Australian Government

Office of the Australian Information Commissioner

Submission by the Office of the Australian Information Commissioner

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

26 October 2022

OAIC

Part 1: Introduction

1.1 The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on Treasury's exposure draft version of *The Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1)* 2022 (the '**draft rules**'). The draft rules expand the Consumer Data Right (CDR) to the telecommunications sector and add operational enhancements.

1.2 The draft schedule dealing with the telecommunications sector includes:

- the types of data holders for the sector and when their obligations will apply
- the criteria for eligible CDR consumers
- the types of telecommunications data that may be accessed through the CDR
- dispute resolution requirements for the sector.

1.3 The operational enhancements include:

- business consumer disclosure consents (BCDCs), which allow business consumers to disclose CDR data to specified persons who may not be accredited
- an ability for business consumers to extend the duration of use and disclosure consents to 7 years
- the removal of the prohibition against CDR representatives engaging outsourced service providers (OSPs)
- amendments to the provisions relating to CDR representative arrangements and CDR outsourcing arrangements.

1.4 The functions of the Australian Information Commissioner (the Information Commissioner) include examining proposed enactments that may have an adverse effect on the privacy of individuals and minimising such effects.[1] Under Part IVD of the *Competition and Consumer Act 2010* (the CCA), the Information Commissioner must also be consulted before rules are made on the likely effect of making the instrument on the privacy or confidentiality of consumers' information.[2]

1.5 The OAIC makes this submission to provide our current consideration of the privacy impacts of the draft rules and how any adverse effects may be minimised. Detailed comments and recommendations regarding the draft rules are below, and we are available to discuss our submission with Treasury.

1.6 The telecommunications sector handles a wide range and large volume of personal information in the course of providing services to their customers. This can reveal rich insights about a consumer and a detailed picture of their personal life. The CDR will create new flows of telecommunications information between participating entities, and outside the CDR system. It will also facilitate telecommunications data being used in new ways, including uses that will result in telecommunications data being combined with consumer data from other CDR sectors. While this will create opportunities for innovation and consumer benefit, it may also

[1] See s 28A(2)(a) of the *Privacy Act 1988 (Cth)*, which outlines the 'monitoring related functions' of the Information Commissioner including in relation to the examination of proposed enactments.

[2] See ss 56BQ and 56BR of the *Competition and Consumer Act 2010 (Cth)*.

give rise to increased privacy risk. This risk has been demonstrated by recent data breaches in the telecommunications sector, in which the personal details of telecommunications customers have been disclosed. This highlights the need for review and appropriate implementation of:

- effective data minimisation policies and procedures
- data handling and retention practices that ensure that information is held securely
- data breach response plans, so that in the event of a data breach, affected consumers can be rapidly notified so they can take steps to limit the risk of harm from their personal information being accessed.

1.7 Providing a consistent, high level of protection under the *Competition and Consumer (Consumer Data Right) Rules* 2020 (the 'rules') is necessary given the sensitive nature of CDR data, but also for maintaining consumer confidence in the integrity of the CDR system, regardless of the CDR sector with which they engage.

1.8 The OAIC recommends Treasury conduct a Privacy Impact Assessment (PIA) in relation to the draft rules to identify privacy risks and how they can be mitigated. This PIA should inform the finalisation of the rules and standards. The OAIC has highlighted specific matters below that should be considered in the PIA.

1.9 We note a reference to a clause in this submission is a reference to a clause in Schedule 5 of the draft rules unless otherwise specified.

Part 2: About the OAIC and our role in the CDR system

2.1 The OAIC is Australia's independent regulator for privacy and freedom of information. The OAIC co-regulates the CDR system together with the Australian Competition and Consumer Commission (ACCC). The OAIC enforces the Privacy Safeguards contained in Part IVD of the CCA as well as the privacy and confidentiality related rules. In addition, the OAIC has a number of statutory advisory and guidance functions under the CDR framework. For example, the OAIC provides advice to the Minister and CDR agencies on the privacy implications of making rules and designating a potential sector,[3] recognising an external dispute resolution scheme,[4] and makes guidelines on the operation of the Privacy Safeguards.[5]

[3] The OAIC has a number of formal statutory functions under Part IVD of the *Competition and Consumer Act 2010 (Cth)* in relation to the making of rules and designation of a potential sector. For example, being consulted about the making of proposed rules and potential designated sectors (sections 56AD(3) and 56BQ), analysing the privacy impacts in relation to the making of proposed rules and potential sectors to be designated, when consulted (sections 56BR and 56AF), and producing a report about an instrument to designate a sector (section 56AF).

[4] Section 56DA(4) the CCA requires the Minister to consult with the Information Commissioner before recognising an EDR under s 56DA(1).

[5] Under section 56EQ, the Information Commissioner must make guidance for the avoidance of acts or practices that may breach the privacy safeguards.

2.2 The OAIC is also responsible for undertaking strategic regulatory and enforcement action in relation to the protection of privacy and confidentiality, as well as investigating individual and small business consumer complaints regarding the handling of their CDR data.

2.3 Our goal as regulator of the privacy aspects of the CDR system is to ensure that the system's robust data protection and privacy framework, and effective accountability mechanisms ensure consumers' CDR data (personal information) is protected.

Part 3: List of Recommendations

Operational Enhancements

Recommendations in relation to the business consumer amendments

(a) In relation to BCDCs, we recommend that Treasury consider further and conduct a PIA in relation to:

  (i) the types of data which are likely to be incorporated into business consumer data, whether it is likely to include personal or sensitive information, if any additional protections are required to respond to privacy and security risks that arise out of BCDCs

  (ii) the risks associated with unaccredited recipients of CDR data

  (iii) security and privacy impacts of BCDCs in relation to small business as consumers.[6]

(b) We recommend that Treasury give further consideration to whether the introduction of BCDCs may diminish the incentives and utility of CDR accreditation to provide business services.

(c) We recommend that Treasury give further consideration and undertake a PIA to assess the likely impacts of enabling CDR business consumers to extend use and disclosure consent durations to 7 years, and consider how any privacy risks may be addressed.

(d) Subrules 9.3(2) and (2A) should require accredited persons to record business consumer statements they or their CDR representative receive.

Recommendations in relation to CDR Representatives and OSPs

Record keeping and reporting

(a) CDR outsourcing arrangements and CDR representative arrangements should require OSPs and CDR representatives to:
  (i) keep records in relation to:

[6] For the avoidance of doubt, the OAIC is not proposing that business consumer disclosure consents should be allowed under the rules, but small businesses should be excluded from being able to give a business consumer disclosure consent, as that may give a competitive advantage to larger businesses.

(A) records of any matters that are required to be retained under Schedule 2[7]
(B) the review and assessment required under clause 1.6 of schedule 2 (which requires OSPs and CDR representatives to '*Implement a formal controls assessment program*')
(C) the plans, procedures and processes required under clause 1.7 of Schedule 2 (which requires OSPs and CDR representatives to '*Manage and report security incidents*') and the records that are required to be kept under clause 1.7(1) of Schedule 2 in relation to 'information security incidents'

(ii) provide the records referred to in (a)(i) to their principals and CDR principals, and records they would receive as a principal in a CDR outsourcing arrangement
(iii) periodically report on the matters referred to in (i) to their principals and CDR principals, and in relation to reports they would receive as a principal in a CDR outsourcing arrangement.

(b) Accredited principals and CDR principals should be required to keep the records referred to in (a)(i) and (ii) under rule 9.3.
(c) Accredited principals and CDR principals should be required to report on the matters referred to in (a)(iii) to the OAIC and ACCC under rule 9.4.

Notifications in relation to data security breaches or information security incidents

(d) CDR representative arrangements should require CDR representatives to notify their CDR principals of data security breaches or information security incidents. CDR outsourcing arrangements should require OSPs to notify their principals of data security breaches or information security incidents.
(e) The rules should make it clear that the notifications referred to in recommendation (d) would separately trigger the obligations of CDR principals and principals under Part IIIC of the ***Privacy Act 1988*** (Privacy Act) and clause 1.7 of schedule 2 to the rules.

Further recommendations in relation to OSPs

(a) At a minimum, OSPs arrangements should contain a requirement for OSPs to comply with Privacy Safeguards 2, 4, 9, 11, 12 and 13 as if they were accredited.
(b) Rule 9.3(2)(i) should be amended to capture an accredited person's direct and indirect OSPs.

Further recommendations in relation to CDR Representatives

(a) Rule 7.2 should include a requirement 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.
(b) Rule 9.3(2A) should require the CDR principal to keep records in relation to the direct and indirect OSPs of each of their CDR representatives.

[7] This mirrors the same requirement for ADRs in r 9.3(2)(l) and CDR principals in r 9.3(2A)(n).

Expansion to the telecommunications sector

Recommendations in relation to sensitive datasets

(a) Sensitive datasets should be excluded or otherwise dealt with by provisions in the designation instrument and failing that, the rules, not by the data standards.
(b) The following datasets should be clearly excluded from CDR data sharing in the CDR rules:
- where the CDR consumer or associate is making a communication, information relating to the destination of communications
- where the CDR consumer or associate is receiving a communication, information about the origin of communications
- data relating to 'over-the-top' services (e.g. WhatsApp, social media applications, streaming services) – to the extent that this data is held by carriers and carriage service providers (CSPs)
- information about a person's race or ethnic origin, religious beliefs, criminal history, or biometric information
- copies of or information in relation to identity verification documents, and
- information about a person's credit worthiness, including information from credit reporting agencies.

Recommendations in relation to Metadata

(a) Metadata should be defined in the rules to delineate the specific types of data that are to be excluded; and to the extent this is not accepted
(b) the rules should exclude specific types of metadata.

Recommendations in relation to hardship data

(a) Hardship data should only be included in the CDR when justified by reference to strong and compelling use cases, and where the extent of inclusion is clearly defined and readily apparent under the rules.
(b) The interaction between the designation instrument and the rules in relation to hardship data should be clearly expressed in the explanatory statement.

Recommendation in relation to account holders who are less than 18 years of age

The exclusion of 'account data or billing data in relation to a joint account or partnership account for which any of the individuals who are account holders is less than 18 years of age at that time' should be extended to all types of data listed under clause 1.3.

Recommendation in relation to sharing of CDR data relating to non-requesting CDR consumers

We recommend that Treasury consider how existing rule 4.12(3)(b) would apply in the telecommunications sector, and whether further enhancements (whether to rule 4.12(3)(b), or in the form of additional new rules) are required to mitigate against the privacy risks that may arise for non-requesting CDR consumers who are the subject of telecommunications CDR data.

Recommendations about cross sectoral data sharing

(a) The PIA should explore privacy risks associated with combining data from different sectors in the CDR and any sector-specific privacy risks for telecommunications, and that rules are made to mitigate these risks.

(b) Risks associated with cross sectoral data sharing should be monitored across the CDR system on an ongoing basis, including through rules maintenance.

Part 4: Operation enhancements

Business consumer disclosure consents

4.1 The draft rules propose to add a BCDC as a new category of consent to rule 1.10A(2). This consent will enable business consumers to consent to their CDR data being disclosed to a specified person, including to unaccredited persons.[8] A 'specified person' is not defined in the draft rules, however the explanatory materials note that specified persons may include unaccredited third parties, such as bookkeepers, consultants and other advisers who are not classified as trusted advisers under the current rules.[9]

4.2 The draft rules include certain requirements which must be met in order to enable such sharing of CDR data, including:

(a) an accredited person or CDR representative must take reasonable steps to confirm that the CDR consumer is not an individual, or that the business consumer has an active ABN[10]

(b) the accredited person or CDR representative must obtain a 'business consumer statement' from the CDR consumer, certifying that the consent is given for the purpose of enabling the accredited person or CDR representative to provide goods or services to the business consumer in its capacity as a business, not as an individual[11]

(c) an accredited person or CDR representative cannot make the giving of a BCDC or specification of a particular person for the purposes of such a consent a condition for the supply of goods or services requested by a business consumer[12]

(d) data standards are to be made about obtaining BCDCs to ensure the consumer is made aware that their data will leave the CDR system when it is disclosed.[13]

---

[8] Draft subrule 1.10A(8)(a).

[9] Explanatory Statement, *Competition and Consumer Act 2010 (Cth) Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2022, p2.*

[10] Draft subrule 1.10A(6).

[11] Draft subrule 1.10A(7).

[12] Draft subrule 1.10A(9).

[13] Draft subrule 8.11(1B).

4.3 Separately, Accredited Data Recipients (ADRs) and CDR representatives are also required to keep a record of the number of BCDC disclosures they make, the persons to whom the CDR data was disclosed, the steps taken to confirm the consumer is a business consumer[14] and the number of BCDC consents received during the reporting period.[15]

Risks in relation to business consumer disclosure consents

4.4 The exposure draft explanatory materials provide that the draft rules are intended to enable business consumers to have choice over who they share their data with and to provide a more comprehensive solution to support the participation of business consumers (particularly small businesses) and accounting platforms in the CDR.

4.5 The changes recognise the different circumstances under which business consumers operate, noting businesses often have existing relationships with service providers, such as software platforms, on which they rely to run their operations and with whom they need to share their information.[16] However, the proposed changes also raise some risks for CDR business consumers including that:

- personal information, including sensitive personal information, may be included in the disclosure of business CDR data
- unaccredited recipients of CDR data will not be subject to the protections in 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
- small businesses who are CDR consumers, may be vulnerable in many of the ways individual consumers are but their CDR data will not have the benefit of the same privacy and security protections as apply to consumers under the CDR.

4.6 In addition to the risks for CDR business consumers, there is a risk that BCDCs could act as a disincentive to become accredited in order to provide CDR-related business products and services. These risks are considered further below.

4.7 It is also unclear why business service providers (including accounting platforms) cannot become accredited or a CDR representative. We understand stakeholders have indicated that CDR obligations may conflict with other legal obligations. However, the CDR contains numerous provisions that enable participants to deal with CDR data as required by law. For example, Privacy Safeguard 6 allows a participant to use/disclose CDR data, and Privacy Safeguard 12 allows a participant to retain CDR data, if doing so is required or authorised by law or a court/tribunal order. In the absence of a clear and compelling rationale for this proposal, we consider the privacy risks may weigh against its introduction.

[14] Draft subrules 9.3(2)(ee) and (ef).

[15] Draft subrule 9.4(2)(viiia).

[16] Exposure Draft Explanatory Materials: Consumer Data Right rules - expansion to the telecommunications sector and other operational enhancements | Treasury.gov.au.

Risks associated with disclosing personal information

4.8 There is a risk that sharing business consumer CDR data may also result in the sharing of personal information, including sensitive personal information. We note the following examples.

(a) Data in relation to sole traders and small business owners is often a mix of personal and business-related data. A disclosure of the business' information for a business purpose may therefore be accompanied by a disclosure of personal information.

(b) An employee's personal and business use of a service may overlap. For example, data relating to business issued mobile phones can reveal business usage but also personal usage. Information about personal usage can also be derived (for example by analysing patterns of communication). Where such data is shared, it is likely that employees would also not be aware the businesses' CDR data, which contains their personal information, is being shared.

(c) Business data can include the personal information of customers. For example, a health service provider may share CDR data with their bookkeeper (as a specified person) for business purposes, but this may contain sensitive personal information relating to their clients.

4.9 While these are pre-existing issues, the efficiency and convenience of CDR data sharing may magnify the potential for harm in these scenarios.

4.10 To properly identify and mitigate those risks, we recommend a PIA be undertaken to examine the types of data which is likely to be incorporated into business consumer data and whether it is likely to include personal or sensitive information. The PIA should consider what, if any, additional controls are required to respond to privacy and security risks that arise out of the proposed changes, including whether any additional safeguards are required to protect the personal information of business consumers, their employees, customers, or other individuals whose personal information may be included in disclosures under a BCDC.

Risks in relation to unaccredited persons accessing CDR data

4.11 The explanatory materials note that under the proposal, the specified persons to whom CDR business data can be disclosed are likely to be bookkeepers, consultants, other advisers and a wide range of software providers who provide services to small businesses in Australia. These specified persons are not classified as 'trusted advisers' and are therefore not subject to the same professional regulatory standards. More generally, the introduction of BCDCs will remove the requirement for a person to be accredited, a CDR representative or a trusted adviser to receive business CDR data under the rules.

4.12 When disclosed to these specified persons, the CDR business data will lose the protections provided by the CDR. Data provided to our Office by the Australian Bureau of Statistics indicates small businesses (defined as having a turnover of 3 million or less)[17] comprised 95.2% of the 2,375,753 businesses trading in Australia. It is also the case that these small businesses are increasingly collecting, holding and handling personal information in connection with their

[17] S6D of the *Privacy Act 1988 (Cth).*

activities and in order to deliver their services.[18] Subject to some exceptions,[19] small businesses are currently not regulated under the Privacy Act and therefore the protections of the Privacy Act, including the Notifiable Data Breach scheme and the Australian Privacy Principles – which set out standards, rights and obligations in relation to the handling, holding, accessing and correcting of personal information – do not apply to the handling of this personal information.

4.13 Further, by implication, as these specified persons are not in the class of 'trusted advisers' they are not subject to other regulatory oversight. The lack of current regulatory oversight and experience of these potential recipients of CDR business data, means these entities may not have well developed processes and systems needed to responsibly deal with CDR data, implement appropriate security controls and respond to privacy or security incidents.

4.14 The lack of regulation of specified persons, either under the CDR, the Privacy Act, or through required professional accreditation, creates risks where personal or sensitive information is included in business CDR data. In these circumstances, for example, a specified person would not be obliged to limit their collection of sensitive personal information to that which is reasonably necessary for its functions or activities,[20] nor would they be required to take steps to protect any personal information they obtain from misuse, interference, loss, unauthorised access, modification or disclosure.[21] In the event of a data breach, the specified person would not be required to take steps to remedy the breach, nor be required to follow Notifiable Data Breach scheme protocols, such as notifying the Information Commissioner and the individuals concerned.

Risks in relation to small businesses as consumers

4.15 We note the following excerpts from the exposure draft explanatory materials in relation to BCDCs and small businesses:

> '*It will also allow disclosures to the wide range of software providers that offer important services to small businesses in Australia….*
>
> *This amendment is intended to provide a more comprehensive solution to support the participation of business consumers (particularly small businesses) and accounting platforms in the CDR*.'

4.16 We support efforts to make the CDR more useful for business consumers. However, we repeat our comments in paragraph 4.7 and note the proposed BCDC amendments may introduce risks to the security and privacy of small business consumers and their data. It is well known that small business consumers are vulnerable to a similar extent and in many of the same ways individual consumers are. For example, small business consumers dealing with larger service

[18] OAIC Submission to the Privacy Act Discussion Paper, December 2021, para 4.11.

[19] For example, health service providers, entities trading in personal information or credit providers: https://www.oaic.gov.au/privacy/privacy-for-organisations/small-business.

[20] Australian Privacy Principle 3.3 requires that the collection of the sensitive information must be reasonably necessary for one or more of the entity's functions or activities, and the individual about whom the sensitive information relates must consent to the collection.

[21] Privacy Safeguard 12 requires accredited data recipients of CDR data to ensure CDR data is protected from misuse, interference and loss, as well as from unauthorised access, modification or disclosure.

providers are subject to unequal bargaining power and often lack the resources to obtain legal, financial, or other forms of advice and adequately engage in dispute resolution processes or seek remedies in the event of a dispute.

This vulnerability suggests small businesses should receive a similar level of protection to that of individual CDR consumers.[22] However, BCDCs will enable small businesses to disclose their CDR data outside of the CDR where it will no longer be subject to the security and privacy protections of the CDR.

Risk of removing incentives to be accredited

4.17 Accredited persons are subject to various compliance obligations and restrictions in terms of their use of CDR data. Therefore, the introduction of BCDCs may put accredited persons at a competitive disadvantage, and disincentivise them from becoming accredited by allowing unaccredited persons to access CDR data and use it to provide business services without being subject to the same obligations and restrictions. For example, an unaccredited person will not be subject to the Schedule 2 security provisions in the rules and will be able to monetise the CDR consumer's CDR data in ways that would not be permitted under the rules, or without satisfying relevant requirements in the rules. We also repeat our comments in paragraph 4.7.

4.18 For the reasons noted above, we have made a number of recommendations below in relation to the risks raised by the introduction of BCDCs.

Durations of business consumer consents

4.19 The Exposure Draft proposes to extend the maximum duration of certain business consents from 12 months to 7 years for business CDR consumers. The extended consent arrangements apply to use and disclosure consents, but excludes collection, AP disclosure consents, direct marketing and de-identification consents. A consumer may still withdraw their consent at any time.

4.20 The draft rules have the potential to increase the complexity of the consent framework and to weaken the framework insofar as it extends to business consumers. Further, to the extent that business CDR data includes personal or sensitive information, the measure may remove or reduce a layer of protection an individual has over the security and privacy of their personal information. Allowing a consent to remain valid for 7 years may remove the prompt a person would otherwise have to reconsider their arrangements with an ADR and choose whether to renew their consent. Further it may not require the entity receiving the consent to consider whether they still have an active need for the consent.

4.21 Business consumers are still required to consent annually to the collection of CDR data; however, this does not necessarily mitigate the privacy risks associated with extending the duration of the other, more specific, consents. The CDR consent framework is designed to ensure consent is transparent and consumers understand what they are agreeing to and any potential consequences. The object of the CDR consent provisions is for consent to be

[22] For example, we understand this formed part of the reasoning for Treasury to extend the unfair contract protections to small businesses through the *Treasury Legislation Amendment (Small Business and Unfair Contract Terms) Act* 2015.

voluntary, express, informed, specific, **time limited** and easily withdrawn.[23] In our view there is the potential for a businesses' circumstances and CDR data to change substantially over a 7-year period and it is not clear that consent over that period of time could be considered current or time limited. We have included a recommendation on this point below.

Recording business consumer statements

4.22 As noted above, a business consumer statement enables a CDR business consumer to:

(a) give a BCDC such that the CDR business consumer's CDR data can be disclosed outside of the CDR

(b) extend the duration of use and disclosure consents to 7 years.

4.23 Because of the significance of this proposal, we consider the CDR system would benefit from a requirement to record these statements under rule 9.3, in addition to the existing requirements to record related consents.

Recommendations in relation to the business consumer amendments

(a) In relation to BCDCs, we recommend that Treasury consider further and conduct a PIA in relation to:

(i) the types of data which are likely to be incorporated into business consumer data, whether it is likely to include personal or sensitive information, if any additional protections are required to respond to privacy and security risks that arise out of BCDCs

(ii) the risks associated with unaccredited recipients of CDR data

(iii) security and privacy impacts of BCDCs in relation to small business as consumers.[24]

(b) We recommend that Treasury give further consideration to whether the introduction of BCDCs may diminish the incentives and utility of CDR accreditation to provide business services.

(c) We recommend that Treasury give further consideration and undertake a PIA to assess the likely impacts of enabling CDR business consumers to extend use and disclosure consent durations to 7 years, and consider how any privacy risks may be addressed.

(d) Subrules 9.3(2) and (2A) should require accredited persons to record business consumer statements they or their CDR representative receive.

[23] Rule 4.9.

[24] For the avoidance of doubt, the OAIC is not proposing that business consumer disclosure consents should be allowed under the rules, but small businesses should be excluded from being able to give a business consumer disclosure consent, as that may give a competitive advantage to larger businesses.

OSPs and CDR representatives

Concerns in relation to further outsourcing arrangements and chains of OSPs

4.24 We understand that further outsourcing arrangements are already permitted by the rules. The draft rules seek to '*clarify 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 OSPs engaged by CDR representatives*'.[25] We support efforts to clarify and strengthen the OSP provisions, as the complexity of the existing provisions may be a compliance obstacle for participants and may therefore raise privacy and security risks for CDR consumers.

4.25 However, additional risks arise from the increasing degrees of separation between a principal and its OSP and particularly where the OSP is engaged by the principal's CDR representative. This increasing separation may also weaken the enforcement framework that underpins the CDR, noting the OAIC and ACCC do not have direct regulatory oversight under the CDR provisions and under the Privacy Act (if they are exempt) in relation to CDR representatives and OSPs. Indirect OSPs are also likely to have limited knowledge and understanding of the CDR and as a result there is a higher possibility they could unintentionally and unknowingly breach CDR obligations.

Concerns in relation to CDR representatives engaging OSPs

4.26 The draft rules remove the prohibition on CDR representatives engaging OSPs. We note CDR representatives were introduced in the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021*, commonly known as the 'version 3' rules to:

- '*facilitate greater participation in the CDR regime by participants*'
- enable '*unaccredited persons to provide goods and services to consumers using CDR data in circumstances where they are in a CDR representative arrangement with an unrestricted accredited person who is liable for them*'.[26]

4.27 The version 3 rules prohibited CDR representatives from engaging an OSP or directly disclosing CDR data to an OSP.[27] We understand part of the reason for this prohibition was that it would require a CDR representative to work more closely with its CDR principal by engaging OSPs through their principal. As a result, the CDR representative would be more likely to comply with the rules by leveraging the resources and expertise of the CDR principal (a person with unrestricted accreditation). By removing this prohibition and thereby reducing the connection between a CDR representative and a CDR principal in respect of OSP arrangements, the OAIC is concerned that this measure has the potential to create privacy and security risks for

[25] Explanatory statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021*, available here: https://www.legislation.gov.au/Details/F2021L01392/Replacement%20Explanatory%20Statement/Text.

[26] Explanatory statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021*, available here: https://www.legislation.gov.au/Details/F2021L01392/Replacement%20Explanatory%20Statement/Text.

[27] See current rule 1.10AA(2)(c). We also note the explanatory statement says '…a CDR representative is able to disclose CDR data as if it is an accredited person. The only exception to this is that a CDR representative cannot disclose CDR data to an outsourced service provider.'

consumers. There is a question about the extent to which CDR principals can, in practice, be responsible for, or control, the actions of multiple layers of a CDR representative's contractors and subcontractors.

4.28 We also note '*any use or disclosure of service data by a direct or indirect OSP of… a CDR representative of [an] accredited data recipient… is taken to have been by the accredited data recipient*'.[28] This appears to support the requirement for CDR representatives to engage OSPs through their CDR principal.

4.29 However, we understand there is a need to balance this risk with the stakeholder feedback noted by the Treasury:

> *'that entities that rely on third parties to help them manage data currently have difficulty functioning in the CDR due to the prohibition on CDR representatives in engaging OSPs'.*

Any implementation in this respect should occur with caution and subject to appropriate safeguards.

Recommendations in relation to OSPs and CDR representatives

Additional reporting and record keeping requirements

4.30 Further to the concerns raised above, the OAIC and ACCC only have direct regulatory oversight over accredited persons and not their OSPs or CDR representatives under the CDR provisions and under the Privacy Act (if they are exempt). This creates significant barriers to the ability of CDR regulators to promote compliance among OSPs and CDR representatives.

4.31 We note draft rules 1.10(2)(b)(i) and 1.10AA(4)(b) require OSPs and CDR representatives to 'take the steps in Schedule 2 to protect the service data as if it were the' principal or CDR principal respectively. This mirrors current rules 1.10(2)(b)(i) and 1.10AA(2)(ii). We note these obligations originate in contract and not in CDR legislation, and therefore OSPs and CDR representatives are not directly regulated by the OAIC (unless they happen to be subject to the Privacy Act) and ACCC.

4.32 We propose OSPs / CDR representatives should be obliged to keep records and regularly report to their principals / CDR principals in relation to their obligations under clauses 1.6 and 1.7 of Schedule 2. This should be accompanied by equivalent record keeping and reporting obligations for their principals / CDR principals under rules 9.3 and 9.4.

4.33 The additional reporting requirements would better enable the OAIC and ACCC to actively monitor the compliance of OSPs and CDR representatives. Rule 9.6 would allow the OAIC and ACCC to have access to the additional records and therefore strengthen their ability to monitor and investigate non-compliance in relation to OSPs and CDR representatives, and take enforcement action against accredited persons where appropriate.

[28] Exposure draft rule 7.6(2).

Notifications in relation to CDR data security breaches and information security incidents

4.34 Schedule 2, clause 1.7 require OSPs and CDR representatives to '*create and maintain plans to respond to information security incidents that it considers could plausibly occur (CDR data security response plans)*.' These '*response plans must include procedures for…*

> *(b) notifying CDR data security breaches to the Information Commissioner and to CDR consumers as required under Part IIIC of the Privacy Act 1988; and*
>
> *(c) notifying information security incidents to the Australian Cyber Security Centre as soon as practicable and in any case no later than 30 days after the accredited data recipient becomes aware of the security incident.'*

4.35 The OAIC recommends CDR representative arrangements require CDR representatives to notify their CDR principals of data security breaches or information security incidents. Similarly, we recommend CDR outsourcing arrangements require OSPs to notify their principals of the same. We recommend the rules make it clear that such notifications would separately trigger the obligations of CDR principals and principals under Part IIIC of the Privacy Act and clause 1.7 of schedule 2 to the rules. This will support CDR principals to comply with their CDR obligations in respect of CDR representatives and OSPs. It would also better enable the OAIC and ACCC to investigate and/or take enforcement action in relation to accredited persons, where they, or their OSPs, CDR representatives or OSPs of their CDR representatives have not notified consumers, the Information Commissioner and regulatory bodies as required by Part IIIC of the Privacy Act and clause 1.7 of Schedule 2 to the rules.

Recommendations in relation to OSPs and CDR representatives

4.16 For the reasons noted above, we make the following recommendations in relation to OSPs and CDR representatives.

Recommendations in relation to CDR Representatives and OSPs

Record keeping and reporting

(a) CDR outsourcing arrangements and CDR representative arrangements should require OSPs and CDR representatives to:
  (i) keep records in relation to:
    (A) records of any matters that are required to be retained under Schedule 2[29]
    (B) the review and assessment required under clause 1.6 of schedule 2 (which requires OSPs and CDR representatives to '*Implement a formal controls assessment program*')
    (C) the plans, procedures and processes required under clause 1.7 of Schedule 2 (which requires OSPs and CDR representatives to '*Manage and report security incidents*') and the records that are required to be kept under clause 1.7(1) of Schedule 2 in relation to 'information security incidents'

[29] This mirrors the same requirement for ADRs in r 9.3(2)(l) and CDR principals in r 9.3(2A)(n).

(ii) provide the records referred to in)(a)(i) to their principals and CDR principals, and records they would receive as a principal in a CDR outsourcing arrangement
(iii) periodically report on the matters referred to in (i) to their principals and CDR principals, and in relation to reports they would receive as a principal in a CDR outsourcing arrangement.

(b) Accredited principals and CDR principals should be required to keep the records referred to in (a)(i) and (ii) under rule 9.3.
(c) Accredited principals and CDR principals should be required to report on the matters referred to in (a)(iii) to the OAIC and ACCC under rule 9.4.

Notifications in relation to data security breaches or information security incidents

(d) CDR representative arrangements should require CDR representatives to notify their CDR principals of data security breaches or information security incidents. CDR outsourcing arrangements should require OSPs to notify their principals of data security breaches or information security incidents.
(e) The rules should make it clear that the notifications referred to in recommendation (d) would separately trigger the obligations of CDR principals and principals under Part IIIC of the ***Privacy Act 1988*** (Privacy Act) and clause 1.7 of schedule 2 to the rules.

Further recommendations in relation to OSPs

4.36 We note the explanatory materials indicate:

> *'Consideration is being given to whether:… the CDR Rules should be further amended to ensure that, under a CDR outsourcing arrangement, OSPs are required to comply with relevant privacy safeguards'.*

4.37 At a minimum, we consider OSP arrangements should contain a requirement for OSPs to comply with Privacy Safeguards 2, 4, 9, 11, 12 and 13 as if they were accredited. We recommend that Treasury give further consideration to whether, or to what extent, OSPs should be required to comply with the remaining Privacy Safeguards without creating undesirable overlaps with the coverage of the Privacy Safeguards in relation to their principals.

4.38 We also support the proposed amendments to rules 7.2(4)(f) and (i) such that they now capture direct and indirect OSPs. We understand that under the current rules, further outsourcing arrangements (i.e. indirect OSPs) were not captured by these provisions. However, we understand current r 9.3(2)(i) also does not capture further outsourcing arrangements nor do the draft rules. An accredited person's inability to keep records in relation to indirect OSPs would challenge the accredited person's ability to ensure its chains of OSPs will comply with their obligations.

Further recommendations in relation to OSPs

(a) At a minimum, OSPs arrangements should contain a requirement for OSPs to comply with Privacy Safeguards 2, 4, 9, 11, 12 and 13 as if they were accredited.

(b) Rule 9.3(2)(i) should be amended to capture an accredited person's direct and indirect OSPs.

Further recommendations in relation to CDR representatives

4.39 We note draft subrule 4.20E(3)(k) & (l) requires:

> *'(3) When asking a CDR consumer to give consent, the CDR representative must give the CDR consumer the following information:*
>
> *…*
>
> *(k) if the CDR data may be disclosed to, or collected by, a direct or indirect OSP (including one that is based overseas) of the CDR representative or of the CDR principal—a statement of that fact; and*
>
> *(l) a statement that the CDR consumer can obtain further information about the collections or disclosures for which consent is requested from the CDR principal's CDR policy if desired'*

4.40 We therefore welcome the exposure draft rules requiring at r 7.2(4)(f) for the CDR principal's CDR policy to include 'a list of the direct and indirect OSPs… of any CDR representative (whether based in Australia or based overseas, and whether or not any is an accredited person)'. However, r 7.2(4)(i) only requires the CDR principal's policy to contain details about the countries the CDR principal may disclose to when making a disclosure to an unaccredited direct or indirect OSP. We recommend a requirement is added so that the CDR principal's CDR policy contains details about the countries the CDR principal's CDR representatives may disclose to when making a disclosure to an unaccredited OSP.

4.41 Further to our recommendation that r 9.3(2)(i) should require accredited persons to keep records in relation to direct and indirect OSPs, we also recommend rule 9.3(2A) is also expanded to require the CDR principal to keep records on the direct and indirect OSPs of each of their CDR representatives. An accredited person's inability to do this would challenge the accredited person's ability to ensure its CDR representative and the CDR representative's chains of OSPs comply with their obligations.

Further recommendations in relation to CDR Representatives

(a) Rule 7.2 should include a requirement 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.
(b) Rule 9.3(2A) should require the CDR principal to keep records in relation to the direct and indirect OSPs of each of their CDR representatives.

Requests in relation to Privacy Safeguards 11 and 13

4.42 We understand there are practical issues that arise in relation to consumer requests for the correction of CDR data made under Privacy Safeguard 11 (quality of CDR data) and that continued work is being undertaken to address these issues. As an interim measure, we support the amendments that allow ADRs and data holders to provide optional functionality through consumer dashboards for consumers to make requests under Privacy Safeguard 11 (draft rules 1.14(2A)(b) and 1.15(2AA)). At paragraph 96 of the exposure draft explanatory materials, Treasury requests feedback on whether 'it would be helpful if data holders could also allow consumers to make requests for the purposes of Privacy Safeguard 13 on their consumer dashboards'. We support this as a further measure for data holders but suggest the same optional functionality should be extended to ADRs as well.

Part 5: Telecommunications rules

Scope of required and voluntary consumer data in the telecommunications sector

Further refinement and specification of datasets in the data standards

5.1 We note the exposure draft explanatory materials indicate a broad range of telecommunications data will be within scope of the CDR:

> *' The Amending Rules define telecommunications data sets by means of **broad descriptors**, combined with minimum inclusions of key data. This approach allows flexibility for further refinement and specification of data sets in the data standards.'*

5.2 The OAIC supports further refinement and specification of datasets in the data standards in relation to datasets that are not sensitive. However, our view is that provisions that exclude or otherwise deal with sensitive datasets should be detailed in the designation instrument, and if not the designation instrument, the rules and not in the standards. This is because:

(a) of the risk of harm posed by these datasets to consumers
(b) the standards are more technical and less suited to dealing with sensitive legal issues
(c) of the lower levels of consultation that standards development and amendments are subject to in comparison to the designation instrument and the rules.

5.3 This is consistent with Treasury's final report on the telecommunications sectoral assessment[30] which states:

> '*The rules will specify the datasets that are required to be shared with more specificity and within the bounds of designation*',

and references are made throughout the report to the rules setting the boundaries of CDR data in the telecommunications sector.

Sensitive telecommunication datasets in the CDR

5.4 The rules and designation instrument capture a broad range of data and appear to include sensitive datasets which may cause or risk harm to consumers. The Information Commissioner expressed similar concerns in her submission to the sectoral assessment consultation[31] and report on the draft Consumer Data Right (Telecommunications Sector) Designation (the designation report).[32]

5.5 These sensitive datasets may include:

(a) where the CDR consumer is making a communication, information relating to the destination of communications
(b) where the CDR consumer is receiving a communication, information about the origin of communications
(c) data relating to 'over-the-top' services (e.g. WhatsApp, social media applications, streaming services) – to the extent that this data is held by carriers and CSPs[33]
(d) information about a person's race or ethnic origin, religious beliefs, or criminal history, or biometric information[34]
(e) copies of identity verification documents[35]

[30] Available here: https://treasury.gov.au/sites/default/files/2021-11/p2021-225262.pdf.

[31] See in particular pages 4 and 5 of this submission, available at https://treasury.gov.au/consultation/c2021-198050-tc.

[32] See in particular part 2 and 3 of this report, available at https://www.oaic.gov.au/engage-with-us/submissions/report-on-the-draft-consumer-data-right-telecommunications-sector-designation-2021.

[33] There is evidence that carriers and CSPs may, in some circumstances, hold some information about a customer's use of 'over the top' services– for example, when the application in question is owned on run by the carrier (see https://www.optus.com.au/about/legal/privacy#the-type-of-information-we-collect-about-you). Providers may also hold information about the use of over-the-top services where the provider bundles carriage services with other products delivered via over-the-top applications, such as television streaming or gaming products. Further, under section 187AA of the Telecommunications (Interception and Access) Act 1979, carriers and CSPs have data retention obligations with respect to the 'type of communication' made by a consumer. The legislation points to social media, emails and forums as examples of 'type[s] of communication' that are subject to the data retention regime – suggesting (but not confirming) that some information about a customer's use of 'over the top' services may be held by carriers and CSPs.

[34] See, for example: https://www.vodafone.com.au/about/legal/privacy; https://www.optus.com.au/about/legal/privacy; https://www.telstra.com.au/privacy#info-collect.

[35] We note that government related identifiers may be present in these documents and this heightens the privacy risk to consumers, particularly in the event of a data breach.

(f) information about a person's credit worthiness, including information from credit reporting agencies.

5.6 These datasets can reveal granular and confidential information about a consumer and third parties (for example the recipients of communications, other members of the consumer's household and non-account holder users for an account). The datasets can be used for identity purposes and therefore expose consumers to the risk of identity theft. This is particularly pertinent in view of the recently added pathways to CDR participation whereby unaccredited persons who are not directly regulated by the CDR provisions and Privacy Act (if they are exempt) can receive and handle CDR data. Further, depending on the data source, some of these information types may not necessarily be correct or subject to robust quality assurance processes.

5.7 For these reasons, the OAIC recommends these datasets should be clearly excluded under the rules.

Recommendations in relation to sensitive datasets

(a) Sensitive datasets should be excluded or otherwise dealt with by provisions in the designation instrument and failing that, the rules, not by the data standards.
(b) The following datasets should be clearly excluded from CDR data sharing in the CDR rules:
- where the CDR consumer or associate is making a communication, information relating to the destination of communications
- where the CDR consumer or associate is receiving a communication, information about the origin of communications
- data relating to 'over-the-top' services (e.g. WhatsApp, social media applications, streaming services) – to the extent that this data is held by carriers and CSPs
- information about a person's race or ethnic origin, religious beliefs, criminal history, or biometric information
- copies of or information in relation to identity verification documents, and
- information about a person's credit worthiness, including information from credit reporting agencies.

5.8 We make further observations and recommendations in relation to sensitive data types below.

Customer data

5.9 Clause 1.3, item 1(a) defines customers as '*information that identifies or is about the person'*. We understand this, and the subitems contained in item(1)(b), could include the sensitive datasets referred to in paragraph 5.5 above and that their inclusion is not supported by strong and tangible applications (e.g. information about an identifiable person's race or ethnic origin, religious beliefs, criminal history, health information that is not relevant to a telecommunications product). Given the inherent sensitivity of these datasets, we repeat the recommendation above, that they be excluded from the CDR unless there are strong and tangible applications justifying inclusion, in which case these applications should be referenced in the explanatory statement. This will increase privacy protection for sensitive

telecommunications data and facilitate participant and consumer certainty about sensitive data types that must not be shared under CDR.

Metadata

5.10 For the reasons outlined in the Information Commissioner's submission to the CDR sectoral assessment,[36] the OAIC supports the exclusion of metadata under clause 3.2(4)(b). However, we note that 'metadata' is not defined for the purposes of 3.2(4)(b) and that some of the data listed under clause 1.3 may capture data that is metadata. For example, under:

- item 3(a)(v), billing data captures '*details of usage*'
- item 5, usage data captures '*information about the use of the relevant product and includes the following data about the relevant product:*
  (i) for a relevant product that includes voice calls—the number and duration of the calls;
  (ii) for a relevant product that includes a short message service (SMS)—the data usage of the SMS and the number of SMS messages;
  (iii) for a relevant product that includes data—the data usage.'

5.11 For clarity, and to avoid a possible conflict between the data included under clause 1.3 and data excluded under clause 3.2(4)(b), the OAIC recommends that metadata or specific types of metadata that are to be exclude should be clearly defined in the rules. This definition should have regard to the risks raised in the Information Commissioner's submission to the CDR sectoral assessment[37] Noting these risks, the OAIC would be welcome further engagement with Treasury on this issue.

Recommendations in relation to Metadata

(a) Metadata should be defined in the rules to delineate the specific types of data that are to be excluded; and to the extent this is not accepted
(b) the rules should exclude specific types of metadata.

5.12 Delineation of these datatypes would clarify that the exclusion of metadata would cover, for example, data in relation to:

(a) where the CDR consumer is making a communication, information relating to the destination of communications[38]
(b) where the CDR consumer is receiving a communication, information about the origin of communications.[39]

[36] In particular, see section titled '*Information required to be retained under the Interception Act ('metadata')*'.

[37] Ibid.

[38] This may include the CDR consumer's browser history, or in relation to the recipient of a communication, their phone number or location information that is not associated with a mobile product.

[39] This may include the IP address of a website user or in relation to a person making a phone call, their phone number or location information that is not associated with a mobile product.

5.13 As outlined in the recommendations in relation to sensitive datasets, the OAIC strongly recommends this information be explicitly excluded. This information can reveal granular and sensitive information about a consumer. For example, if a consumer frequently called a specific health service provider or regularly visited a webpage for a particular health clinic, this could reveal information about the consumer's health.

Hardship, concession, accessibility, and similar types of data

5.14 Account data is defined under clause 1.3, item 2 as 'information that identifies or is about the operation of the account'. Item 2(c) excludes 'information about whether the account is associated with a hardship program'.

5.15 This mirrors the exclusion of hardship data in the energy sector. Based on how hardship information was excluded from data sharing in the energy sector, we understand that billing information would not reveal whether the consumer is a part of a hardship program and under which circumstances. However, there appears to be a risk that hardship data can be captured under the other types of telecommunications data listed in clause 1.3. For example, hardship data could be captured as:

(a) customer data under item 1 where it relates to a customer's eligibility for a particular product
(b) concession information under item 2(b)(iv)
(c) accessibility information under 4(b)(vii).

5.16 In particular, we note the overlap between the hardship exclusion and concession information also occurs in schedule 4 in relation to the energy sector. The OAIC is aware of some instances where this has given rise to confusion about the extent to which these datasets are included in or excluded from the CDR.

5.17 As noted in the designation report, inclusion of hardship data could support compelling applications that help consumers experiencing hardship or vulnerability to secure telecommunications products and services that best serve their specific requirements. However, information about hardship and vulnerability is particularly sensitive. Given the inherent sensitivity of this type of information, its inclusion, or the extent of its inclusion under the rules, should be clear. If hardship data is to be totally excluded from the CDR for the telecommunications sectors, we recommend the exclusion applies to all types of data at clause 1.3 and not just account data. To the extent that it is intended to be included in the CDR, it should only be included where justified by reference to strong and compelling use cases, and where the extent of inclusion is clearly defined and readily apparent under the rules.

5.18 Finally, we note that in contrast to hardship data being excluded from account data under the rules, the designation instrument intentionally captures hardship data because of use cases raised in the associated consultation.[40] To avoid doubt, we make the following recommendation.

[40] See the Explanatory statement for the Consumer Data Right (Telecommunications Sector) Designation 2022 under the heading 'Section 8 – information about products'.

Recommendations in relation to hardship data

(a) Hardship data should only be included in the CDR when justified by reference to strong and compelling use cases, and where the extent of inclusion is clearly defined and readily apparent under the rules.
(b) The interaction between the designation instrument and the rules in relation to hardship data should be clearly expressed in the explanatory statement.

Exclusion of account and billing data where an account holder is less than 18 years of age

5.19 Clause 3.2(4)(a)(ii) excludes 'account data or billing data in relation to a joint account or partnership account for which any of the individuals who are account holders is less than 18 years of age at that time'. We recommend this exclusion extends to all types of data listed under clause 1.3. For example, usage data in relation to an account holder that is under 18 may be at least as sensitive as account or billing data.

Recommendation in relation to account holders who are less than 18 years of age

The exclusion of 'account data or billing data in relation to a joint account or partnership account for which any of the individuals who are account holders is less than 18 years of age at that time' should be extended to all types of data listed under clause 1.3.

Historical data

5.20 The draft rules provide that data relating to closed accounts is not required consumer data except in certain limited circumstances set out in clauses 3.2(5) – (6) of Schedule 5.

5.21 We note recent data breaches in the telecommunications sector have raised significant privacy concerns about the storage of historical data.[41] These breaches have highlighted the privacy risk associated with data holders retaining potentially sensitive telecommunications data for periods of time and when it may no longer be necessary.

5.22 The inclusion of historical telecommunications information in the CDR system creates added privacy risk by increasing the scope and volume of data that can be requested and shared.[42] Historical data may also be less relevant and useful to consumers in the CDR system. Accordingly, we recommend that historical data should only be included in the CDR system if the information is likely to be useful to consumers.

5.23 The draft rules are consistent with the recommendation in the designation report that data holders should not be required to retain data for any longer than required under the data

[41] ABC News, 'Past Optus customers have had their data exposed – why did the company still have it?' <https://www.abc.net.au/news/science/2022-10-02/why-is-optus-keeping-customer-data-for-so-long/101491200>.

[42] See pages 13 of the Designation report.

retention scheme in the *Telecommunications (Interception and Access) Act 1979* (TIA Act).[43] The OAIC supports the amendments and maintains the position that data should not be retained where it is no longer required.

External Dispute Resolution

5.24 Clause 4.2 sets out the external dispute resolution (EDR) processes for the telecommunications sector, subject to a notifiable instrument being made.

5.25 Under the draft rules, data holders who are carriage service providers must be members of the Telecommunications Industry Ombudsman. Accredited persons must be members of the Australian Financial Complaints Authority (AFCA).

5.26 We appreciate that having two EDR schemes helps to align with existing processes in the telecommunications sector and is also consistent with the approach taken in the energy sector.

5.27 However, as the CDR is extended to more sectors and more EDRs are introduced into the system, it is important to acknowledge the heightened risk of confusion for consumers and participants in relation to EDR schemes. It is important that CDR participants give consumers clear information about which EDR they should approach in relation to a CDR complaint and how they can access the relevant EDR schemes. We would support ongoing monitoring in relation to the effectiveness of CDR EDR framework, taking issues such as accessibility and efficiency into account.

Sharing CDR data of non-requesting CDR consumers

5.28 It appears that an account holder may initiate a consumer data request in relation to the telecommunications CDR data of non-requesting users of the account. For example:

(a) the account holder of a household account could initiate a consumer data request in relation to the telecommunications CDR data of other members of a household
(b) a landlord could initiate a consumer data request in relation to the telecommunications CDR data of tenants
(c) an employer could initiate a consumer data request in relation to the telecommunications CDR data of employees.

5.29 While we recognise that account holders may already be able to access sensitive data about third party users through existing methods outside of the CDR (e.g. through bills), there are still considerable privacy risks associated with the sharing of this data in a CDR context. Notably, notice and consent are key mechanisms through which privacy and confidentiality are protected in the CDR, and yet under current arrangements there would be no requirement for a thirdparty user to be notified of, or consent to, the sharing of data about them at the request of the account holder. The CDR also enables sharing of data in a digital format, which could enable recipients to use and aggregate third party data new ways. This could reveal more detailed and granular insights into third party product use. We therefore consider caution

[43] See pages 13–14 of the Designation report.

should be exercised in relation to any proposal or risk that the CDR could be used to share CDR data of non-requesting CDR consumers with only the account-holder's knowledge and consent.

5.30 This is a matter the OAIC has previously raised in the context Treasury's CDR Energy Rules (Version 4 Rules) consultation.[44] We understand that CDR Rule 4.12(3) provides some protection to third parties by prohibiting an accredited person from asking for a consent to use CDR data *for the purpose of* identifying, compiling insights in relation to, or building a profile in relation to an identifiable person who is not the requesting CDR consumer. However, this rule alone may not be sufficient to protect third party account users from privacy risks associated with CDR data sharing. For example, it appears rule 4.12(3) would not prohibit an ADR from using CDR data in a way that results in a person being identified, provided this was not *the purpose of the use*. Additionally, rule 4.12(3) does not appear to cover situations where a CDR consumer seeks to compile insights in relation to an identifiable individual, but the accredited person has no such purpose.

Recommendation in relation to sharing of CDR data relating to non-requesting CDR consumers

We recommend that Treasury consider how existing rule 4.12(3)(b) would apply in the telecommunications sector, and whether further enhancements (whether to rule 4.12(3)(b), or in the form of additional new rules) are required to mitigate against the privacy risks that may arise for non-requesting CDR consumers who are the subject of telecommunications CDR data.

Cross sectoral data sharing

5.31 Combining consumer's CDR data across designated sectors can allow richer and more granular insights to be derived about individual CDR consumers and their associates.[45] While this can have benefits for consumers in receiving services that suit their needs, it may also increase the privacy risks for consumers and associates participating in the CDR.

5.32 Existing privacy, confidentiality and security requirements in the existing CDR rules and data standards create a strong foundation to protect consumers' information. However, it is important that the cumulative privacy and security risk associated with combining datasets from multiple sectors is closely monitored as CDR is applied to new sectors in the economy, including the telecommunications sector.

5.33 The Designation report recommended that a thorough analysis should occur when telecommunications-related rules are made to ensure that the CDR operates as intended and any privacy risks arising from combining cross-sectoral data in new ways are adequately addressed.[46] We repeat recommendation 9 from the report and further recommend that risks associated with cross sectoral data sharing should be monitored across the entire CDR system

[44] See part 5 of the OAIC's Submission to Treasury's CDR Energy Rules (Version 4 Rules) Consultation.

[45] For further information, see Information Commissioner's telecommunications report, page 16.

[46] Designation report, page 16.

on an ongoing basis and as the CDR expands into new sectors, we suggest this is a matter which could be considered as part of rules maintenance.[47]

Recommendations about cross sectoral data sharing

(a) The PIA should explore privacy risks associated with combining data from different sectors in the CDR and any sector-specific privacy risks for telecommunications, and that rules are made to mitigate these risks.

(b) Risks associated with cross sectoral data sharing should be monitored across the CDR system on an ongoing basis, including through rules maintenance.

Staged implementation

5.34 We support the staged application of the CDR to data holders based on their ability and capacity to develop compliant CDR systems that offer sufficient privacy protections for consumers. Industry participants have strongly recommended that sufficient time is provided for data holders to develop systems and processes to meet their CDR obligations (including in relation to privacy). We support the development of a staged application schedule that provides sufficient time for data holders to prepare for and meet their CDR obligations.

5.35 We note that following the implementation of the mandatory data retention scheme under the TIA Act, service providers were given 18 months to upgrade their systems to meet the retention and encryption requirements under the mandatory data retention scheme (see Division 2 of Part 5-1A). To the extent that information covered by the mandatory data retention regime is included in CDR data sharing (and particularly if any metadata is included), we recommend that Treasury carefully consider the interaction between the TIA Act and the CDR, and ensure the timeframe for implementation of the CDR is adequate for data holders to comply with all security and privacy obligations applicable to them.

[47] Consumer Data Right - CDR Rules Maintenance.