.
[24] See proposed CDR rule 1.10(4); Service data in relation to a person who is a direct or indirect OSP of a chain principal means any CDR data of a CDR consumer of the chain principal held by the person that: (a) was disclosed to the person by the chain principal for the purposes of the relevant CDR outsourcing arrangement; or (b) was collected from a CDR participant by the person on behalf of the chain principal in accordance with the relevant CDR outsourcing arrangement; or (c) was disclosed to the person by another direct or indirect OSP of the chain principal in accordance with the relevant CDR outsourcing arrangement for the other direct or indirect OSP; or (d) directly or indirectly derives from such CDR data.
[25] See proposed CDR rule 1.10AA.
[26] CDR rule 4.3A.
[27] See proposed CDR rule 1.10AA(3)(a).
[28] See proposed CDR rule 1.10AA(4). We note that the OAIC recommended in their submission that OSPs should comply with Privacy Safeguards 2, 4, 9, 11, 12 and 13, however we note that the current or proposed CDR rules 7.3, 7.3B, 7.8B, 7.10A 7.11, 7.12 and 7.16 already provide related protections to CDR consumers.
[29] See proposed CDR rule 7.3B.
[30] See proposed CDR rule 7.8B.
[31] See CDR rules 7.11 & 7.12
[32] See subdivision 7.2.3 of the CDR Rules.
[33] See s 56ER of the CCA. It is also noted that there is a question of whether OSPs and CDR representatives should be regulated by or come within the OAIC and ACCC Part IVD enforcement powers.

(Schedule 1, Part 2, Rule 2.2(1)(a)), or a documented process for ADRs to record the steps taken by their CDR representatives/OSPs to comply with the agreed requirements.[34]

4.5.12. The proposed amendments to CDR outsourcing arrangements would enable CDR data to be disclosed to further OSPs down the chain, for the purpose of providing goods and services to a principal. Stakeholder feedback has raised concerns that the proposed measures may dilute the direct application of the Privacy Safeguards and responsibility for CDR data shared down the line. However, as outlined above, the onus is on the ADR to ensure OSPs and CDR representatives that they contract with act in a manner that is compliant with the CDR Rules, and the relevant CDR outsourcing or representative arrangement. But ensuring compliance down the chain may be difficult for ADRs. A key concern raised was in relation to possible cyber incidents involving CDR representatives and how an ADR would be able to retain responsibility for compromised CDR data held by their CDR representative/s in practice.[35] The OAIC suggested a process whereby CDR representatives are required to notify principals of data breaches in consultations.

4.5.13. To promote transparency, the proposed amendments include a requirement for accredited persons to identify whether CDR data is likely to be disclosed to an OSP and the countries that OSPs are likely to be based, with their CDR policy updated accordingly.[36]

4.5.14. Feedback from stakeholders raised concerns about the practicality of this measure as the OSP chain grows.

[34] This concern was raised by numerous stakeholders including the Australian Competition and Consumer Commission.
[35] This concern was raised by numerous stakeholders including Cuscal and Telstra.
[36] See proposed CDR rule 4.11 and 4.20E. This concern was raised in the OAIC's submission.

Part 5. Analysis of Privacy Impacts and Risks

5.1 Analysis of privacy risks

This section provides an assessment of the key privacy impacts and risks that have been identified in relation to the proposed expansion of CDR through the operational enhancements to the CDR framework that are proposed in the draft operational enhancement rules. The impacts and risks are identified from the updated proposed draft operational enhancement rules package.

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
Measure 1: Business consumer disclosure consent (**BCDC**)			
1.	Individuals who are not CDR business consumers may become the subject of CDR data that is disclosed under a BCDC. There are more consumers potentially involved in the CDR data of a CDR business consumer than just the business owner/director. There is a risk that the non-CDR business consumer's data is incorrectly inferred with the behaviour of the business and subsequently used for purposes that the consumer did not consent to or would not reasonably expect. Once disclosed under a BCDC, any personal information (including sensitive personal information) would no longer be held within the CDR system and therefore would not be protected by the CDR data security requirements and Privacy Safeguards. Further, an individual could be identified by CDR business consumer data. By way of example, sole traders/ small businesses where the CDR business consumer data could relate to only one or a small number of individuals.	CDR Rule r4.12(3)(b)(iii) prohibits ADRs from requesting consent to use CDR data for the purpose of identifying, compiling insights in relation to, or building a profile in relation to any identifiable person who is not the CDR consumer making the consumer data sharing request. The data minimisation principle also limits the CDR data that can be collected, and also limits the uses that can be made of collected CDR data. Some unaccredited recipients may be subject to obligations outside of the CDR to protect the data they receive about a CDR business consumer as their customer (e.g. general professional/contractual obligations, or existing Privacy Act obligations if they are not exempt and to the extent to which the data may be personal information).	We **recommend** that Treasury considers a method to encourage ADRs to communicate the scope of the business consumer's consent to unaccredited recipients. The way this could occur (e.g. via the Rules or Guidance)) would be open for Treasury to consider. We also **recommend** that Treasury considers a method to require unaccredited recipients to delete or de-identify consumer data once there is no longer a purpose to retain it (e.g. pursuant to APP 11). See also **recommendations** in No. 4 below which may also assist with limiting the risk.
2.	Unaccredited recipients of CDR data will not be subject to obligations under the CDR, may not be subject to the Privacy Act, and may lack the resourcing and skills needed to safely and securely deal with CDR data.	As above - CDR Rule r4.12(3)(b)(iii) prohibits ADRs from requesting consent to use CDR data for the purpose of identifying, compiling insights in relation to, or building a profile in relation to any identifiable person who is not the CDR. consumer making the consumer data sharing request. The data minimisation principle also limits the CDR data that can be collected, and also limits the uses that can be made of collected CDR data. Privacy Safeguard 6 only permits disclosure of the CDR data in accordance with the CDR Rules	As above - we **recommend** that Treasury considers a method to encourage ADRs to communicate the scope of the business consumer's consent to the unaccredited recipient. The way this could occur (e.g. via the Rules or Guidance) would be open for Treasury to consider. We also **recommend** that Treasury consider a method to require unaccredited recipients to delete or de-identify consumer data once there is no longer a purpose to retain it (e.g. pursuant or similar to APP 11). We also **recommend** that user testing should be undertaken with unaccredited recipients to determine how they will understand the impact of the consent provided by the business consumer against their ability to use the data.

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
			See also **recommendations** in No 4 below which may also assist with limiting the risks.
3.	A further authentication risk is in relation to nominated representatives under the age of 18 who purport to be eligible to authorise data sharing. This could particularly be problematic if a minor ran a small business or was a sole trader, and provided a business consumer disclosure consent to an ADR.	CDR Rule 1.13(1)(c)) requires DHs to ensure that a non-individual CDR consumer has nominated one or more individuals that are 18 years of age or older (**nominated representative**) to consent to data sharing on behalf of the business.	It may not be clear to participants that the onus to administer CDR Rule 1.13(1)(c) rests with a DH alone. While this scenario may not occur often, it may be prudent for the ACCC to issue guidance to DHs (and/or ADRs and business consumers) on how to deal with minors potentially attempting to represent a business, particularly to highlight that the onus is on DHs to confirm the age of a nominated representative, and what this means for other parties (i.e. ADRs, and businesses involving minors) in practice.
4.	A CDR business consumer may not understand the consequences of providing or withdrawing a business consumer disclosure consent allowing disclosure of their CDR data to a third party ('**receiving party'**). For example, a business consumer may unintentionally provide consent to disclose data for non-business purposes or may not be able to distinguish whether the information being disclosed is their personal information or that of others or business data of the business.	CDR Rules 4.11(1) and (3) require an accredited person seeking consent from a CDR consumer to clearly indicate the particular types of CDR data to which the consent will apply, and the specific purposes that they are consenting to. The CDR consumer must also be made aware of how the requested use complies with the data minimisation principle (i.e. the use would not go beyond what is reasonably needed). CDR Rule 4.11(3) requires an accredited person seeking consent from a CDR consumer to provide a statement that their consent can be withdrawn at any time. Proposed CDR Rule 1.10A(7) will introduce the concept of a business consumer statement, designed to certify that a (business related) consent is given for the purpose of enabling an accredited person or CDR representative to provide goods or services to a CDR business consumer in its capacity as a business (and not an individual). Another existing mitigation strategy is the requirement for the Data Standards Chair to make standards for disclosure of CDR data to a person under a BCDC. Further Treasury intends to add a requirement for the for the Data Standards Chair to make standards for business consumer statements.	We **recommend** user testing and/or use case development is completed with CDR business consumers to ensure that the business consumer consent processes designed by the DSB are fit for purpose and ensure the correct consent(s) are provided. Such testing should consider whether CDR business consumers fully understand what disclosures they are consenting to, and the extent to which they understand that their disclosure will allow CDR data to be shared with an unaccredited third party (who will not be subject to CDR requirements). We also **recommend** Treasury considers defining 'business purpose' in the CDR Rules. This could focus on the types of 'receiving parties' intended to be in scope for these consents, and how the subsequent use of a business consumer's data can be limited for the purpose specified. We also **recommend** Treasury considers whether additional rules should be imposed on the administration of business consumer statements, such as a requirement to ensure the statements are retained for regulatory oversight. Stakeholder submissions included suggestions to require the statements to include the name of the receiving party, the scope of the consent, and/or any regulatory or professional standard obligations that the receiving party would be expected to comply with. Some stakeholder submissions indicated a preference that the statements be administered online (such as in dashboards) rather than in paper form.
5.	An ADR requires the giving of a business consumer disclosure consent as a condition for the supply of goods or services	CDR Rule 1.10A which prevents ADRs requiring the giving of consent as a condition for the supply of goods or services is	The extension of the CDR consent framework under CDR Rule 1.10A to prohibit the requesting of a BCDC as a condition for the supply of goods or

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
	requested by the CDR business consumer.	being extended to cover business consumer disclosure consents.	services requested by the CDR business consumer appropriately mitigates this risk.
Measure 2: Extending the duration of business consumer use and disclosure consents			
6.	Varied consent durations could create confusion for business consumers, who under the proposed changes could give consent for up to seven years in some circumstances, but only up to 12 months in others. This could open up risks of businesses forgetting or failing to have regard to a consent that has not been renewed or reviewed for some time.	The maximum duration of use and disclosure consents given by a CDR business consumer will be extended from 12 months to seven years (although a shorter consent period would be able to be selected) (see proposed CDR rule 4.12(1)). Collection, AP disclosure, direct marketing and de-identification consents will not be included in this extension. We understand it will be matter for businesses to determine whether an extended consent is appropriate to their business needs, and that an extension to a 7 year consent would not be appropriate in many instances.	It is **recommended** that guidance is issued on the available options for business consumers in providing extended consent for the specified purposes and disclosures available under a BCDC, including how and when it would be appropriate for a consent to be extended, and the circumstances that should prompt any extended consent to be reviewed. It would be open to Treasury to determine the most suitable method to issue business consumers with such guidance. For example, updated Guidance could be issued by the OAIC under the 'CDR privacy safeguards': https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguardsAlternatively, Treasury could consider adding further relevant guidance for business consumers in the 'Resources for Consumers' webpage: https://www.cdr.gov.au/resources or the 'Consumer Data Right Support Portal': https://cdr-support.zendesk.com/hc/en-us.
7.	If the maximum durations of certain business use and disclosure consents are extended from 12 months to seven years (although a shorter period would be able to be selected) there may be situations where the 'nominated representative' within a business has moved on, or other circumstances involving business changes occur, and therefore the business is no longer able to be authenticated.	The Consumer Data Standards for 'authentication flows' state that "*Data Holders must request a user identifier that can uniquely identify the customer and that is already known by the customer in the redirected page*". We understand that the amendments to the Rules will not materially affect authorisations, which will continue to have a maximum duration of 12 months before they need to be renewed under rule 4.23.	The existing framework for authentication flows require DHs to ensure that they are dealing with the correct nominated representative.
Measure 4: Exemptions or deferrals of CDR obligations in respect of data generated as a part of trial products			
8.	DHs in the banking sector may use multiple trial products to avoid attracting CDR obligations. The risk for potential CDR consumers is that they will not have the benefit of consistent CDR protections from the use of trials, particularly where a consumer seeks a means to disclose the data to an ADR.	Rule 1.10E clearly defines the meaning of a 'trial product'. By placing clear parameters on this, the risk identified is mitigated.	It is **recommended** that Treasury consider placing limits on the number of trial products, or amending the definition of trial products to prevent or mitigate opportunistic actions of this nature, noting the benefits of the trials and their intended purpose. It is acknowledged that this is not an immediate risk as trial products are short term, and could be monitored over time as more trials are introduced.
Measure 5: Enhancements to CDR representative arrangements and CDR outsourcing arrangements			

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
9.	CDR consumers are unaware that their CDR data is being shared and handled by OSPs or CDR representatives.	CDR Rule 4.11(3) provides that when asking a CDR consumer to give consent, an accredited person must give the CDR consumer: a statement advising that the CDR data may be disclosed to, or collected by an OSP or CDR representative of the accredited person, a link to the accredited person's CDR policy; and a statement that the consumer can obtain further information about such disclosures from the policy if desired.[37] The proposed CDR rule 7.2(4)(f) requires ADRs to list direct and indirect OSPs and CDR representatives in their CDR Policy. Further, the onus is on the ADR to ensure OSPs and CDR representatives are compliant with the relevant outsourcing arrangement or CDR representative arrangement. The proposed draft operational enhancement rules make ADRs liable for the actions of their direct and indirect OSPs, as well as those of the direct and indirect OSPs of their CDR representatives.	It is **recommended** that a requirement be added under CDR Rule 7.2 for the CDR principal's CDR policy to contain details about the countries the CDR principal's CDR representatives may disclose to when making a disclosure to an unaccredited OSP. We consider the requirement that ADRs list direct and indirect OSPs and any CDR representative in their CDR Policy helps to appropriately mitigate remaining risks in relation to OSPs.
10.	OSPs use or disclose CDR data in a manner or for purposes that are not permitted by the CDR Rules.	Under proposed CDR Rule 1.16(1), ADRs are responsible for ensuring that direct and indirect OSPs are compliant with their applicable CDR outsourcing arrangement, which is a written contract that must include the required provisions (or terms) outlined in proposed CDR Rule 1.10(2), breach of which is subject to a civil penalty provision. The terms cover compliance with applicable CDR Rules.	The strengthening of requirements for OSPs under the draft operational enhancement rules package seeks to mitigate this risk. This includes the responsibility for ADRs to ensure that OSPs are compliant with the CDR rules under the proposed amendments to CDR Rule 1.10, as well as additional recordkeeping and reporting requirements. It is **recommended** that guidance materials (such as those issued by the OAIC) are updated to support ADRs in understanding their obligations with respect to OSPs, including but not limited to the circumstances where an OSP must cease use of CDR data.
11.	Allowing unaccredited CDR representatives and OSPs to outsource to other unaccredited entities may result in increased complexity in the CDR and reduce accountability of entities handling CDR data resulting in an erosion of consumer trust in the CDR framework	The proposed CDR Rules changes referred to above take a similar approach to making ADRs liable for the actions of the direct and indirect OSPs of their CDR representatives.	It is **recommended** that Treasury consider whether additional record keeping and reporting obligations, including in relation to notifiable data breaches, should apply to CDR representatives, OSPs and their principals. It is also **recommended** that ADRs require any unaccredited CDR representatives and OSPs to immediately notify the ADR of a data security breach or information security incident involving CDR data.

[37] This obligation also applies to CDR representatives, see proposed CDR rules 4.20E(3)(k) and (l).

Appendix 1. Glossary

Term	Description
Accredited Data Recipient	has the meaning given to that term in section 56AK of the CCA.
Accredited Person	means a person who holds an accreditation by the Data Recipient Accreditor (i.e. the ACCC) under subsection 56CA(1) of the CCA. This person and the ADR are the same person.
ACCC	means the Australian Competition and Consumer Commission, who has CDR rule making powers and is responsible for, among other things, maintaining the Register of Accredited Persons for the purpose of the CDR regime (as set out in Part IVD of the CCA).
Australian Privacy Principles	means the Australian Privacy Principles at Schedule 1 to the Privacy Act.
CCA	means the *Competition and Consumer Act 2010* (Cth).
CDR Consumer	has the meaning given to that term in subsection 56AI(3) of the CCA.
CDR data	has the meaning given to that term in subsection 56AI(1) of the CCA.
CDR Participant	has the meaning given to that term in subsection 56AL(1) of the CCA.
CDR Privacy Safeguards	means the 13 privacy safeguards set out in Division 5 of Part IVD of the CCA for which the OAIC is responsible for administering.
CDR Privacy Safeguard Guidelines	means the CDR Privacy Safeguard Guidelines published by the OAIC in February 2020 under section 56EQ(1)(a) of the CCA. The Guidelines were updated in July 2020 (version 2), June 2021 (version 3) and November 2022 (version 4).
CDR Rule/s	means the *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) as in force on 10 February 2022.
Consumer Dashboard	means: a) in relation to an Accredited Person, an online service described in paragraph 1.14(1) of the CDR Rules; and b) in relation to a Data Holder, an online service described in CDR Rule 1.13(1)(a).
Consumer Data Request	means a request for CDR data as described in CDR Rule 1.4s.
Consumer Data Standards	means the technical standards developed by the Data Standards Body which represent the current baseline for implementation of the CDR by the relevant participants. See version 1.18.0, 11 August 2022: https://consumerdatastandards.gov.au/2022/08/consumer-data-standards-1180
Consumer Experience Guidelines	means the consumer experience guidelines developed by the Data Standards Body to support the implementation of the Consumer Experience Standards: https://d61cds.notion.site/d61cds/Consumer-Experience-Standards-and-Guidelines-dffe42d39d4942c5b4f2c7612ba4f6e0
Consumer Experience Standards	means standards developed by the Data Standards Body in relation to consumer experience under CDR Rule 8.11 and may have binding effect under section 56FA of the CCA: https://d61cds.notion.site/d61cds/Consumer-Experience-Standards-and-Guidelines-dffe42d39d4942c5b4f2c7612ba4f6e0
Customer Provided Data	means data provided by the CDR Consumer including name of account holder, contact details including billing address or postal address, and information provided about the property including appliances.
Data Holder "DH"	has the meaning given to that term in section 56AJ of the CCA.
Data Minimisation Principle	means a requirement that needs to be complied with by an Accredited Person and has the meaning given to that term in rule 1.8 of the CDR Rules.
Data Standards Body	means a person appointed under section 56FJ of the CCA. At present, this person is CSIRO's Data61.
Data Recipient Accreditor	means the person appointed under subsection 56CG(1) of the CCA. At present, this is the ACCC.
Designation Instrument	means a statutory instrument designating a particular sector to implement the CDR regime.
Eligible CDR Consumer	means a CDR Consumer that is described as such under the CDR Rules (in relation to a particular sector of the Australian economy).

Personal Information	has the meaning given to that term in the Privacy Act.
Privacy Act	means the *Privacy Act 1988* (Cth).
Register of Accredited Persons	means the register of Accredited Persons maintained by the Accreditation Registrar in accordance with Subdivision B, Division 3 of Part IVD of the CCA.

Appendix 2. Abbreviations

Abbreviation	Definition
ACCC	Australian Competition and Consumer Commission
ADR	Accredited Data Recipient
AEMO	Australian Energy Market Operator Limited
APP Code	Privacy (Australian Government Agencies – Governance) APP Code 2017.
APPs	13 Australian Privacy Principles under schedule 1 of the Privacy Act 1998 (Cth)
CCA	Competition and Consumer Act 2010 (Cth)
CDR	Consumer Data Right
CDR Rules	Competition and Consumer (Consumer Data Right) Rules 2020
CX	Consumer Experience
DSB	Data Standards Body
Guidelines	CDR Privacy Safeguard Guidelines
Minister	The Prime Minister, the Treasurer, and the Minister for Superannuation, Financial Services and the Digital Economy
NBL	Non-Bank Lending
OAIC	Office of the Australian Information Commissioner
OSPs	Outsourced service providers
PI	Personal information
PIAs	Privacy Impact Assessments
Privacy Act	Privacy Act 1988 (Cth)
Safeguards	13 CDR Privacy Safeguards
SPIA	Supplementary Privacy Impact Assessment
Treasury	Commonwealth Department of the Treasury

Appendix 3. List of materials reviewed

We reviewed the following key materials while preparing this SPIA:

a. Competition and Consumer Act 2010 (Cth).

b. Competition and Consumer (Consumer Data Right) Rules 2020 (Cth).

c. Consumer Data Right May 2022 Guideline 'Compliance Guide for Data Holders'

d. Consumer Data Right Webpage 'Guidance for data holders - assessing whether a product is in scope for CDR' (December 2021).

e. Consumer Data Standards and the latest CX Standards and Guidelines version 1.17.0.

f. Draft proposal of the draft operational enhancement rules .

g. KPMG's 25 May 2020 (with analysis as at 27 April 2020) PIA 'Consumer Data Right in the Energy Sector: Supplementary Privacy Impact Assessment for the Commonwealth Department of Treasury' (commissioned by Treasury)

h. Maddocks' 29 November 2019 (with analysis as at 23 September 2019) PIA 'Consumer Data Right Regime' (commissioned by Treasury).

i. Maddocks' 29 October 2021 (with analysis as at 26 October 2021) PIA 'Consumer Data Right Regime: Update 4 to Privacy Impact Assessment' (commissioned by Treasury).

j. Maddocks' 29 September 2021 (with analysis as at 17 September 2021) PIA 'Consumer Data Right Regime: Update 3 to Privacy Impact Assessment' (commissioned by Treasury).

k. OAIC's May 2020 Guideline 'Guide to Undertaking Privacy Impact Assessments'.

l. Privacy Act 1988 (Cth).

m. Privacy (Australian Government Agencies - Governance) APP Code 2017.

n. Treasury Laws Amendment (Consumer Data Right) Act 2019 (Cth).

o. Treasury's March 2019 PIA 'Privacy Impact Assessment: Consumer Data Right'.

Appendix 4. List of stakeholder submissions reviewed

Treasury provided submissions from the following stakeholders. We reviewed these submissions while preparing this SPIA. We acknowledge each stakeholder's contribution and appreciate their support:

a. Adatree
b. AGL Energy
c. Australian Banking Association
d. Australian Competition & Consumer Commission
e. Australian Finance Industry Association
f. Australian Securities and Investments Commission
g. Biza.io
h. Chartered Accountants Australia & New Zealand, CPA Australia & Institute of Public Accountants (combined submission)
i. Commonwealth Bank of Australia
j. Council of Small Business Organisations Australia
k. Cuscal
l. Digital Service Providers Australia New Zealand
m. Energy Australia
n. FinTech Australia
o. iSelect
p. Law Council of Australia
q. Mastercard
r. Office of the Australian Information Commissioner
s. Optus
t. Origin Energy
u. Red Energy and Lumo Energy
v. SISS Data Services
w. Tech Council of Australia
x. Telecommunications Industry Ombudsman
y. Telstra Corporation Limited
z. Xero, Intuit & MYOB (combined submission)