TELSTRA CORPORATION LIMITED

Response to Consumer Data Right rules – expansion to the telecommunications sector and other operational enhancements

Public version

14 October 2022

Executive Summary

We welcome the opportunity to comment on Treasury's draft rules for the Telecommunications Consumer Data Right (**CDR**). Telstra supports the development and application of the CDR, particularly if it offers a safe place in which customers and businesses can share and use each other's data, and the regulatory burden is not too great.

Treasury's proposed rules for the telecommunications sector reflects many of the matters advocated for by the industry during the August 2021 sectoral assessment consultation process, the 2021 consultation on the Designation Instrument and the Design Rules consultation in March 2022. We appreciate Treasury's consideration of these industry views, however, we remain concerned that Treasury's proposed amendments to the CDR rules set too big and too fast an agenda for our industry, and the aggressive time frames proposed for implementation will elevate the risk of implementation and compliance errors.

We are concerned about the following aspects of the introduction of the telco sector into CDR:

1. **Delivering all CDR obligations in a single tranche**. The three major telcos are required to meet all CDR obligations in the first tranche, as Treasury's staged approach only applies to service providers other than Telstra, Optus and TPG. The full set of Telco CDR obligations include:
    - fixed and mobile product sets: including anything bundled with them, and including legacy/grandfathered products;
    - all five data categories, namely customer data, account data, billing data, product data and usage data;

    across both consumer and small business customer segments.

    In addition, the three major telcos must develop the full authentication and consent flows (which contain nine unique consent types). Bringing the full CDR obligations on board for the three major telcos in a single tranche is too difficult and risks implementation errors in the rush to meet the implementation deadline.

2. **Chains of outsourced service providers (OSPs) as data recipients**. The proposed amendments to the CDR rules introduce greater flexibility in the structure of OSPs (sub-contractors) as data recipients. This includes introducing the concept of an Indirect OSP and extending "sponsored Accreditation" to Indirect OSPs as data recipients (i.e., the OSP is not directly accredited, but is sponsored). Against a backdrop of heightened sensitivity around data breaches, Telstra is concerned about losing sight and control of the data about its customers through a potential web of Direct and Indirect OSPs, who need not necessarily be accredited in their own right. We have reservations about the risk of potentially sensitive data being inadequately protected, potentially betraying consumer trust in the CDR and in the event of a breach, causing harm to individuals and brand damage to other CDR participants.

3. **Lack of precision in the definitions of data types**. Lack of precision in the definition of the term "bundled" and the use of broad descriptors used to capture data sets creates ambiguity for service providers and should be narrowed to avoid risk and inconsistent implementation.

4. **Definition of large-scale customers**. While we support Treasury's intention to exclude large-scale account customers, we consider the drafting does not fulfil this intention. In particular, we consider smaller businesses who operate under an enterprise umbrella may be unintentionally caught, e.g., individual real estate agencies or municipal councils. Our submission suggests changes to ensure Treasury's intention is more appropriately captured.

5. **Privacy**. The introduction of tailored privacy safeguards for the CDR regime continues to be a point of concern for the privacy community as it creates a range of realised and potential inconsistencies for organisations.

6. **Secondary users**. CDR eligibility is extended to secondary users on an account (also called "authorised representatives"). Due to the different levels of authorisation commonly employed in the telecommunications sector, we are concerned that secondary users will be able to provide CDR consent without the primary account holder's knowledge or consent.

Keeping customer information safe and secure is of the utmost importance to Telstra. With the heightened awareness on breaches and security, and the potential for complex structures involving third-party outsourced service providers (OSP), we are strongly of the view that consumers need an opportunity to become familiar with whom their data may be transferred to in a gradual approach.

Telecommunications is a very complex industry, and to minimise risk, we strongly recommend a phased implementation that commences with just product data for a single product and progressively expands to finally include all proposed data types for the telecommunications sector. We believe this would be a prudent and pragmatic approach with a review at the end of each phase to further de-risk the implementation of the telecommunications sector into CDR.

We remain committed to the CDR, and we look forward to engaging with Treasury on these important aspects.

Contents

1 Introduction

We welcome the opportunity to comment on Treasury's proposed amendments to the Consumer Data Right (**CDR**) Rules to introduce the telecommunications sector. Telstra is committed to the development and application of the CDR to the economy, as the CDR has potential to be the place where consumers and businesses can safely share and use each other's data. It is important that the telecommunications sector is introduced successfully and at low cost for consumers and telecommunications services providers. This entails introducing the sector in a way that offers customers the benefits intended by the CDR policy, while ensuring adequate safeguards, consistency in consumer experience and minimising the implementation and regulatory burdens for businesses.

Our submission is structured as follows. Section 2 commences with our view that the telecommunications sector is a complex sector due to the array of product types and customer use cases. We strongly recommend a gradual approach to introducing CDR is required, and we explain how this can be done through the phased implementation we describe in section 3.

Sections 4, 5 and 6 look at the CDR data types and recommend that tightening of the description of CDR data for the telecommunications sector is required, especially in the context of bundles (section 5) and excluded data (section 6).

Section 7 explores eligible CDR customers with a specific focus on large scale customers and secondary users. In both cases, we strongly recommend further tightening of the definitions and scope is required.

Sections 8 and 9 look at consent and outsourced service providers, where we elaborate our concerns with these aspects of the CDR regime, and finally, section 10 looks at the dispute resolution aspects of the CDR regime, where we support Treasury's proposed approach.

2 CDR implementation must not be rushed

We support the introduction of the telecommunications sector into CDR. As a policy objective, bringing telecommunications into CDR will enable customers to "…*choose products and bundle solution that best suit their needs, and encourage more competition in the sector*".[1] It will also allow CDR consumers to share their data for a range of other uses such as general research, that will ultimately benefit consumers and the economy more broadly through innovation and the creation of new products and services.

However, the competitive landscape for telecommunications is quite distinct and different from other sectors such as banking and energy. Barriers to switching in the telecommunications sector are already low thanks to number portability schemes, and customers already benefit from enhanced information transparency through the Critical Information Summaries (CISs) and from industry codes that ensure service quality and consumer protection. We also note that for Telstra customers, the My Telstra app and website provides customers with readily accessible usage and billing data.

Given the low barriers to switching, high levels of information transparency and strong competition outcomes, we consider it imperative that sufficient time is taken to fully consider and understand any risks that may arise through the introduction of the telecommunications sector. This is best done using an incremental approach that gradually enables the benefits CDR will bring to telecommunications customers, while simultaneously monitoring and managing any risks.

---

1 Explanatory Memorandum, Attachment A, paragraph 1, p.5.

CDR is a new concept for many telecommunications companies and has not been implemented for the telecommunications sector elsewhere in the world. Introducing the telecommunications sector into CDR will not be like introducing banking and energy. We consider introducing the telecommunications sector will be considerably more complex, given the breadth of products, nature of the customer relationships and data availability (including a lack of standardised products) across providers. It is appropriate to take the necessary time to ensure appropriate consideration of the rules and a full understanding of the implementation. If this is rushed, the consequences if not implemented well (given the nature of data that is being sought and shared) are potentially harmful to customers. We are concerned regarding what appears to be a very short time frame, with Treasury advising participants that they expect rules to be finalised by the end of this calendar year (government priorities permitting).[2]

Getting these rules right is important and will set the industry and consumers up for success, whilst minimising the cost burden to industry. The sectoral assessment for telecommunications consultation in May 2021 was one of the first times many telecommunication companies had been engaged on the CDR so for many, this concept is only one year old. In addition to the expansion to the telecommunications sector, communications providers are being asked to consider other operational enhancements including extending the scope of CDR to trusted advisors/third parties which telcos are being asked to comment on even before the telco rules are settled. At present, there are also three other consultations that require response including Exposure draft legislation to enable action initiation, CDR Rules Maintenance and the OAIC's consultation on amendments to the CDR Privacy Safeguards. This, coupled with hundreds of pages of general CDR provisions, hundreds of pages of compliance obligations and guidance materials across the CDR Act, Rules, OAIC Privacy Safeguard guidelines, accreditation guidelines, and the vast array of technical standards covering consumer experience, information security, engineering and data, is an overwhelming task to achieve in a four-week consultation process on how the CDR should apply to our sector.

Finally, these rules are also being considered at a time when there is considerably more awareness and concern by consumers about their personal information and how businesses collect, use, disclose and store data. We understand the Federal Government has recently prioritised its consideration of how companies collect and store data in the context of recent data breaches. In addition, the Attorney-General's Department's broad ranging Privacy Act Review that is expected to be shortly completed and will have important implications for organisations subject to the Privacy Act as well as the CDR regime. In our view, it does not make sense to rush through the rules at a time when Australia's overarching privacy regulatory framework is in the midst of a significant review, the outcome of which may lead to duplication or inconsistency with the CDR. In addition, we recommend that processes for CDR be considered sequentially, otherwise an organisation's ability to engage is limited. This in turn, will elevate the risk of regulatory non-compliance and have a negative impact on this important policy.

3 Phased implementation is required to limit risks

The Amending Rules set out a *staged application* of the CDR to the telecommunications sector, which provides additional time for smaller carriage service providers (above the de minimis threshold of 30,000 active services), excluding the 'big three' of Telstra, Optus or TPG. For Telstra, Optus and TPG, this means we are required to comply with **all** CDR obligations from the tranche 1 date. While the tranche 1 timeframe is described as a minimum of 12 months after the making of the rules, even if a longer time period is afforded, we are concerned about the risks of delivering all the CDR obligations in a single tranche.

Given: 1) the breadth of data captured by the rules; 2) inclusion of both consumer and small business customer segments for both fixed internet and mobile "relevant products"; 3) the significant increase in complexity related to Outsourced Service Providers (OSPs); and 4) the heightened sensitivity around data breaches and data security, we urge Treasury to reconsider the timeframes and introduce a *phased*

2 Treasury Forum, 28 October, Draft telecommunications amendments to the CDR Rules

implementation. By way of comparison, we observe with the banking sector, the major four banks were permitted to introduce banking products across three discrete phases[3] across roughly 7 months (1 July 2021 for phase 1 through to 1 Feb 2022 for phase 3). Similarly in the energy sector, gas products are not in scope for Version 1 of Energy CDR, but instead are flagged for consideration in the future.

Given the complex nature of the data captured by the CDR rules, the anticipated complexity in the technical standards and service requirements (including expectations around data latency and responsiveness), and the possibility of a complex web of OSPs introduced in the proposed amendment to the CDR rules, we strongly recommend a phased implementation approach for the three major telecommunications service providers, as follows:

1. **Publicly available product specific data**.[4] This is generic plan information (i.e., excludes customisation as described in item 4(b)(vii) of the table in Schedule 5 clause 1.3, such as "*features and benefits, including discounts, incentives and bundles*"). Note: we describe our concerns with bundles in section 5. This should be no earlier than 12 months after the CDR Rule and CDR Standards for telecommunications are completed.

   Sharing publicly available product specific data related to a particular CDR consumer (i.e., the product(s) they currently purchase) would not require a CSP to build the sort of authentication flows required for sharing customer data, account data, billing data or usage data. Commencing with product specific data in the first phase will ensure CDR consumers are able to avail themselves of the benefits of CDR at an earlier time by facilitating transfer of details about the product the CDR consumer is currently using to obtain a quote from a competitor, which is a principal objective of the CDR regime.

2. **Consumer**. No less than 6 months later, customer data, account data, billing data and usage data (the remaining four categories in the table in Schedule 5 clause 1.3, which requires authentication flows) for consumer (residential) customers.

3. **Small Business customers**. Finally, and notionally a further 6 months after the two initial phases, customer data, account data, billing data and usage data for small business customers (also requiring authentication flows).

If CDR were launched in this way, this would see CDR introduced progressively, and for the major three telcos, still within 24 months of the completion of the CDR rules and standards. Importantly, it would allow Data Holders such as Telstra the opportunity to gain some experience with the array of entities that could come to hold customer data through various OSP structures that may arise.

Commensurate with the banking and energy sectors, who were permitted to introduce different products progressively through a phased implementation, we believe there is merit in considering whether certain products/services should be introduced progressively under a future version of the Rules, for example, commencing with Fixed Internet services, then moving to mobile services, and finally moving to legacy and/or grandfathered products and plans. It is worth remembering that each of these product categories is not a single product, but rather a plethora of products within the two broad product categories. Introducing two product categories simultaneously is ambitious, especially where there is no international precedent for data portability in the telecommunications sector. Australia is leading the world on the introduction of our sector into a CDR regime, which is in stark contrast to Australia's position in the

---

3 CDR Rules, proposed amendments, Schedule 3, clause 1.4 and the Commencement Table in Schedule 3, clause 6.6. Note that the phasing for banking was amended, and the ACCC's website contains the final phasing for banking, dated 19 February 2021. It is available at https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0/accc-makes-amendments-to-the-consumer-data-right-rules, and the infographic available on that website sets out the timing: https://www.accc.gov.au/system/files/20-64FAC_CDR_Phasing_D07.pdf

4 i.e., the information described in Item 4 in the table in Schedule 5, Clause 1.3.

previous two sectors, where the banking sector was modelled on the UK Open Banking system,[5] and the energy sector, which was modelled on a program of work undertaken by HoustonKemp[6] to enhance consumer access to energy data.

We strongly recommend overlaying the phased implementation we describe above by progressively implementing telecommunications products for two key reasons. Firstly, introducing multiple product types simultaneously increases implementation effort, as data must be curated across multiple products, and each product takes time/effort to develop the IT system capabilities, APIs, etc to compile and curate the data. Secondly, being a new sector, we are yet to understand the unintended consequences of sending consumer data to third parties including ADRs and the range of possible OSPs (especially when the users of the services are not always the account owners).

Finally, the CDR regime is new to telco and a phased implementation will allow both Treasury and telco providers to test consumer demand and the correct functioning of the foundational processes such as the consent flows before moving onto the next phase. Not only is the development of the CDR an operationally complex implementation to businesses, it is also very costly. Therefore we consider a phased implementation better supports the policy objective and telcos in getting the right outcomes for consumers.

4 Telecommunications sector data that may be accessed under the CDR Rules

We welcome Treasury's Amending Rules which seek to provide further clarity on the CDR data sets for the telecommunications sector. However, we consider that Treasury's approach of defining telecommunications data sets by means of broad descriptors combined with minimum inclusions of key data (to be worked through with data standards) is problematic and we consider the introduction of an explicit list of data fields is appropriate for the telecommunications sector.

4.1 Customer data is too broad

Treasury's proposed rules in relation to *customer data* is consistent with the approaches undertaken in the banking and energy sectors. However, we consider this information remains too broad and should be narrowed to provide better guidance on what Treasury considers is, and is not, captured within the definition of CDR Customer Data. Narrowing the scope of data sets reduces ambiguity and simplifies implementation for telecommunications carriage services providers whilst minimising cost burden.

Item 1(a) of clause 1.3 in schedule 5 states customer data "*means information that identifies or is about the person*." We consider that the term 'about the person' is very broad and would unnecessarily extend to the information listed beyond Item 1(b). In addition, Item 1(b) itself is very broad. For example, Item 1(b)(iii)(A) specifically says "*any information the person provided at the time of acquiring a particular relevant product*" and (B) "*relates to their eligibility to acquire that relevant product."* We consider that this may extend to important information, such as government ID information and credit information, as such information is required for identity verification and credit purposes. As such, we recommend further work is required to tighten the definition of customer data to explicitly exclude any "high-risk" data types from the CDR data definitions. We recommend Treasury convene a working group to look at the types of data typically captured by telecommunications service providers, with a view to create an explicit list of product data tightening the CDR Rules to explicitly remove "high-risk" data types from the CDR data types.

Sending Customer Data through CDR, especially information provided at the time of acquiring the relevant product, or that demonstrates the customer's eligibility to acquire the relevant product is not

5 UK Open Banking

6 Facilitating access to consumer electricity data (Houston Kemp Report).

required in the Telecommunications sector to facilitate changing service provider. Processes for pre-port verification (PPV), mobile number portability (MNP) and local number portability (LNP) are well established and have been developed to minimise the risk of fraudulent activity. These processes seek to reduce the risk of fraudulent activity by requiring a gaining service provider establish the identity of a customer they are attempting to gain before then invoking the MNP/LNP process. PPV then provides an extra layer of security, by requiring the customer explicitly accept the MNP/LNP transfer attempt.

4.2 Billing data

Item 3(b) of cause 1.3 in schedule 5 on billing data is defined as "*information about a payment or other transaction made in relation to a relevant product*". While we understand Treasury's intention here is to simply capture the method used to pay the account (e.g., the account was paid by direct debit, or credit card, or BPay, etc), we are concerned that neither the proposed amendment to the CDR Rules or the explanatory materials adequately clarify that it excludes actual payment details such as details of the bank account from which the direct debit was transacted. While we do not think it is Treasury's intention, we are concerned that "*information about a payment*" could be interpreted as specific information about the transaction such as the account numbers a direct debit is made from. We recommend Treasury clarify the definition of "*information about*" with an explicit removal of everything beyond the method used to make a payment.

4.3 Product specific data

4.3.1 Alignment with Critical Information Summaries will achieve CDR objective at lowest cost for industry

In previous submissions we have noted the Critical Information Summary (CIS) approach[7] adopted by telecommunications providers provides an appropriate baseline of product specific information. The purpose of the CDR is to allow customers to transparently compare offers against key product metrics. We consider the CDR should in all instances mimic the required product specific information and be limited to the same information.

The CIS specifies what is included in the product, service or plan, any limitations or exclusions, the fees and charges for the product or service, and the minimum contract duration. While there is some overlap, we consider the definition of CDR Product Specific Data should be explicitly aligned with the CIS approach.

4.3.2 The Rules need to specify the type of accessibility data to be included

Item 4(b)(vii) of clause 1.3 in schedule 5 requires "accessibility data" is included. We are committed to improving the accessibility of our products and services for our customers,[8] but we are unclear of the type of information expected to be collected or provided within this field of the product specific data, and the Explanatory Materials document does not provide sufficient clarity. Devices and/or other hardware purchased with a fixed internet or mobile plan may have various accessibility capabilities, however the attributes of a plan (included calls, SMS messages or download allowance) isn't accessible or inaccessible, per se. Similarly, Telstra has improved accessibility to our services through our website to meet the Web Content Accessibility Guidelines (WCAG 2.1) standard,[9] which will be of assistance to our customers when seeking support on the products and services we offer, however, a statement saying

7 ACMA Critical Information Summaries (CISs), available at https://www.acma.gov.au/critical-information-summaries

8 Information on Telstra's commitment to ensuring our products are accessible and inclusive of customers with various needs can be found on our website at: https://www.telstra.com.au/aboutus/community-environment/community-programs/disability

9 See https://www.w3.org/TR/WCAG21/

our website meets WCAG 2.1 may not be the information Treasury is intending by "accessibility data" either. As stated in our previous submission, we request further guidance on this aspect.[10]

4.4 Usage data

Item 5(b) of clause 1.3 in schedule 5 specifies usage data in relation to a particular relevant product. This includes the number and duration of voice calls, the data usage of the SMS and the number of SMS messages, and the volume of data consumed, for the product. As per our previous submission,[11] we consider usage data relating to voice and SMS should be excluded as we consider there are few, if any, valid use cases for voice and SMS which could justify the cost of implementation, particularly where fixed internet and/or mobile plans contain "all-you-can-eat" volumes of calls and SMSs, and where customers are increasingly utilising OTT services for these types of interactions.

However, should Treasury consider voice and SMS usage data to be necessary, we consider clarifying in the draft rules that this usage information is provided on an aggregate basis only, i.e., not on a per call basis. Item 5(b)(i) in clause 1.3 of schedule 5 says "*for a relevant product that includes voice calls—the number and duration of the calls*." We are concerned about the ambiguity in the language of this definition. When a person calls another person, they call that person's "number". As such, the "number and duration" of the calls could reasonably be interpreted as providing a list of calls made, with each entry on the list containing the destination phone number and the duration of the call. Data of this nature may reasonably be considered metadata (discussed in section 6.1). Usage data also includes the "*number and duration of calls*". We consider the duration of an individual call is metadata, as call duration is information *about* the communication, not the *content* of the communication. We recommend the word "aggregate" is inserted in front of "duration of the calls" to avoid any possible conflict with metadata.

In any event, the language in the proposed amending rules is ambiguous in the context of the telecommunications industry. We consider item 5(b)(i) would be better worded as "*for a relevant product that includes voice calls—the ~~number~~ volume and aggregate duration of the calls*."

Similarly on SMSs, we are unclear as to what Treasury intends by "the data usage of the SMS" (at item 5(b)(ii)), as SMSs and MMSs are simply counted, rather than measured in terms of data volume.

We also understand from our interactions with Treasury that the intention is to capture the type of information that would exist on a customer's bill. Thus, clarifying the definition as above will still meet Treasury's objectives and will allow consumers the ability to better right plan and supports the propositions that the vast majority of plans which are currently in market. In addition, and consistent with our comments regarding the specification of product data, we consider that data captured under usage data must be in the form of an explicit list. This would also assist telecommunications providers in meeting the requirements of the CDR in the least cost way.

5 Clarify the definition of "bundled"

The Explanatory Materials document states the "…*inclusive nature of the definition of 'relevant product' means it can cover bundled products as well as handset and other associated hardware*".[12] Bundles are expressly included in the definition of "product" in clause 1.2 of schedule 5 and in the requirements at

---

10 For example, Telstra is required to offer Priority Assistance to its residential retail customers under the terms of its Carrier Licence Conditions. This requirement was introduced by the Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997 (Amendment No. 1 of 2002). There are currently no regulatory obligations on providers other than Telstra that require the offering of Priority Assistance to Customers. An indication of whether a customer is a Priority Assistance customer is likely to be a good example of what should be included as "accessibility data".

11 Telstra's August 2021 submission to Treasury's consultation on the CDR sectoral assessment for Telecommunications, available at: https://treasury.gov.au/sites/default/files/2021-11/c2021-198050-tc-telstra.pdf

12 Explanatory Materials document, Attachment A, paragraph 1, p.5.

Item 4(b)(vii) in the table in clause 1.3 of schedule 5. The definition of 'product' is linked to the Designation Instrument, which says:

> ***product*** means:
> (a) a carriage service; or
> (b) a good or a service that is offered or supplied in connection with supplying a carriage service.

These definitions are extremely broad in the context of telecommunications products and how they are sold. Under these definitions, most of the products and services offered or supplied to consumers by service providers in the telecommunications industry could be said to be "*in connection*" with supplying a carriage service. It could include anything from a gateway modem supplied with a fixed internet service, through to a set-top box (such as a Roku or Fetch-TV set-top box) with a streaming video on demand (SVOD) service, through to premium technical support or other support services such as priority assist,[13] or devices such as mobile handsets and tablets.

When the vast expanse of possible goods, services and devices that can be supplied "in connection" with a carriage service was raised at the stakeholder briefing session run by Treasury on 28 September 2022, Treasury clarified that under the CDR, "value added services" would only be denoted by a binary "yes/no" flag for the additional elements. While superficially, this may appear to "simplify" things (as there is no need to include details such as model numbers, or details of the SVOD package or premium technical support level), we are concerned the absence of detailed information could misinform consumers attempting to use the information to compare offers from different telecommunications service providers.

For example, consider service provider A who bundles a $400 mobile handset device into a 50 Gbyte/month plan with a minimum contract period of 12 months, and service provider B who bundles in a $1200 device, also into a 50 Gbyte/month plan but contracted for 24 months. If both plans retail for a similar price (say $70/month), and both show they include a device (without specifying which as additional elements are denoted by a binary "yes/no"), then the only apparent difference in the CDR data is one plan locks the user in for two years. If the customer assumes similar quality devices on each plan, then superficially the plan with the shorter lock-in period would appear the better offer, whereas the opposite would be correct.

Service providers offer different features in their products and include add-ons to consciously differentiate from other service providers, not to match their competitors. Therefore, by their very nature, direct comparisons between the offerings from different service providers is not possible because the range of features and add-ons a consumer chooses are not necessarily available from all service providers. Even where similar add-ons are available from different service providers, they may not be directly comparable in the consumer's eyes (a person may prefer Netflix to Binge, and even though both are SVOD services, that person may not be willing to replace Netflix with Binge for cheaper fixed internet rental price). The combination of products, features and add-ons that is best for a customer is an individual matter based on that individual consumer's needs, preferences and tastes. It may be that comparison between offerings from different service providers is not the primary use case for CDR data, and therefore that elements outside the primary fixed internet or mobile plan are less important and only confuse the ability to compare offerings.

Explicit clarity is required in the CDR rules to guide what goes into the CDR standards, and the guidance needs to start with a clear set of practical uses cases for which the CDR data is to be used. Further work is required to define more precisely what is meant by 'bundled' products, goods and services. Simply leaving this to the CDR standard setting process may not achieve Treasury's goals for CDR, as the temptation will simply be to include more descriptive detail into the CDR data. This will slow down

[13] For details, see: https://www.telstra.com.au/consumer-advice/customer-service/priority-assist

implementation and may not improve the ability of consumers to make an educated comparison of offers.

6 Data that is explicitly excluded from the CDR

6.1 Metadata

We are pleased that metadata in relation to communications is explicitly excluded from both required and voluntary CDR data for the Telecommunications sector (as per schedule 5, clause 3.2(4)(b)). Metadata is susceptible to re-identification, and we observe Treasury is going to reasonable lengths in the CDR rules to facilitate supply of de-identified data (including de-identified redundant data) for research purposes and for sale (or otherwise) to third parties.

However, we observe the term “metadata” is not defined in proposed amendments to the CDR Rules, or in the Explanatory Materials document. Metadata is commonly understood as data which describes other data and could cover certain billing data and usage data. Consequently, a clear definition of metadata would be very helpful to CDR participants or, at a minimum, examples of metadata of communications given.

6.2 Historical data

Including historical data is likely to drive significant incremental cost into business implementation. To that end, we are pleased that Treasury has sought to limit the extent of historical data that must be provided to 12 months.

As we have raised previously, we do query the use case and utility of historic data to the CDR regime. If it is deemed necessary, Treasury should seek to limit the data sets to basic information regarding account and billing but not product specific data or customer data. Determining the exact nature of data sets should be subject to further consultation and align with identified use cases, especially in light of the heightened sensitivity regarding storage of sensitive customer information.

6.3 Closed accounts

Whilst we support in principle the exclusion of closed accounts, we do not support Treasury’s exceptions to this, i.e., when the customer opens another account within 12 months and has a closed account with relevant transactions within 12 months. As we have previously submitted, we recommend closed accounts should be explicitly excluded from the CDR Rules. Even with the minimal exceptions available under the draft rules, including closed accounts in the scope of CDR data will introduce unnecessary complexity into the business implementation (particularly as use cases and benefits of the CDR are yet to be proven).

Closed accounts broadly fit into one of the following categories:

1. No longer requires the service – for example, in credit management and any debt has been sold
2. Has ported to another carrier
3. Has disconnected the services due to a change of ownership
4. Has consolidated services to another billing account
5. Has migrated to our digital stack IT system (internal IT change).

Under scenarios 1, 2 and 3, customers would have no use for CDR data, therefore building capability for these data flows is wasteful and irrelevant. Under scenarios 4 and 5, CDR data about the service will be captured under the new account, again making the inclusion of closed accounts irrelevant.

We see no need for closed accounts to be included in the CDR regime, and strongly recommend they are explicitly excluded in the CDR Rules.

6.4 Enterprise products

We understand it is Treasury's intention to exclude products exclusively offered to large-scale commercial customers (enterprise and large business customers). This is by virtue of the exclusion of any products that are not "publicly offered".[14] However, we are concerned this approach is not sufficiently effective for products available to business and enterprise customers. The term "publicly offered" products does not clearly enough exclude products available to enterprise and business customers from CDR Product Data requests.

Further work is required to accurately define a term for enterprise products so that they can be excluded from CDR Product Data requests. Communications Alliance has addressed this point in their submission, which we agree with and support.

7 Eligible CDR customers in the telecommunications sector

Clause 2.1 of schedule 5 sets out additional eligibility criteria for the telco sector. We support Treasury's Amending Rules which require an account nominated by a CDR consumer which relates to a relevant product, to be set up in a such a way that it can be accessed online, and not be a large-scale commercial account.[15] Nevertheless, we propose further clarifications are required to ensure Treasury's intent is captured, which we outline in the subsections below.

7.1 The definition of large-scale commercial customers must be narrowed

It is Treasury's intention that large-scale commercial accounts should not be captured under the CDR framework for the telco sector. We support Treasury limiting the scope, however, as drafted we consider that a significant tranche of large-scale commercial customers may inadvertently still be caught by the definition. We do not consider this to be Treasury's intention.

As we stated in our March 2022 submission, there is no single, all-encompassing industry standard for classification and standardisation across enterprise customers. It is important to note that not all large-scale commercial accounts negotiate terms. For example, a council that sits under a local government contract does not get to negotiate terms, may not meet the spend threshold but still should not be subject to the CDR given it sits under an umbrella enterprise contract.

In addition, our recent company strategies around digitisation and simplification of contractual terms means more of our Enterprise customers are captured under this definition (which we acknowledge matches the definition in the TCP code). This change presents challenges in giving Enterprise customers a consistent service treatment under the CDR regime. Standard terms move a greater number of sophisticated, and even listed, companies into scope of the TCP Code. Where Telstra may be a redundant or back-up carrier, the customer may also become caught under the CDR, as they spend less than $40,000 with Telstra but much more with another provider. In that circumstance, the customer would be caught under the CDR regime as a Telstra customer but are outside the bounds of the CDR with another carrier.

To ensure large scale customers are not inappropriately captured, we consider that an additional limb needs to be added to the definition of large-scale commercial customers to note that customers who are account managed by carriage service providers be specifically excluded. Account management can take many forms, including one to one or one to many. However, the key distinction is that the carriage service provider will have a personalised relationship with the customer. This will provide industry necessary clarity as it seeks to implement the CDR. Meeting any of these limbs would then satisfy exclusion under the CDR.

---

14 CDR Rules, proposed amendments, Schedule 5, Clause 3.2(2)(b)(v)(A).

15 CDR Rules, proposed amendments, Schedule 5, Clause 2.1(1).

7.2 Two-factor authentication for online accounts

The Amending Rules require the account relating to a relevant product must be set up in such a way that it can be accessed online, which we agree with and support. However, we consider that the eligibility criteria for "accessed online" must be restricted to those CDR accounts that use two-factor (or even multi-factor) authentication. Therefore, accounts without two-factor authentication (or higher) should not be captured under the CDR. Two-factor authentication is now commonly accepted practice across many sectors of the economy including banking and telecommunications, especially where accessing the online account by malicious actors could have reasonably significant consequences for the owner of the account.[16]

To keep customers' information safe and ensure a workable CDR system is developed, eligibility of accounts for CDR must be via two-factor authentication. Not specifying this risks significant differences in the way in which carriers implement the measures, resulting in inconsistent consumer experience, which undermines confidence in the CDR regime.

7.3 Secondary Users

We understand Treasury's intention is to exclude secondary users from the Telco sector for CDR. Paragraph 11 of the Explanatory Material observes that "*On the basis of stakeholder consultation, Schedule 5 of the Amending Rules does not make use of the concept of a secondary user*." The Explanatory Memorandum notes this is because carriage services providers only have a relationship with the account holder, and not with each individual end user of its products. This is the correct understanding of the relationship between carriage service providers and the *end users* of their products, and we welcome Treasury's acknowledgement of the relationship. However, a secondary user is not the same as an end user and further clarification from Treasury is required to give effect to the intention.

A Secondary User as defined under the CDR rules as an additional person with account privileges in relation to an account is not necessarily an end user. Likewise, an end user is not necessarily a secondary user. For example, a Primary Account Owner (PAO) may have four end users with mobile phones on their account. They may also have one of those additional end users designated with account privileges, which we call an "authorised representative".

Schedule 5 is silent on secondary users, which, we consider does not achieve Treasury's objective of excluding secondary users. There are many clauses throughout the CDR rules that place obligations on data holders and accredited data recipients in relation to secondary users. For example, obligations on a data holder in relation to the Consumer Dashboard as contained in section 1.15(5), or on a data holder in relation permission to disclose data contained in section 4.6A, or on a data holder in relation to notification obligations in section 4.28.

Including secondary users as defined in the CDR rules (i.e., an additional person with account privileges in relation to the account) for the telco sector introduces several problems, primarily because there is no simple, single definition of a "secondary user" for our sector. Telstra has three levels of authorised representative (beyond the primary account owner), as we describe on our websites[17] for personal and small businesses. Our permissions are set so that we have a single PAO. The PAO can then give third parties full or limited authority to perform all or only some tasks on behalf of the PAO.

---

16 In the case of telecommunications services, one significant risk is being able to port the phone to another provider, where coupled with SIM swap fraud, a malicious actor can get a new SIM configured with the target (victim) customer's phone number. Once the number is ported, the malicious actor receives any calls or SMSs intended for the victim, allowing the malicious actor to receive one-time passcodes (one-time PIN) sent as part of the two-factor authentication process used by banks, employers to access a firewalls, etc.

17 For consumer accounts, see: https://www.telstra.com.au/support/account-payment/give-another-person-access-to-account
For small business accounts, see: https://www.telstra.com.au/small-business/online-support/accounts-payments/authorise-access-to-an-account

Importantly, this is not akin to a joint account holder arrangement as seen in banking, where both parties would act as PAO. Telstra uses the following model to manage a customer account:

- Each customer account has a single PAO, who is the Account Owner and Legal Lessee of the product they have purchased from us.
- A customer account can also have other authorised representatives (with different levels of authority and permissions, such as Full Authority and Limited Authority). These contacts have the authority to enact certain transactions on the account, but are not the legal lessee of the account.

We are concerned that the extension of eligibility beyond the PAO would lead to unintended privacy consequences for consumers and introduce a range of complexities for organisations:

- When a PAO sets up an authority on an account, they are informed of the types of transactions that an authority is permitted to make in relation to the account. The PAO would not have been informed that the authority is permitted to approve the sharing of the PAO's account, usage, and personal information with third parties.
- As previously mentioned, the telecommunications industry has a "one to many" model, where customers can have multiple services under their account. It is likely that some of those services (in particular, mobile services) will be primarily used by others who are not the PAO. While those end users will be aware that the PAO has access to their general usage information as the bill payer, they are unlikely to be aware that the PAO:
    - may have set up other authorities on their account; and
    - those authorities can approve the sharing of this data with third parties.
- By extending CDR eligibility to both primary and secondary users, individuals may gain control over the transfer of other individuals' data without their knowledge or consent.
- The PAO can revoke an authority on their account at any time, which may complicate valid CDR consent flows if a non-PAO can approve the sharing of CDR data.

Due to the definition of secondary user referring to a person with account privileges, we consider Treasury has not excluded ***secondary*** *users* from the Telco sector for CDR, as per its stated intention. Rather, Treasury has simply avoided introducing additional ***end*** *users* into CDR for the telecommunications sector. Further work is required in the body of the CDR Rules to explicitly remove secondary users from obligations such as Consumer Dashboards, Permissions and Notification obligations (amongst other obligations).

Another point worth noting is that if secondary users are included for the telecommunications sector, it does not align with Chapter 3 of the CDR Privacy Safeguards dealing with consent: "*The CDR Rules state that the objective of Division 4.3 is to ensure that consent given by a consumer is voluntary, express, informed, specific as to purpose, time limited and easily withdrawn*." If a secondary user is a CDR consumer capable of making requests on behalf of the primary account holder (and vice versa), the user whom the CDR information relates to cannot provide 'voluntary' consent to the sharing of their CDR information if they are unaware the consent is being made. This interpretation is further supported by clause 10.16 of the Privacy Safeguards,[18] which states "*Where the CDR data disclosed relates to an account with a secondary user, and the secondary user is also a consumer for the CDR data, the data holder must notify both the account holder and secondary user*."

[18] Privacy Safeguards, Chapter 10, clause 10.16. https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines/chapter-10-privacy-safeguard-10-notifying-of-the-disclosure-of-cdr-data

We recommend that CDR Customer Data and providing CDR consent should be limited to the PAO only. This means that where there is additional Customer Data[19] about other end users stored on an account, that information is expressly excluded from the CDR dataset for the telecommunications sector. Similarly, only PAOs should have permission to share CDR data (i.e., provide CDR consent).

8 Consent

Trust is fundamental to the success of the CDR, and consent is fundamental to building and maintaining trust. It is in this context that we are somewhat concerned about the complexity in the types of consent, and how this will overlay the existing consents collected by telecommunications service providers, especially for more vulnerable customers. While we are not recommending any changes to the CDR Rules on this topic, we are noting it as an area that is crucial to the success of CDR, and one that will have to be managed carefully to avoid customers misunderstanding what they are consenting to. We are also concerned that if data is compromised, it will adversely affect Telstra's brand. This section of our submission address three specific concerns: 1) the number of CDR consent types; 2) lack of visibility of how a customer's CDR data may proliferate through a chain of OSPs; and 3) clarifying for our customers the difference between consent provided for CDR versus other forms of consent we ask them for.

There are at least nine consent types in clause 1.10A of the CDR Rules including: a) *collection* consent; b) *use* consent; c) *disclosure* consent; d) *direct marketing* consent; and e) *de-identification* consent. Disclosure consent is further divided into five sub-categories, including: i) disclosure to an accredited person; ii) disclosure to an accredited person for direct marketing; iii) disclosure to a trusted advisor; iv) insight disclosure; and v) business consumer disclosure. Each of these consents can be tailored for "*particular CDR data*" (i.e., a subset of the CDR data types).

We appreciate the intention is to provide consumers with fine-grained control to manage *which* type(s) of CDR data they are sending to *whom* and for *what* purpose. However, today many consumers simply click on "I Agree" when terms and conditions are presented to them on a website or an app without reading the detail, and we are concerned the level of granularity in the consent structure, consumers will be tempted to simple click on the equivalent "I Agree" and will provide their consent without understanding the detail. We also anticipate many data recipients will simplify the consent down to a single consent request encompassing all CDR data types and consent types, perhaps with an option to opt-out of specific consent types, as is commonly done with accepting tracking "cookies" on websites.

Our concern is that due to the complexity of the consent regime, the propensity for consumers to not engage with the detail, and the data recipient having an incentive to make the consent process as simple as possible, there is a risk consumers will end up consenting to activities they didn't necessarily intend to, such as direct marketing and de-identified data. It is reasonable to anticipate that consumers experiencing this situation will be disillusioned with CDR and will develop a poor perception of CDR participants involved with their data, including the original data holder. We appreciate the new Division 4.3A places new obligations on CDR representatives regarding the giving and amending consent, however, the inherent complexity in the number of consent types and possible use cases for CDR data means CDR consent will be confusing for some, or possibly even a great portion of the population.

Secondly, we raise our concerns about OSPs and chains of direct and indirect OSPs in section 10 of our submission. We appreciate CDR Rule 4.11(3)(f) requires an accredited data recipient to include in their CDR policy a list of outsourced service providers, the nature of their services, the CDR data and classes of CDR data that may be disclosed to those outsourced service providers.[20] However, we wonder how

---

19 For clarity, we are only talking about excluding any additional Customer Data about additional end users (as defined in item 1 of schedule 5, clause 1.3). We are not advocating for any of the other four data types (i.e., Account Data, Billing Data, Product Data or Usage Data as defined in items 2-5 of schedule 5, clause 1.3) to be excluded as/where they relate to other individual end users.

20 See CDR Privacy Safeguards, Chapter C. https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines/chapter-c-consent-the-basis-for-collecting-and-using-cdr-data#_ftn79

many CDR consumers will actually read a data recipient's CDR policy, and whether the policy will be kept up to date. Similarly, the sample CDR consent flow[21] shows a worked example for obtaining CDR consent, which shows that by clicking on a link, a pop-up dialog will appear showing the names of third-party providers who will have access to the consumer's data.[22] Nevertheless, we wonder whether CDR consumers will fully comprehend the extent to which their data may be shared through a possible chain of OSPs?[23, 24]

Thirdly, and separately to the CDR regime, but still related to the topic of consent and the potential for consumers to be confused, today Telstra provides (for example) the ability for its customers to opt out of direct marketing.[25] We see the potential for customer confusion where a customer opts out of direct marketing through the My Telstra service, subsequently becomes a CDR consumer and without fully appreciating what they're consenting to, consents to direct marketing through the CDR regime and subsequently starts receiving marketing material.[26]

As stated above, we are not recommending any changes per se to the CDR Rules on this topic, we are simply noting it as an area that is crucial to the success of CDR. The number of CDR consent types, the potential for complex structures of OSPs, and the coexistence of the CDR consent regime with consent(s) obtained by telecommunications service providers in the ordinary course of running their business, we remain concerned about the potential for misunderstanding. We worry that this will lead to complaints and will adversely affect consumers' perception of the CDR regime and impact the brand and reputation of data holders such as Telstra. We consider this is an additional reason to introduce the telecommunication sector into the CDR regime gradually, using the phased implementation approach described in section 3 of our submission. This will afford telecommunications service providers, CDR consumers, data recipients and the government a better opportunity to learn gradually from the implementation, and to correct issues as they arise.

9 Dispute Resolution

We support Treasury's multiple dispute resolution body structure for complaints relating to the CDR. For telecommunications the use of the TIO is well understood by carriage service providers and customers and we welcome this continuity in process.

We support Treasury's proposal to align internal dispute resolution standards to the existing telecommunications standard (*Telecommunications (Consumer Complaints Handling) Industry Standard 2018*) for data holders, and accredited persons that are also carriage service providers.

In addition, Treasury's proposed approach to external dispute resolution (EDR) seek to align EDR solutions with existing requirements of the sector. In the case of telecommunications, that means a telecommunications data holder must be a member of the TIO. However, in the case of ADRs who are not Carriage Service Providers, the draft rules state that they do not need to be party to the TIO scheme.

---

21 CDR Consent Flow Version 1.4.0: https://consumerdatastandards.gov.au/sites/consumerdatastandards.gov.au/files/uploads/2020/07/v1.4.0-Consent-flow.pdf

22 See the first step in the consent stage (fourth step overall) titled "Data request" acknowledges third parties under the heading "Supporting third parties".

23 Division 4.3A, Clause 4.20E(3)(k) of the CDR rules does say "*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*", however, a statement from a data recipient saying "Your data may be disclosed to an OSP" may not fully convey the extent (number of parties) to which outsourced parties may have access to a consumer's data.

24 Subdivision 4.3.5, clauses 4.18 through 4.20A of the CDR rules contain the notification obligations in relation to consent. There are no requirements in these clauses for a CDR consumer to be notified if the number or structure of OSPs in an OSP chain changes.

25 See Telstra's privacy statement under the heading "Direct Marketing", where our customers can opt out of direct marketing through My Telstra or by calling 1800 039 059. https://www.telstra.com.au/privacy#:~:text=and%20other%20processes.-,Direct%20marketing,-%E2%80%93%C2%A0We%20want%20to

26 This is also against the backdrop of reforms currently under consideration as part of the Privacy Act review, in relation to a universal opt-out / right to object in relation to the collection, use and disclosure of personal information for direct marketing.

As a matter of principle, any party holding/receiving/transacting with telecommunications data should be subject to the same rules as Data Holders. It is not clear to us at this stage if the rules regarding disputes that apply to the TIO and ACFA are sufficiently similar to ensure that AP's who receive telecommunications data will be held to the same level of rigour as the processes that will apply under the TIO scheme. In our view, it is imperative that they are.

10 Outsourced Service Providers (OSPs)

We are very concerned that the proposed amendments to the CDR rules introduces greater flexibility in the structure of OSPs (sub-contractors) as data recipients. This includes introducing the concept of an Indirect OSP and extending "sponsored Accreditation" to Indirect OSPs as data recipients (i.e., the OSP is not directly accredited, but is sponsored). Against a backdrop of heightened sensitivity around data breaches, Telstra is extremely concerned about losing sight and control of data about its customers through a potential web of Direct and Indirect OSPs, who need not necessarily be accredited in their own right. We have grave reservations about the risk of potentially very sensitive data being inadequately protected, potentially betraying the trust CDR consumers have shown in consenting to their data being transferred and causing brand damage to the telecommunications service providers.

While we appreciate data will only be transferred to data recipients (either Accredited Data Recipients, or OSPs under a "sponsored Accreditation") with the CDR consumer's express consent, this does not necessarily imply the CDR consumer will fully understand the extent to which their data may be proliferated through an extended chain of direct and indirect OSPs.

In the event of a data breach, customers can incur significant harm and distress. It almost goes without saying that malicious actors can use data obtained through nefarious means to steal identities, gain access to online accounts, and steal money or perform other malicious activities. Even if these don't occur, loss of control of personal information capable of being used to validate an identity will result in those individuals having to apply for new drivers licences, passports, Medicare accounts and the like, all at significant time, cost and inconvenience to the individual.

Beyond impacts to individuals affected in a data breach, there is the potential for brand damage to the CDR participants. Here, it is not solely the data recipient or OSP whose brand is affected; it is entirely possible the brand of the telecommunications service provider is also affected.

The complete re-writing of clause 1.10 of the CDR rules exposes the CDR regime to a plethora of outsourced service providers, not only for the telecommunications sector, but also for the banking and energy sectors. While the re-written rules attempt to put in place pivotal roles ("***principals***" and "***chain principals***") in the hierarchy of OSPs that may be developed, we are concerned that clauses such as clause 1.10(2)(b)(iii), which states that an OSP "…*must not use or disclose the service data other than in accordance with a contract with the principal*;" provides scope for contracts to be established instructing an OSP use or disclose information in ways that the original data holder has no visibility of.

We are concerned at the prospects of a proliferation of OSPs where the Data Holder has no visibility but nevertheless has brand reputation at stake. We strongly request Treasury re-think their approach to introducing direct and indirect OSPs and the potential web of service providers it creates, and re-engage with all three sectors (banking, energy and telecommunications) to redesign clause 1.10 of the CDR rules.