



Consumer
Data Right



Australian Government
The Treasury

DATA
STANDARDS
BODY

Consumer Data Right in the telecommunications sector

CDR rules and standards design paper

1 March 2022

Opportunity to provide feedback

This paper is designed to obtain feedback in order to develop draft CDR rules and standards. Draft CDR rules and standards will be the subject of formal consultation at a later stage, with the opportunity to make formal submissions.

You are invited to provide informal feedback to the Treasury and Data Standards Body by **5 April 2022** through either:

- lodging comments on the public [GitHub repository](#) maintained by the Data Standards Body; or
- by email to Treasury at data@treasury.gov.au. Respondents who would like to provide feedback on a confidential basis should ensure that this is clearly indicated.

Feedback posted on GitHub is public by nature at the time of submission. Content posted on GitHub should be made according to the community engagement rules published by the Data Standards Body.

During the consultation period, Treasury will also host an online forum to provide stakeholders with an opportunity to raise questions and discuss any feedback.

Table of Contents

Context and purpose.....	3
Telecommunications sector Data Holders.....	5
Role of the data standards and relevant artefacts	6
1. Scope of data sharing in the telecommunications sector.....	8
1.1. Topic Overview	8
1.2. Rules considerations	8
Which data holders should be required to share CDR data?	8
What products and what product-related datasets are in scope?	9
What is required data sharing?	11
Reciprocal data sharing obligations for certain ADRs	15
1.3. Standards considerations.....	16
Technical standards considerations	16
Consumer experience considerations	17
2. ‘Eligible CDR consumers’ in the telecommunications sector.....	18
2.1. Topic overview	18
2.2. Rules considerations	18
Users without online access	20
Enterprise customers interaction with CDR	20
2.3. Standards considerations.....	21
Technical standards considerations	21
Consumer experience considerations	21
3. Other design issues for the telecommunications sector	23
3.1. Rules considerations	23
White labelled products	23
Internal dispute resolution requirements	24
External dispute resolution requirements	25
3.2. Standards considerations.....	25
Technical standards considerations	25
Consumer experience considerations	26
3.3. Implementation considerations.....	26
Staged implementation	26

Part A – Overview

Context and purpose

1. On 24 January 2022, the Minister for Superannuation, Financial Services and the Digital Economy, Senator the Hon Jane Hume, (the **Minister**) formally extended the Consumer Data Right (**CDR**) regime to the telecommunications sector via a designation instrument. The designation instrument specifies the telecommunications data holders – carriers and carriage service providers (**CSPs**) – and data sets to which CDR applies.¹
2. The designation instrument does not enliven data sharing obligations for data holders and amendments to the *Competition and Consumer (Consumer Data Right) Rules 2020 (CDR Rules)* and Consumer Data Right Standards will ultimately specify what designated data is required to be shared, by whom and when.
3. This paper seeks feedback on the design and principles to support the development of recommended amendments to the CDR rules and standards to implement the CDR in the telecommunications sector:
 - a. The rules will determine the scope of data sharing requirements for data holders, the scope of consumers that will be eligible to share data and other requirements; and
 - b. The standards will specify the technical and consumer experience requirements for the development of suitable Application Programming Interfaces (**APIs**) including data language standards used to describe data clusters and permissions.
4. The CDR is an economy-wide regime that uses sector-agnostic rules and standards in relation to the above matters wherever possible. With the CDR extending to a third sector, there will be more opportunities for consumers to benefit from innovative cross-sectoral use cases.
5. The existing CDR rules and standards include requirements that will apply to the telecommunications sector, as outlined below:
 - **General provisions relating to data holders and to accredited data recipients:** Set out requirements for product and consumer data request services, services for managing consumer data requests made by accredited data recipients, obligations relating to CDR outsourcing and representative arrangements, and deletion and de-identification of CDR data.
 - **Product data requests:** Set out requirements for disclosing product data (i.e. product information) in response to product data request, refusal to disclose required product data in response to product data request and use of data disclosed pursuant to product data request.

¹ The Designation Instrument is available online at: <https://www.legislation.gov.au/Series/F2022L00068>.

- **Consumer data requests made by eligible CDR consumers:** Set out requirements for disclosing consumer data in response to a valid consumer data request and refusal to disclose required consumer data in response to consumer data request.²
 - **Joint accounts:** Set out requirements for disclosure options and consumer data requests that relate to joint accounts.
 - **Rules relating to accreditation for recipients of consumer data:** Set out requirements for applying to be an accredited data recipient, consideration of applications to become accredited data recipients, obligations of those recipients, transfer, suspension, surrender and revocation of accreditation, and rules relating to the Register of Accredited Persons.
 - A ‘data minimisation principle’ also applies to accredited data recipients. Accredited data recipients can only collect and use CDR data that is reasonably needed for the provision of the good or service that the consumer has consented to and cannot seek to collect CDR data that relates to a longer time period than is reasonably needed.
 - **Consumer data requests made by accredited data recipients:** Set out requirements for consumer data requests made by accredited data recipients to CDR participants, including giving and amending consents, and authorisations to disclose CDR data.
 - **Rules relating to dispute resolution:** Set out requirements for dispute resolution for data holders and accredited data recipients (both internal and external dispute resolution).
 - **Rules relating to privacy safeguards:** Set out requirements for rules relating to consideration of CDR data privacy, collecting CDR data, dealing with CDR data, integrity and security of CDR data, and correction of CDR data.
 - **Rules relating to data standards:** Set out requirements for the Data Standards Advisory Committees, reviewing, developing and amending data standards, and data standards that must be made including technical data standards in relation to the sharing of data through API calls and consumer experience related data standards.
 - **Other matters:** Set out requirements for miscellaneous matters such as reporting and record keeping, audits and civil penalty provisions for breaches of obligations.
6. The aim of this paper is to identify areas where sector-specific rules and standards are needed to effectively apply the regime to telecommunications entities, and to design these in a way that is aligned with existing sectoral arrangements, seeking to minimise costs for participants. Similarly, we seek information on how the telecommunications sector currently structures its systems to collect and use information and how customer accounts are structured. Throughout the paper, Treasury has identified minded to and proposed positions for the purposes of seeking feedback

² Note: a data holder may refuse to disclose required consumer data in response to the request if the data holder considers this to be necessary to prevent physical, psychological or financial harm or abuse, in relation to an account that is blocked or suspended, or in circumstances (if any) set out in the data standards.

from stakeholders. Feedback from this and other consultation processes will inform Treasury's advice to the Minister as the decisionmaker for the rules.

7. These areas are the subject of **Part B** of this paper, which covers three topic areas:
 - a. **Section 1** seeks feedback on the potential scope of data sharing in the telecommunications sector and outlines the policy objectives, and rules and standards considerations. This section also discusses whether a de minimis threshold should be recommended for mandatory data sharing obligations.
 - b. **Section 2** seeks feedback on the consumers that should be eligible to share telecommunications data under the CDR regime and how consumer accounts are currently structured in the telecommunications sector. This section also discusses whether enterprise customers should be eligible for data sharing.
 - c. **Section 3** seeks feedback on other design features recommended as part of implementing CDR in the telecommunications sector including treatment of white labelled products and internal and external dispute resolution requirements for data holders and accredited data recipients (**ADRs**). This section also discusses options for phased implementation of CDR data sharing obligations.
8. We invite stakeholders to provide feedback and specific examples of use cases that can be supported by designated telecommunications data, including cross-sectoral use cases.
9. Feedback at this stage of the process will be used to develop draft CDR rules and standards. Draft CDR rules and standards will be the subject of formal consultation at a later stage, with the opportunity to make formal submissions.

Telecommunications sector Data Holders

10. Data holders are entities that are specified in a designation instrument as holding data included in the designation instrument. The telecommunications designation instrument captures carriers and CSPs as data holders and, as outlined in the sectoral assessment final report, our policy intention remains to exclude providers of 'over the top' (OTT) communications services and network providers from data holder obligations.
11. Our intention is that data sharing obligations will be recommended for data holders in relation to publicly offered products and consumer-related data as specified in the rules and standards. Data about publicly offered products (also known as 'product reference data' or 'generic product data') will be available to anyone via APIs while access to consumer-related data requires accreditation to receive that data as well as consent from the consumer to which the data relates. In certain circumstances, such as disclosure to a trusted adviser, receipt of certain consumer-related data is allowed without accreditation.
12. Data holders have a range of obligations and many of these obligations are sector-agnostic. This paper focuses on data holder obligations that require consideration in developing rules and standards for the telecommunications sector. Specifically, the obligation to provide dashboards for consumer authorisations that relate to data held by the data holder, and obligations about CDR consumer complaints and record keeping may require the development of sector-specific

rules and standards. We also seek feedback from stakeholders in the broader CDR community that have an interest in receiving data held by the telecommunications sector as the design of the rules and standards for telecommunications will have an impact on the information that ADRs will be able to access.

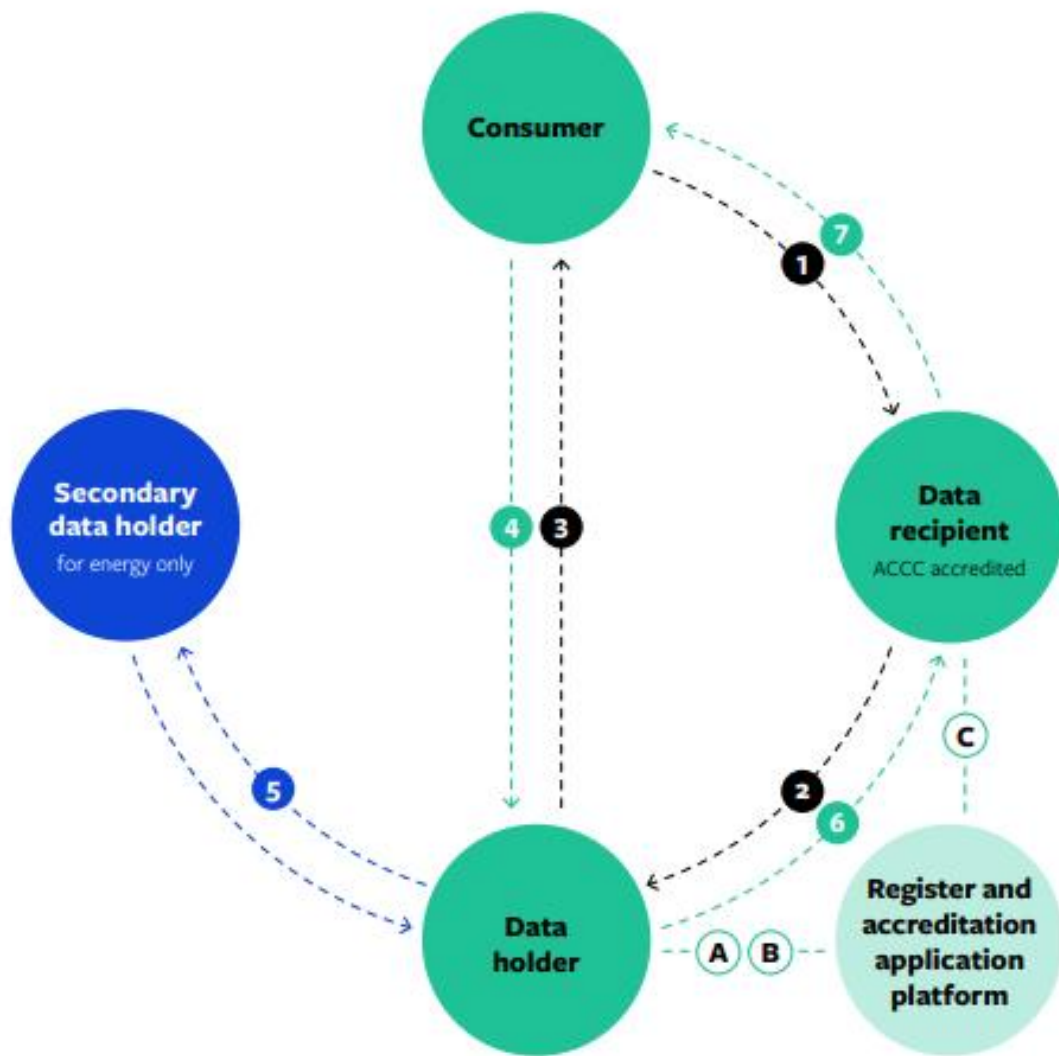
Role of the data standards and relevant artefacts

13. The Consumer Data Right Standards (standards) underpin the technical delivery of the CDR. They set out requirements for data security and format, and cover consumer experience.
14. The standards are developed and maintained by the Data Standards Body (**DSB**) in the Treasury and made by the Data Standards Chair.³ The standards must be made in accordance with the Consumer Data Right Rules.
15. The standards for [Consumer Experience](#), [Security Profile](#) and [API definitions](#) are published on the Consumer Data Standards website.⁴ The standards are also publicly available on [GitHub](#), where issues with the standards can be raised. There is also a regular maintenance iteration process.⁵ The CDR stakeholder community is strongly encouraged to contribute to standards development in relation to the telecommunications sector.
16. **Figure 1** on page 7 provides an overview of the standard data flow used in the standards, which we recommend adopting for the telecommunications sector.
17. The Consumer Experience Guidelines (**CX Guidelines**) can be found [online here](#). These artefacts provide optional implementation examples for key rules, standards, and recommendations. They include annotated wireframes, open-source assets, prototypes, and a [checklist](#) outlining key requirements. The CX Guidelines are being used to assist CDR implementation in the banking and energy sectors.
18. Specific wireframes have been created for this paper to illustrate certain concepts, issues, scenarios, as well as aid comprehension. Wireframes can be found online (see [Miro | PDF](#)), along with an [interactive prototype](#). These artefacts demonstrate possibilities and do not represent final policy positions.
19. Stakeholders can comment on the telecommunications data clusters, wireframes, and prototype via the [GitHub issue for this design paper](#), or directly on the [Miro artefacts](#) using the comment function by typing 'C' on your keyboard. The wireframes are annotated for easy referencing.

³ See Section 56FA of the *Competition and Consumer Act 2010* (Cth).

⁴ The current version of the standards is available online at: <https://consumerdatastandardsaustralia.github.io/standards/>.

⁵ For more information on the regular maintenance process for the standards visit GitHub: <https://github.com/ConsumerDataStandardsAustralia/standards-maintenance>.



- 1** Consumer engages an ADR and gives them their consent to collect CDR data for a specific purpose
 - 2** The ADR then requests data from the consumer's data holder
 - 3** The data holder confirms that the consumer has authorised the disclosure of the requested data
 - 4** The consumer confirms to their data holder that they authorise the requested data be shared
 - 5** For energy only – the data holder requests the data from the secondary data holder (AEMO). AEMO provides the requested data to the data holder
 - 6** After confirming the consumer's request, the data holder shares the requested data with the data recipient
 - 7** The data recipient uses the consumer's data to provide them with a service, then deletes or de-identifies the data in accordance with the consumer's preferences
- A** Data holders required to check the RAAP to confirm data recipients' accreditation within 5 minutes of sending data
 - B** If a data recipient is not accredited, public product information can still be shared by API
 - C** Data recipients required to register with the RAAP prior to receiving CDR data

<p>Treasury policy rules</p>	<p>DSB (standards) technical standards consumer experience</p>	<p>ACCC accreditation register compliance</p>	<p>ACCC Australian competition and consumer commission</p> <p>API Application programming interface</p> <p>DSB Data standards body</p> <p>RAAP Register and accreditation application platform</p>
-----------------------------------------	-------------------------------------------------------------------------------	--------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Figure 1 – High-level CDR standard data flow

Part B – Issues for feedback

1. Scope of data sharing in the telecommunications sector

1.1. Topic Overview

20. This section discusses the recommended scope of data sharing for the telecommunications sector and provides commentary in relation to:
- a. which data holders should be subject to mandatory data sharing obligations;
 - b. which product and consumer datasets (such as customer, account, billing and usage data) should be shared as part of these data holder obligations; and
 - c. whether ‘reciprocal’ data sharing obligations should be recommended for certain data recipients to ensure a fair and robust data sharing system.
21. Views are also sought on sector specific considerations that might be relevant to these aspects of data sharing (and other standards-related considerations).
22. We note that the designation instrument specifically excludes certain data sets from CDR data sharing including the content of communications and location data.⁶ As a result, we do not seek feedback on these excluded data sets.

1.2. Rules considerations

Which data holders should be required to share CDR data?

23. The designation instrument designates carriers and CSPs, as defined under the *Telecommunications Act 1997* (Cth), as data holders for product and consumer data in the telecommunications sector. However, the CDR Rules could require only a subset of designated data holders to share CDR data. A ‘de minimis’ threshold could exclude certain data holders from mandatory data sharing obligations based on the size of the data holder.
- a. This may be particularly appropriate in sectors where there is a ‘long tail’ of retailers, including very small entities.
 - b. Any excluded data holders would still be able to share data through the CDR on a voluntary basis.
 - c. A de minimis threshold was applied in the energy sector. Energy retailers with 10,000 residential and small business customers or less do not have mandatory obligations as

⁶ See section 9 of the Designation Instrument. Note that location data is excluded but account information such as a customer’s address has not been excluded as it is not considered location data.

data holders under the CDR Rules, unless they become accredited data recipients or they voluntarily participate as a data holder.

24. Given the large number of carriers and CSPs in the sector, we are minded to recommend a de minimis threshold and seek feedback on how that threshold could be cast.
25. The *Telecommunications (Consumer Complaints) Record-Keeping Rules 2018* requires entities with equal to or more than 30,000 'services in operation' to keep certain complaints records. We seek feedback on whether this is an appropriate threshold for mandatory participation or if there is a more appropriate way to distinguish between the size of carriers and CSPs.
26. We invite feedback on whether a threshold should be recommended for consumer data sharing obligations or to both product reference data and consumer data. A different approach to product reference data may be justified as sharing of product data can facilitate product comparison use cases and product data sharing can be less costly than consumer data sharing.

Rules questions

1. Do you support establishing a threshold for mandatory participation in CDR for the telecommunications sector (i.e. recommending a de minimis threshold)? How should such a threshold be established (for example, should it be based on the number of customers a carrier or CSP has)?
2. Should a de minimis threshold be recommended for consumer data sharing obligations only, or to both consumer and product data sharing obligations?
3. Are there any existing regulatory thresholds that can be adopted for the purpose of establishing a clear de minimis threshold in the CDR?

What products and what product-related datasets are in scope?

27. Under the existing CDR Rules, data holders are required to share 'product data' and 'product specific data' from a prescribed list of products that are in scope.
28. We intend to include publicly available phone (mobile and fixed line telephone services), internet (e.g. fixed wireless internet connection) and broadband (e.g. fixed broadband services) products as products for the telecommunications sector. Product-related datasets under the existing CDR rules for banking and energy sectors is data that:
 - a. identifies or describes the product and includes information about its type, name, price (including fees and charges), associated features and benefits (including discounts and availability of bundles), eligibility criteria, terms and conditions, and availability of a product;
 - b. in the case of data that is about availability– is data that is publicly available; and
 - c. is held in digital form.

29. The intent behind the required product data category is to support the sharing of data that is commonly contained in disclosure documents in machine-readable form, as dictated by the standards. In the telecommunications sector, the rules for required product data would support the sharing of information that is of the kind currently available in a telecommunications critical information summary or key fact sheet. The intended benefit of including product information that is currently made available is to leverage the benefits of this information being made available in a standardised and machine-readable form, which will facilitate more efficient transmission, analysis and reproduction.
30. We seek feedback on how to best describe the core phone, internet and broadband products across carriers and CSPs to support the most meaningful product comparison and data sharing (for example, whether it is sufficient to list mobile phone products or whether categories like pre-paid, post-paid, SIM-only plans and business mobile plans would be more helpful). Specifically, we are interested in the appropriate level of granularity to describe these classes of products to ensure use cases are adequately supported.
31. Treasury recommends only including publicly offered products in scope for generic product reference data sharing. This was the approach taken in the banking and energy sectors. This means that legacy or grandfathered products would not be shared as product reference data (as for other sectors, there is no policy reason to do so given they are no longer available to consumers). Similarly, we recommend that products that are offered to enterprise customers⁷ and are highly negotiated would also be excluded from product data sharing on the basis they are not publicly offered.
- a. We seek feedback on whether there are other products that would not be appropriate for inclusion, for example, in earlier consultations, products with a very low margin that are only offered to customers experiencing financial difficulty were raised as a potential exclusion.
 - b. To the extent an eligible CDR consumer uses a product (which may include a legacy product), we intend for that product data to be in scope as consumer data.

Rules questions

- 4. How can we best describe the core classes or types of phone, internet and broadband products across carriers and CSPs to support meaningful product comparison and other use cases, and to ensure products are adequately described for the purposes of consumer engagement and consent?
- 5. Do you support excluding products offered to enterprise customers from product reference data sharing? Should this exclusion be limited to products that are not publicly available and are highly negotiated?
- 6. Are there any sectoral considerations in relation to limiting product data sharing to publicly offered products that we should be aware of?

⁷ Generally, we consider enterprise customers to be large businesses or companies (but would not include small and medium-sized enterprises).

7. Are there other products that would not be appropriate for inclusion?

What is required data sharing?

32. The CDR Rules include the concept of 'required' product data (as discussed above) and 'required' consumer data. This is data that data holders are required to share in response to a valid product or consumer data request.
33. After receiving a consumer's consent, an ADR can request consumer data from a data holder. If an ADR has made a valid consumer data request, the data holder will seek authorisation from the consumer to disclose the data and once the authorisation has been made, the required consumer data will be disclosed to the ADR.
34. A data holder cannot charge a fee for the disclosure of required product or consumer data. Voluntary data, which is designated CDR data that is neither required data nor excluded data, can be shared and fees can be charged for the provision of it.
35. In relation to the scope of required data sharing for both product and consumer data, Treasury is minded to follow a similar structure to the banking and energy rules.⁸ That is, include as categories of required data: 'product data' (information about products), 'customer data' (customer details), 'account data' (account details), 'billing data' (generally speaking, the type of data a consumer has access to on their bill or through online or mobile accounts), and 'product specific data' (data that relates to products that a specific consumer uses). These datasets would be included to the extent they are held by the data holder in digital form.

Customer data

36. Customer data for CDR in other sectors is:
 - a. information that identifies or is about a person, and includes the person's name, contact details (telephone number, email address, physical address);
 - b. information that a person provided at the time of acquiring a particular product and that relates to their eligibility to acquire that product; and
 - c. in the case of business customers, a business name and ABN.
37. A customer's date of birth is not included as a dataset.
38. We expect to include customer data as outlined above for the telecommunications rules, but seek feedback on any sector-specific considerations we should be aware of.

⁸ *Competition and Consumer (Consumer Data Right) Rules 2020*, Schedules 3 and 4, clauses 1.3, 3.1 and 3.2.

Rules question

8. Are there any considerations specific to the telecommunications sector that we should be aware of in relation to customer datasets as outlined in this paper?

Account data

39. Account data for CDR in other sectors includes:

- a. Information that identifies or is about the operation of the account including account number (other than to the extent this is masked as required by law or in accordance with acceptable industry practice), the date an account was created, payment schedule associated with the account (including payment method and frequency of payments, and any concessions, rebates, or grants applied to the account) and information about the plan associated with the relevant account.

40. We expect to include similar information in scope for the telecommunications rules.

41. We do not recommend including information about whether the account is associated with a hardship program at this time.

Rules question

9. Should information about whether a customer's account is associated with a hardship program be excluded?
10. Are there any other sector specific considerations relating to account information we should be aware of?

'Billing' data

42. We recommend including a category of 'billing data' in the rules. This dataset is intended to include the key datasets that are commonly found on a customer's bill or available to customers through their online or mobile account, namely:

- a. Information about a bill that has been issued in relation to the arrangement to which the bill relates, including:
 - i. The account number, billing period, date the bill was issued, the total amount payable, applicable tariffs and charges and details of usage;
- b. Information about a payment or other transaction made in relation to the arrangement, including:
 - i. The nature of the transaction, the date and time of the transaction, the amount paid and the payment method; and
- c. The account balance at any time.

43. We are minded to including certain metadata about communications (such as dates and times of communications) in the CDR rules. This data falls within 'billing information' under the designation instrument as this information is provided to consumers on bills or otherwise made available through online accounts.
44. We welcome feedback on the types of metadata that are typically made available to consumers on their bill or through their accounts. We also seek feedback on the usefulness of including this data within the scope of required data sharing.
45. We do not recommend including called party numbers (including messaged party numbers) in the CDR Rules.

Rules questions

11. What types of metadata are typically made available to consumers on their bill?
12. To what extent can insights be drawn from the inclusion of metadata within the scope of required data sharing?

Usage data

46. We also recommend including usage data within the scope of required data, such as the total number of calls or SMSs, or total amount of data uploaded and downloaded over a certain period. Accordingly, we welcome feedback on:
 - a. The different types of usage data displayed on bills (for example, total number of calls or SMSs, or total amount of data used over a certain period)⁹;
 - b. How usage data may differ across products (for example, unlimited compared to limited products);
 - c. The extent to which insights can be drawn about a consumer based on their usage data; and
 - d. Whether usage data is of interest to ADRs to support use cases (even with respect to plans with unlimited usage).

Rules questions

13. What are the different types of usage data displayed on bills or otherwise made available through online accounts (for example, total number of calls or SMSs, or total amount of data used over a certain period)?
14. How may usage data differ across products (for example, unlimited compared to limited products)?

⁹ We note that clause 5.3.1 of the [Telecommunications Consumer Protections Code](#) sets out bill content requirements but does not specify the different types of usage data to be displayed on the bill.

15. To what extent can insights be drawn about a consumer based on their usage data? Is usage data of interest to ADRs to support use cases (even with respect to plans with unlimited usage)?

'Historical' data

47. An important objective is for the CDR in telecommunications to support anticipated use cases such as price comparisons and switching based on previous usage. To facilitate these and other use cases, we are minded to require carriers and CSPs to disclose consumer data for up to the past 2 years, subject to the 'earliest holding day' of 1 January 2022, as outlined in the designation instrument.
48. This approach is analogous to the one taken for consumer data in the energy sector and is also consistent with existing mandatory data retention regime requirements for telecommunications under the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA Act**) where certain carriers and CSPs are required to retain a particular set of telecommunications data for at least 2 years. We also note that the *Telecommunications (Consumer Complaints) Record-Keeping Rules 2018* require data to be retained for 2 years. We welcome feedback on the recommended timeframe for disclosing consumer data and whether other considerations exist concerning the disclosure of historical consumer data.

Rules questions

16. Do you support the time frame of requiring carriers and CSPs to disclose consumer data for up to the past 2 years, subject to the earliest holding day of 1 January 2022?
17. Are there any considerations specific to the telecommunications sector that we should be aware of in relation to historical data?

Closed account data

49. We recommend to exclude data from closed accounts as required consumer data, unless the customer still has an account open with the carrier or CSP. In particular, this is in recognition that it could be difficult for the carrier or CSP to authenticate a former customer for data sharing.
50. To the extent closed account data is in scope, we welcome feedback about the appropriate approach to sharing it, for example, how much data could be shared on a closed account and when a data sharing request could be made on a closed account. By default, closed account data could be subject to the same 2 year historical data limit noted above, and this would be similar to the approach taken in the energy sector for closed accounts. In the banking sector, a data sharing request on a closed account must be made within 24 months of the account closing,

whereas in the energy sector, there is no time limit on when a data sharing request on a closed account can be made.¹⁰

Rules questions

18. Do you support the inclusion of closed account data for customers with an open account?
19. Do you have any comments on the approach to sharing closed account data – for example, when a request could be made and how much data on a closed account could be shared?

Accessibility data

51. We are minded to recommending the inclusion of accessibility data as a type of required product data to enable ADRs to develop use cases that can support customers with a disability in identifying products that suit their needs. We welcome feedback on the types of accessibility data that could be shared under the data standards if accessibility data were to be included as required product data. For example, information about the ability to receive information in alternative formats (like braille or large font) and services that enable customers to convert voicemail to text.

Rules questions

20. If accessibility data were to be included as required product data, what types of accessibility data could be shared?

Reciprocal data sharing obligations for certain ADRs

52. Reciprocity is a concept that, in broad terms, requires data recipients to have the same data sharing obligations as a data holder in respect of certain data to ensure a fair and robust data sharing system.

53. Currently, the CDR Rules include reciprocal data sharing obligations for ADRs that generate and hold data in respect of banking products they publicly offer (for example, non-bank lenders). At this stage, we do not intend to make rules that would require ADRs to have reciprocal data holder obligations in respect of telecommunications products. Similar to the energy sector, we understand there are no entities other than carriers or CSPs who generate and hold telecommunications data and for whom reciprocal data sharing obligations would be appropriate. However, we welcome views about whether there are entities other than carriers or CSPs that generate and hold telecommunications data, and therefore should be subject to reciprocal data sharing obligations (if those entities were to become accredited).

54. The existing CDR Rules also include a mechanism that enables designated data holders (energy retailers and authorised deposit-taking institutions) that become accredited to become data holders of CDR data they receive through the regime, if certain conditions are met. We intend to

¹⁰ Note: While there is no time limit for the data request, the data that is available to be shared is still subject to the requirement to have at least one open account and, in relation to billing data, that the data is within 2 years of the day of the request.

draft similar rules for consultation in the telecommunications sector. That is, if a carrier or CSP became accredited, they could become a data holder of the CDR data they receive under the regime – rather than an ADR – if particular conditions are met. Following the approach taken in banking and energy, these conditions would likely include that the ADR is a carrier or CSP, that the customer has acquired a product with the ADR, and that a specific consent has been given by the customer for the ADR to hold the customer’s data as a data holder.

Rules question

21. Are there entities (other than carriers or CSPs) that generate and hold telecommunications data, and if so, should these entities be subject to reciprocal data sharing obligations (if they were to become accredited data recipients)?

1.3. Standards considerations

Technical standards considerations

55. When developing technical standards for data sharing of designated data clusters, there are several specific concerns that can influence the complexity of the standards development process and subsequent implementation by participants. These concerns are outlined below and feedback specific to the telecommunications sector or to individual data clusters would be welcome.
56. **Data latency** – For some data clusters the amount of time it takes to provide accurate data, the volume of data available or the temporal extent of historical data held in readily accessible systems can all create issues. For the data clusters being considered, feedback on issues relating to data latency would be helpful in planning standards development.
57. **Data quality** – The variability of data quality held, both with regard to accuracy but also structural consistency, can heavily influence the development of data standards. The standards prioritise strongly typed structures as this maximises the value of the data transferred. Feedback on areas of known data variability for the data clusters being considered would be helpful.
58. **System fragmentation** – It is helpful to understand the level of existing architectural fragmentation of systems that hold and present the data clusters being considered. This has a direct impact on the technical difficulty in defining consistent standards but can also influence phasing of standards implementation.
59. **Existing standards** – The preference of DSB is to leverage existing industry standards that are already widely adopted and accepted, where possible. Suggestions are therefore requested on any existing standards that may accelerate the development of standards for telecommunications.

Consumer experience considerations

60. Data language standards form part of the consumer experience (CX) data standards and include mandatory descriptions of datasets to be used by CDR participants. The purpose of the data language standards is to provide comprehensible and meaningful descriptions and groupings of datasets to facilitate informed consumer consent.
61. The existing data language standards can be found [here](#), which cover the language to be used when requesting banking and energy data. New data language standards will need to be developed for telecommunications data, which will build on already established language standards.
62. Preliminary data language has been developed for the telecommunications sector based on the information contained in the designation instrument. A list of the preliminary language can be found online (see [Miro | PDF page 1](#)), and in the context of the consumer-facing consent step (see [Miro | PDF page 2](#), including an [interactive prototype](#)). Data language will be consulted on and refined further alongside the technical standards.
63. To assist the development of data language standards, the Treasury and DSB welcome feedback on appropriate dataset groupings and descriptions to support consumer comprehension and informed consent, including where certain datasets may be considered sensitive. Feedback is also welcome that includes how the telecommunications sector may currently describe the recommended designated data to consumers, and any relevant terminology and language standards.

Standards questions

22. Are there any considerations specific to the telecommunications sector that we should be aware of in relation to the technical standards considerations outlined in this paper?
23. Are the preliminary data clusters grouped and described appropriately and in a way that reflects existing structures and experiences? See [Miro | PDF page 1](#) for a preliminary data language list, and see [Miro | PDF page 2](#) for how this language features in the consent flow.

2. 'Eligible CDR consumers' in the telecommunications sector

2.1. Topic overview

64. While a broad range of consumers are 'CDR consumers' under the regime, the CDR Rules narrow which CDR consumers can initiate data sharing through the concept of an 'eligible CDR consumer' (namely, eligible to initiate CDR data sharing requests). This section addresses which CDR consumers should be 'eligible' to make CDR data sharing requests in the telecommunications sector.
65. The sector-agnostic definition of 'eligible CDR consumer' is at rule 1.10B and states that, subject to any additional criteria set by sector-specific rules, a CDR consumer is eligible in relation to a particular data holder at a particular time if, at that time:
- a. the CDR consumer is either an individual who is 18 years or older or a person who is not an individual; and
 - b. the CDR consumer is an account holder or secondary user¹¹ for an account with the data holder that is open.
66. A CDR consumer that is a partner in relation to an open partnership account is also eligible.
67. Schedules for each sector may add additional sector-specific criteria for eligibility, such as in clause 2.1 of Schedules 3 and 4 for the banking and energy sectors, respectively. For example, for a CDR consumer to be eligible in relation to a particular data holder in the banking sector, the consumer needs to be able to access an account online. This can be compared to the energy sector, where to be eligible in relation to a particular retailer, a consumer needs to be a customer of the retailer and have an account that uses less than 5GWh per year.

2.2. Rules considerations

68. For the telecommunications sector, we seek feedback to determine whether criteria additional to the sector-agnostic definition of eligible CDR consumer are appropriate.
69. In this regard, we welcome feedback on the nature of different user relationships with telecommunications retailers. For example, how accounts are managed (including billing and customer management for different types of accounts) and the type of engagement customers have with their retailer (for example, the extent of digital engagement across the sector, and whether this correlates to particular products or customer types).

¹¹ Under the CDR Rules, a person must have account privileges in relation to an account with a data holder in order to be a secondary user for the account. The definition of account privileges is sector-specific. For example, in the energy sector, a person has account privileges if they are authorised to access data under national energy legislation.

70. We also seek to understand whether the concept of ‘secondary user’ in the agnostic definition is extendable to telecommunications. In this respect, we welcome feedback on any definitions or differentiation between account privileges in the sector.
- a. For context, to be a secondary user for an account (under the existing CDR Rules), a person must: be an individual who is 18 years or older, have account privileges in relation to an account, and the account holder/s must have given the data holder instruction to treat the person as a secondary user for the purposes of the CDR.
71. For non-individuals (businesses), ‘nominated representative’ rules (see rules 1.13(1)(c)(i) or 1.13(1)(d)(i)) require data holders to provide a service that enables non-individuals to nominate one or more individuals, 18 years or older, to give, amend and manage authorisations to disclose CDR data on behalf of the business. These rules provide flexibility for retailers to determine the precise mechanism and process for the nomination. We consider these existing, sector-agnostic rules would be recommended for the telecommunications sector, however, we welcome feedback on the extent to which sector-specific modifications may be appropriate.
72. We assume there are not many, if any, ‘joint accounts’ in the telecommunications sector that would meet the existing rules definition for a ‘joint account’. In the event that such accounts exist, we expect they would be subject to the existing provisions in the CDR rules and we do not recommend making sector-specific rules about joint accounts.
73. We note that sharing data from accounts with more than one user may allow account holders to access consumer data about third party users of the account (for example, employers accessing information about an employee’s service linked to the business account). For these accounts, we welcome feedback on whether consumer data should not be shared in these circumstances, noting that the content of communications and location data has already been explicitly excluded by the designation instrument, and that the type of data we expect to be included under billing data is data that should be already available to the account holder. Therefore, we note that access to sensitive data about third party users may be an existing issue related to how account access is structured and does not specifically arise due to CDR’s application to the telecommunications sector.

Rules questions

24. What kinds of ‘secondary users’ (users with account privileges, other than the account holder) exist in telecommunications? You may wish to comment generally on account structures and/or the prevalence of additional users with account privileges, and whether this is product or customer-type specific. Are user accounts structured the same across different product types? If so, does this affect how secondary or other users should be defined?
25. How are account privileges defined in telecommunications? Is there an existing definition of account privileges that distinguishes between different types of users?
26. Is there a hierarchy of users, for example, whether different users have different authorisations or levels of access? If there is a hierarchy of users, how do carriers and CSPs tier privileges? Should all users in a hierarchy benefit from CDR data sharing or should access be limited in some way?

27. Where account holders may be able to access consumer data about third party users of the account (for example where an employer is an account holder for an employee's product or service), should data not be shared in these circumstances? If not, how can these types of accounts be excluded?

Users without online access

74. We seek feedback on whether 'offline customers' should be considered eligible CDR consumers, as they are in the CDR in the energy sector. Only consumers with at least one online account are eligible in the banking sector. An 'offline customer' is defined as a customer who does not have access to or has not created an online account.

75. For offline customers, authentication and dashboard requirements could be met by issuing a one-time password or facilitating offline users to create an online account if they wish to.

Rules question

28. Should 'offline customers' (i.e. customers who do not have online access to the relevant account) be considered eligible CDR consumers?

Enterprise customers interaction with CDR

76. In the enterprise segment of the telecommunications market, there may be particularly large customers with highly customised contracts and arrangements that are not referable to publicly available products captured under generic product data sharing obligations. Such customers may also be unlikely to consider switching to the types of standard products that would be available through product reference data sharing.

77. With this in mind, we welcome feedback on the costs and benefits of facilitating consumer data sharing for large enterprise customers. We welcome feedback on the extent to which this segment of customers' data exists within core operational systems as opposed to separate systems and whether, from the perspective of an accredited retailer or other ADRs, there may be benefit in receiving consumer data for this cohort to support pricing and negotiation for bespoke products in the future, or other use cases.

78. We note that there are already delineations between market segments in the telecommunications sector that could be considered for an eligibility threshold (for example, the Telecommunications Consumer Protections Code distinguishes between consumers that spend more or less than \$40,000 on services), and welcome further stakeholder feedback on the issue.

Rules questions

29. Should the definition of eligible consumer for the telecommunications sector exclude some or all types of enterprise customers? If some enterprise customers should be excluded, how should the rules distinguish between eligible and ineligible enterprise customers?

2.3. Standards considerations

Technical standards considerations

79. We seek feedback on the strength of identity verification (such as 100 points identification check) and authentication (such as one-time password (**OTP**) as part of the authorisation and consent process) in the sector in relation to primary and secondary user for CDR data sharing purposes. We also seek feedback on the existing types of permissions for joint accounts or services and how they are managed over time as well as any further considerations for consumer dashboards that are not addressed by the consumer account structures identified above.
80. The standards considerations for eligible CDR consumers are largely captured by the consumer experience considerations below.

Consumer experience considerations

81. A number of existing CX standards deal with different consumer and account types. These specific issues relate to the data holder space and include:
- a. [Authentication standards](#), which work in conjunction with the [Security Profile](#) and require a unique user identifier and OTP to be used for authentication purposes, including by account holders, secondary users, and nominated representatives;
 - b. [Authorisation standards](#), which allows data holders to:
 - i. Offer a profile selection step to support scenarios where a single identifier provides access to different customer accounts, such as business and individual consumer accounts;
 - ii. Allow consumers to select which accounts they would like to share data from, and provide additional information where an account may not be shareable;
 - c. [Notification standards](#) for joint accounts; and
 - d. [Withdrawal standards](#), which include messaging standards relating to joint accounts and secondary users.
82. [CX guidelines](#) exist to accompany the above standards and provide examples for a range of scenarios, including permissible implementations that may be required due to customer segment or sectoral differences.
83. Sectoral differences may include lower digital adoption, varying authentication practices and credential use, and the structuring of accounts, plans, or services that may result in alternate data segmentation and data subjects. Wireframes are provided to note where these issues may arise, and feedback is invited to highlight where sectoral differences may exist that will impact the consumer experience, including successful authentication and data sharing, consumer control, and consent management. These wireframes can be found online, see [Miro | PDF page 2](#), along with an [interactive prototype](#).

Standards questions

30. Are the existing verification and authentication mechanisms in the telecommunications sector strong enough to protect primary and secondary users for CDR data sharing purposes?
31. What are the existing types of permissions for joint accounts or services and how are they managed over time?
32. Do you have any feedback or further considerations specific to the telecommunications sector in relation to consumer dashboards?

3. Other design issues for the telecommunications sector

3.1. Rules considerations

White labelled products

84. White labelled products are typically supplied by one entity (a white labeller) and branded and retailed to consumers by another entity (a brand owner). White labelled products exist in the telecommunications sector where consumer data may be held by two CSPs, one being a brand owner and another a network provider/white labeller.

85. The existing approach to sharing data for white labelled products under the CDR is broadly:

Product data sharing

- a. Where there is a single data holder involved in providing a white label product (whether that is the white labeller or the brand owner), the data holder must respond to product data requests in relation to the product.
- b. Where there are two data holders involved in providing a white label product, the data holder that has the contractual relationship with the consumer must respond to product data requests. The other data holder may also respond to product data requests. However, in the interests of avoiding unnecessary duplication, this is not mandatory.
 - i. The data holder that has the contractual relationship with the consumer may agree with the other data holder that the other data holder will perform that obligation on their behalf.

Consumer data sharing

- a. Where there is a single data holder involved in providing a white label product (whether that is the white labeller or the brand owner), that data holder must comply with consumer data request obligations under the rules.
- b. Where there are two data holders involved in providing a white label product, it is the data holder that has the contractual relationship with the consumer who will be considered responsible, to avoid unnecessary duplication.
 - i. The data holder that has the contractual relationship with the consumer may agree with the other data holder that the brand owner will perform that obligation on their behalf. In this example, the data holder that has the contractual relationship with the consumer remains accountable for the performance of the obligation.

86. In the telecommunications sector, we understand it is the brand owner CSP (which may be a carriage service intermediary, as a type of CSP) who typically has the contractual relationship with a consumer and, under the existing approach to white labelling in the CDR rules, would therefore be considered responsible for discharging CDR data holder obligations for both product and consumer data sharing.

87. We are minded to maintain the existing approach for telecommunications and welcome feedback on whether this approach raises particular issues for the telecommunications sector.
88. We understand that CSPs cover all brand owners reselling white labelled products. If all brand owners are CSPs who have the contractual relationship with the consumer, we seek feedback on whether white labelling rules are required for the telecommunications sector.

Rules question

33. Does the cross-sectoral approach to white labelling as outlined in this paper suit the telecommunications sector? Why/why not?
34. If all brand owners are carriers or CSPs who have the contractual relationship with the consumer, are white labelling rules required for the telecommunications sector?

Internal dispute resolution requirements

89. As a first step to resolve complaints from CDR consumers, data holders are required to have internal dispute resolution (**IDR**) processes in place that meet the requirements set out in the relevant sector schedule of the designated sector in which they operate. ADRs must have processes that meet the requirements of one or more designated sector).
90. As of 1 August 2019, the *Telecommunications (Consumer Complaints Handling) Industry Standard 2018* (the **Complaints Handling Standard**) contains complaints handling rules for IDR in the telecommunications sector. The Complaints Handling Standard applies to all carriers and CSPs responsible for network units that are used in the supply of services by CSPs. The Complaints Handling Standard include the definitions, processes, timeframes, and record-keeping requirements for consumer complaints and has been largely uplifted from the previous Telecommunications Consumer Protection Code, with consideration of the AS/NZS 10002:2014 Guidelines for complaint management in organizations.
91. In addition to the Complaints Handling Standard, if retail CSPs have equal to or more than 30,000 services in operation, complaints records must be kept under the *Telecommunications (Consumer Complaints) Record-Keeping Rules 2018* (the **Record-Keeping Rules**). The Record-Keeping Rules address the type of complaints records that must be kept, the timeframes for reporting complaints data and the process for reporting complaints data.
92. We are minded to leverage existing sector-specific IDR provisions in the CDR Rules. This follows the precedent set in the banking sector, where Australian Securities and Investments Commission's (ASIC) ASIC's Regulatory Guide 271 was adopted. We note that when the CDR Rules commence for the energy sector, ADRs who are not energy retailers but share energy data will be subject to the ASIC's Regulatory Guide 271. Accordingly, we seek feedback on whether existing sector-specific IDR standards (in particular the Complaints Handling Standard) can be leveraged for data holders who become ADRs sharing telecommunications data.

Rules question

35. For internal dispute resolution, should existing sector-specific IDR provisions (such as the Complaints Handling Standard) be leveraged for data holders who become ADRs sharing telecommunications data?

External dispute resolution requirements

93. Treasury will consider the feasibility of leveraging existing external dispute resolution (**EDR**) schemes for data holders and in circumstances where carriers or CSPs become ADRs, we are minded to follow the approach taken in previous designated sectors, which is to only require such data holders to become members of the Australian Financial Complaints Authority (**AFCA**) where they use data to offer services outside the telecommunications sector (for example, where a carrier or CSP ADR, as an ADR, is providing services using banking and/or energy data). Treasury is currently in discussions with AFCA about recognising AFCA as the EDR provider for ADRs in the telecommunications sector. Accordingly, the EDR scheme for ADRs is subject to AFCA's formal agreement to perform that function.

Entity	Recommended EDR body
Carriers and CSPs	Telecommunications Industry Ombudsman
ADRs	Australian Financial Complaints Authority
Carriers and CSPs who become accredited (and use the data to offer services within the telecommunications sector)	Telecommunications Industry Ombudsman
Carriers and CSPs who become accredited (and use the data to offer services outside of the telecommunications sector)	Australian Financial Complaints Authority

3.2. Standards considerations

Technical standards considerations

94. DSB is minded to CDR standards for the telecommunications sector to align with existing telecommunications industry standards for sharing data such as the [TM Forum](#) and [Global System for Mobile Communications](#) (GSMA).
95. In relation to identity management, DSB is minded to utilising current in place identity and access management systems, government identity initiatives such myGovID or third party identity providers.
96. We seek feedback as to whether there are any specific regulatory frameworks for the telecommunications sector that align with the current standards [Security Profile](#). For example,

whether carriers or CSPs use the GSMA's Mobile Connect API, which is a universal identity service that enables authentication, authorisation and secure identity verification.

97. Aside from being relevant to the rules, the identification of data flows for white labelling arrangements is also relevant for the technical standards. We seek feedback on whether the architecture of white labelling arrangements in telecommunications is covered by the existing standard data flow in the standards (see **Figure 1**). If not, we seek feedback on any white labelling arrangements that exist within the sector (for example, a brand owner that outsources products to numerous white labellers).

Standards questions

36. Are there any specific regulatory frameworks for the telecommunications sector that align with the current standards [Security Profile](#)?
37. Is the architecture of white labelling arrangements in telecommunications captured by the standard data flow? If not, what other data flows exist for white labelled products in telecommunications?

Consumer experience considerations

98. Based on the items currently raised above, there are no further consumer experience considerations to add to this section.

3.3. Implementation considerations

Staged implementation

99. The staged application of the CDR Rules to CDR participants was a feature of the rollout of CDR to the banking and energy sectors. The banking sector had three phases and phased in obligations both by participants, by type of product, and by type of customer (with corporates phased in last). The energy sector has four tranches which phase obligations by participants and by the complexity of data sharing functionality.
100. We are considering whether a staged approach to introducing data holder obligations may be appropriate. For example:
- a. the first tranche might be the largest carriers and CSPs sharing product data only;
 - b. the second tranche might be the largest carriers and CSPs sharing consumer data with accredited data recipients; and
 - c. the final tranche might be the remaining carriers and CSPs (subject to a de minimis threshold if one is recommended) sharing both product and consumer data.
101. Additional tranches may potentially be inserted based on customer accounts or based on products. For example, a first tranche product data could be subject to further phasing based on the type of product such as starting with prepaid products.

102. The recommended implementation timetable is yet to be set by the Australian Government but we welcome feedback on considerations for the potential implementation timetable as outlined above.

Implementation question

38. Would you support a phased approach to the application of CDR obligations for the telecommunications sector? Why/why not? If you support a phased approach, how should it be phased?