Executive summary:

Adatree is pleased to provide commentary on the Government's draft changes to the CDR Rules. We appreciate the collaborative approach the Government has adopted by seeking and listening to industry feedback.

We acknowledge the amount of work which has gone into designing these Rules amendments to ensure that the CDR takes into account the needs of businesses and the importance of enabling flexible outsourcing arrangements. We think the proposed changes will improve the overall workings of the CDR system, but have identified specific areas where further improvements to clarity and performance can be made.

Though we think that these Rules changes are a step in the right direction, more work is still needed to ensure that the CDR system appropriately serves to both protect and empower consumers. We see the CDR as a fundamental consumer right and piece of digital infrastructure that is necessary to ensure Australia's continued economic advancement. For the system to succeed there must be clearer expectations on Data Holders to make consumer data easily accessible, as well as fewer restrictions around how a consumer can consent to their data being shared and used to provide them with innovative goods and services.

A summary of our key comments are:

- We are conscious of the **mounting complexity of the Rules**. Though we think that proposed changes are important to ensure the ongoing improvement of the CDR system, we urge the Government to consider whether there are ways to accomplish these changes through the removal of existing regulation, rather than through the addition of further layers of complexity. Including examples and/or diagrams would also assist in providing clarity for participants.
- We broadly **support the increased flexibility for business consumers** through the new 'business consumer disclosure consent' and extended consent duration. We think that similar changes should also be enabled for non-business consumers to give everyone who chooses to participate in CDR greater autonomy over how they use their data.
- We argue that **further procedural changes are needed to ensure business consumers are able to easily disclose the CDR data held by their Data Holders**. The manual nomination processes currently required by many Data Holders for business consumers are inappropriate and

P: 02 8005 1826
W: adatree.com.au
A: Suite 1408, 3 Spring St, Sydney

prevent businesses from effectively participating in CDR. We call upon the Government to urgently address these issues.

- We **support the proposed changes to outsourcing arrangements**. These changes ensure that there remains clear regulatory oversight for the conduct of outsourced service providers, while providing greater flexibility in how these arrangements can be commercially and technically enabled.
- **CDR Representatives should not be able to disclose CDR data under a disclosure consent**. This increases the likelihood of consumers having their data inappropriately shared and coming to harm, and introduces an untenable amount of risk for the CDR Principal who bears ultimate regulatory responsibility for the CDR Representative's actions.
- We **support the inclusion of trial products**, though we argue that the current thresholds should be increased to better align with industry needs. We also argue that a similar concept should be implemented to allow prospective data recipients to trial the system before being required to demonstrate compliance with all of the CDR requirements.
- While we **agree with the designation of telecommunications in the CDR**, we **disagree with the limited definition of CDR consumer for the telecommunications sector**, with the current definition of a large-scale commercial account removing the opportunity for a significant number of businesses to benefit from the CDR. We also think that greater clarity should be given to the treatment of bundled products and the expectations around data holders' secondary brands.

About Adatree

Adatree has been a pioneer in the Consumer Data Right (CDR) since June 2019 with its turnkey Software as a Service platform for Data Recipients. Adatree's platform removes technical complexities so companies can focus on leveraging data instead. Our platform enables companies across all industries to receive real-time consented banking data via API.

Adatree's award-winning platform simplifies the hardest part of the CDR – the technical connection and security standards – by providing connectivity to the CDR ecosystem through one API.

As the first ADR to take on a CDR Representative, Adatree has proven our ability to adapt and scale within the evolving regime. We facilitate all of the new access models introduced in October 2022.

As a company, we have significant expertise operating within the CDR ecosystem and first-hand experience navigating its challenges. As first-movers in the CDR market, we understand the real-world challenges faced by startups and smaller companies who would rather participate in the CDR than rely on unregulated and
unethical forms of data-sharing, like screen scraping.

Detailed Comments

Business consumer changes:
Adatree broadly supports changes to rule 1.10A to increase the range of business services that can be facilitated using the CDR with the business consumer disclosure consent (BCDC). These changes align with businesses' expectations around how they need to use their data and will help to increase the ability for the CDR to provide consumer-empowering services. The steps required to be taken by an ADR to confirm that their customer is a business under rule 1.10A(6) - being that the customer is not an individual or that they have an active ABN - will likely be manageable for an ADR to achieve without introducing too much friction.

Adatree notes that ADRs themselves will not actually be able to benefit from the increased flexibility associated with receiving data under a BCDC, as these providers will need to continue to handle the data in line with the stricter requirements of the CDR. We do not agree with this outcome. If it is determined that a lower level of protections are sufficient and appropriate for certain kinds of CDR data or CDR consumers, then all participants should be able to equally benefit from the increased flexibility associated with this. If entirely un-vetted participants are allowed to receive business data without any specific CDR obligations then the same must be allowed for accredited persons. This is not an attempt to shirk appropriate CDR protections, but it is an appeal to ensure that both accredited and non-accredited participants are able to equally benefit from these different access models. This point equally applies to other processes where CDR data is disclosed 'outside the system', including as CDR Insights and to Trusted Advisers.

Adatree also notes that these updates will not change the processes non-individual business consumers need to go through to authorise a Data Holder to disclose their CDR data to an ADR or to elect a nominated representative. Current experiences in industry demonstrate that the processes being put in place by Data Holders are inappropriate and are seemingly intended to discourage uptake of the system. We are seeing processes that are bespoke, confusing and in many cases paper-based being put in place before data sharing can effectively commence.

This is hugely problematic for data recipients looking to service business consumers and reinforces the continued use of existing data sharing channels

like screenscraping and proprietary bank feeds. Until there is some level of standardisation as to how a Data Holder must meet their regulatory obligations we will continue to see limited uptake of CDR by businesses. Alternatively, a solution akin to that used for Joint Accounts could be implemented where all those who have online access to a business bank account have data sharing capability automatically set to 'on'. This should be the case regardless of when their account was opened.

Prescription versus principle-based rules

As a general comment, the Rules are inappropriately prescriptive towards ADRs and principle-based towards Data Holders. This approach does not align with the needs and incentives of the different parties.

The Rules are very prescriptive around how **ADRs** are required to act and operate in the system. This includes in regards to how CDR data can be used, how OSPs can be engaged, how consents must be sought, what security assessments can be relied upon for accreditation, etc. This level of prescription significantly inhibits the ability for these participants to drive innovation and create new services - a key goal of the CDR system. If the current prescriptive Rules were replaced with broader principle-based consumer protections (like the consent objectives at rule 4.9 and the Data Minimisation Principle at rule 1.8) then there would be greater ability for ADRs to innovate and consumers to benefit.

Conversely, the Rules are more principles-based in respect to how **Data Holders** must comply with their obligations. Examples of this include the processes for adding nominated representatives, requirements around authentication, etc. Though we can understand that this is in order to ensure that Data Holders may continue to comply with existing regulations and do not face excessive implementation costs, it has fostered uncertainty around compliance and ultimately resulted in a variety of inconsistent and incoherent practices across different Data Holders. Making the rules relating to Data Holder obligations more prescriptive would give Data Holders, ADRs and consumers greater certainty around the processes that must be implemented by these providers.

Extended consent durations:
Adatree generally supports extending the maximum duration for use consents for business consumers to 7 years. To enable a more streamlined consumer experience, we think it would also be worth extending the maximum duration for collection consents and authorisations to 7 years as well. Most business arrangements are measured in a matter of years, rather than weeks or months. Extending the maximum duration for collection consents and authorisations

would assist in further removing additional friction that there would be in transitioning to CDR from screen scraping where no such limitations exist.

We note that this solution may not entirely resolve the issue of a business consumer having their service interrupted by failing to renew consent and having all of their data deleted. It may therefore be worth including a provision that specifies that an ADR who has been provided a business consumer statement may retain CDR data held in relation to that statement for a specified period past the expiration of consent before that CDR data becomes redundant data. We appreciate that this could result in confusion for the consumer in tracking and managing their data and so would require additional rules relating to details that must be provided through their dashboard and notifications. This should only apply in instances where the consent has expired, not where the consumer has revoked or withdrawn their consent.

Adatree also considers that longer maximum consent durations should be made available to non-business consumers as well. There are already a significant range of requirements in place to ensure that a consumer remains aware and in control of how their data is being used, including consent receipts, the 90 day notification requirement and the ability to request CDR data to be deleted at any time. These requirements should reduce the need for the system to rely on heavy-handed limitations through maximum consent durations. Additionally, though the consequences of failing to re-consent to a CDR service are often likely to be less severe for a non-business consumer than a business consumer, it will still be incredibly frustrating for a consumer if all of their CDR data is immediately and unintentionally deleted (including derived data which the consumer may have themselves devoted significant amounts of time and energy to collating and improving).

Outsourcing arrangement changes:
Adatree supports the proposed changes to CDR outsourcing arrangements enabled through rule 1.10. The Rules previously imposed inappropriate restrictions on the commercial and technical relationships that an ADR Principal could enter into with its OSPs, despite the ADR bearing ultimate regulatory responsibility and providing a clear point of recourse for consumers. These changes provide a more appropriate stance to outsourcing, where the ADR maintains regulatory responsibility for the actions of those it brings into the CDR but is free to structure its commercial and technical processes in a way that best serves its specific business needs. For instance, we understand that the following outsourcing arrangements would now be permitted under the proposed amendments:

Figure 1.1 - Commercial arrangements

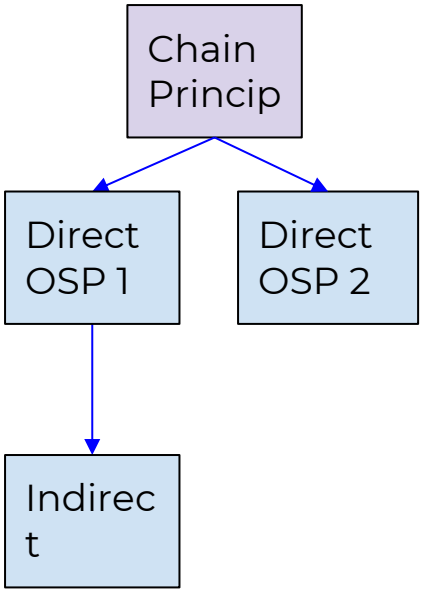

Figure 1.2 - Regulatory arrangements

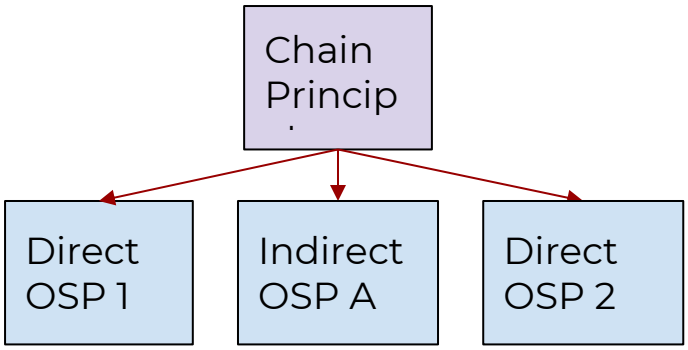

Figure 1.3 - Technical arrangements

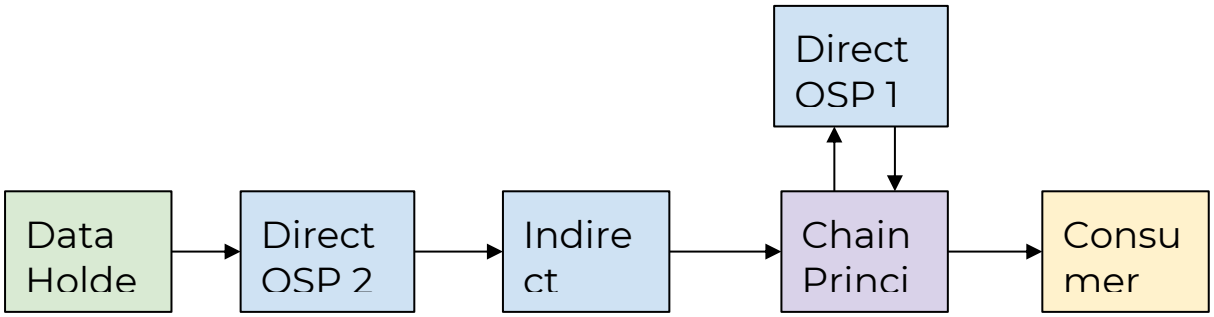

Figure 2.1 - Commercial arrangements

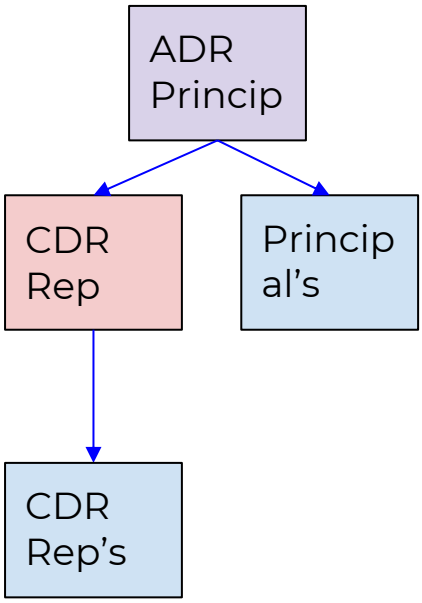

Figure 2.2 - Regulatory arrangements

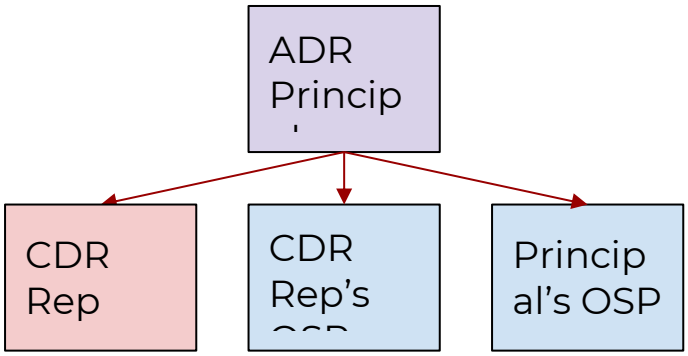

Figure 2.3 - Technical arrangements

OSPs play a valuable role in the CDR ecosystem by facilitating specialisation and minimising the risks associated with ADRs being required to undertake highly technical functions 'in house'. It is often significantly safer, cheaper and more

reliable for an ADR to outsource certain functions like data collection, de-identification or categorisation to a specialised third-party partner. By removing inappropriate restrictions on how an ADR can structure its OSP arrangements, these changes will increase the ability for the CDR to facilitate the safe and secure delivery of new and diverse customer services.

During the Treasury's Rules consultation forums it was raised that these changes could increase complexity for a consumer in understanding how their data may be used or increase issues for the consumer in managing their data sharing arrangements. We disagree that these changes will exacerbate these issues. The Chain Principal is still responsible for detailing to the consumer any OSPs that their data may be shared with, including during the consent flow, in their CDR Policy and in the CDR receipt. An OSP can already further outsource services under the current Rules so, if anything, these changes will actually make it easier for a consumer to understand how their data is being used.

Another point was also made in the aforemention Treasury forum that Data Holders will not be automatically provided with information about an ADR's OSP arrangements or how their data will be used 'downstream'. We think that limiting the amount of information that is automatically shared with a Data Holder is appropriate and in line with the CDR's general ethos that the consumer is in control of who their data is shared with and how their data is used. For instance, it is not necessarily appropriate or relevant for a Data Holder to know if a consumer is sharing their data with a comparison website to find a better provider.

We do, however, think that improvements could be made to ensure that a consumer can track their consents from a location of their choice. As the CDR expands to the telecommunication sector, non-bank lending sector and beyond this will become more and more important.

To increase comprehensibility, we ask that clearer defined terms are included for the different kinds of OSPs, and that there be distinct terms used for 'Principal' in CDR Representative arrangements and in OSP arrangements. We also ask that the final explanatory materials include both diagrams and examples to demonstrate how a chain of CDR outsourcing arrangements may look and to clarify what kinds of disclosures would be permissible - particularly when these chains include a CDR Representative. Such examples would be hugely beneficial for promoting a consistent interpretation across industry.

Though we do think that the changes to rule 1.10 will be beneficial for the CDR by increasing the ability to leverage third-party expertise, we have some concerns around the legislative complexity that they have introduced. In our experience, more complex rules can introduce opportunities for unintended limitations that lead to consequences down the line. We wonder whether the same outcome of reduced prescriptiveness around OSP arrangements could be achieved by simplifying the existing Rules, rather than introducing new rules. While we support the changes being progressed largely as written - given their significant value in increasing flexibility for participants in the system - we do ask the Government to consider whether there may be opportunities to reduce the Rules' complexity as they continue to be refined in future.

CDR Representative changes:
Adatree agrees with the changes to rule 1.10AA to allow CDR Representatives to have their own OSPs, noting that the ADR must maintain effective regulatory responsibility and approval for any such arrangements.

We seek clarity as to the regulatory role of a CDR Representative's ADR Principal where that CDR Representative engages an OSP. The Rules indicate that in such a case the CDR Representative will be the Chain Principal, however this is confusing when the CDR Representative is responsible to yet a higher Principal who takes regulatory responsibility for their actions. Though we agree with what we understand to be the proposed outcome - where the ADR Principal takes on regulatory responsibility for the CDR Representative and through transitivity all of their Direct and Indirect OSPs - we do think that this could be made clearer. This confusion could be partially addressed through our suggestion that there be clearer defined terms and distinct terminology for 'Principals' in OSP and CDR Representative arrangements.

We also seek to clarify that a CDR Representative would not be prohibited from using an OSP to collect CDR data from its Principal when its Principal has given it authority to do so. The Rules changes clarify that a Principal may disclose CDR data to its CDR Representative through an OSP (rule 1.10(2)(b)(ii)), but are quite unclear as to whether a CDR Representative can collect data from its Principal through an OSP as in figure 2.3 (rule 1.10AA(3) Note). From both a regulatory and technical perspective there is no difference between a Principal disclosing data to a CDR Representative through an OSP and a CDR Representative collecting data from its Principal through an OSP. This is purely a commercial difference. As such, we argue that both models should be permitted.

Adatree does not support the proposed changes to allow CDR Representatives to disclose data under disclosure consents. This increases the risk that the CDR Representative's Principal will be unable to effectively monitor and limit how its CDR Representative may share consumer data both within and outside the CDR system. Expanding the scope of the Rules in this way will introduce an untenable risk to consumers. Though we acknowledge that a CDR Representative would only be permitted to make such disclosures with consumer consent and when doing so is an authorised service under the CDR Representative arrangement, we consider that it is necessary for some functions to be reserved for those who have gone through the full accreditation process and who have their own direct CDR obligations. Only those persons with unrestricted accreditation can be guaranteed to have the appropriate degree of regulatory oversight to ensure that they are incentivised to act responsibly and have fully satisfied the CDR's requirements. This distinction between what is possible for a CDR Representative and a fully accredited ADR is required to ensure that, across the entire system, incentives are aligned appropriately to ensure the disclosure of CDR data is done in a responsible way.

If the Government is committed to allowing CDR Representatives to disclose CDR data, then we argue that they should at least be limited from using the new business consumer disclosure consent. We think that such a limitation is reasonable given the amount of detailed information that could be inappropriately disclosed. Clear guidance should also be provided in relation to how a consumer must be made aware of the roles of the different participants when a CDR Representative seeks to make a disclosure consent.

Though we welcome these improvements to the CDR Representative model, further changes are still required to promote consumer understanding and engagement. For instance, the Rules should not require a CDR Representative to 'adopt' their Principal's CDR policy (rule 1.10AA(4)(f)). A single CDR Principal may have multiple services, CDR Representatives and OSPs listed in its CDR policy which are entirely irrelevant to the use case provided by a specific CDR Representative. A single CDR Principal may even sponsor competing CDR Representatives who should not need to reference each other in the policies they present (though the Principal should of course still need to include the details of both in their own CDR Policy). Requiring all of this information to be provided to a consumer will only serve to confuse them. A CDR representative should only be required to provide the details from its Principal's CDR policy that are relevant to the service they provide. The CDR Representative should also be able to clearly brand such policies with their logos, etc.

Additionally, while we welcome the steps taken at Division 4.3A to clarify how CDR Representatives must seek consumer consent, we think that further work is needed to reduce the prescriptiveness around how CDR consents must be sought generally to ensure the required processes are in line with consumer expectations and industry practices. We understand that work to this effect is being undertaken by the Data Standards Body and we ask that this be progressed as a priority. This is particularly important for those businesses seeking to act as CDR intermediaries, where their primary role is to provide backend functionality to enable access to the CDR and to CDR data.

Relatedly, details about a CDR Representative are currently not included in the Data Holder's authorisation process (Division 4.4). The CDR Representative model assumes that the consumer's primary relationship is with the CDR Representative and not the Principal, so only displaying details about the CDR Principal in the authorisation flow leads to significant consumer confusion. As the purpose for disclosing the CDR Representative's details to the Data Holder is to improve the consumer experience, we think it is reasonable that this information be provided.

Finally, we strongly advocate that anyone seeking to take on a CDR Representative should be required to have a third-party management framework as is required for those seeking to sponsor an Affiliate (Schedule 1, Part 2, Rule 2.2(1)(a)). Sponsoring an Affiliate introduces a lower degree of risk to consumers and the system than taking on a CDR Representative, so requiring a third-party management framework in both instances would be measured and appropriate. This framework should set out how the Principal will meet their positive obligations under rule 1.16A to ensure that any CDR Representatives are complying with their CDR requirements. An accredited person should be required to provide their framework to the ACCC prior to their being permitted to enter into any CDR Representative arrangements, as well as at regular intervals thereafter (e.g. 6 monthly). To assist with this, greater guidance should be provided in either the Rules or supplementary regulatory materials as to what due diligence an accredited person should be expected to undertake when taking on a CDR Representative, as well as what practices or processes would not themselves be deemed sufficient.

Trial products:
Adatree supports the proposal to allow Data Holders to create trial products that do not attract Data Holder obligations for a period. This will allow for greater

innovation by Data Holders and assist in reducing unnecessary regulatory burden. The time and participant parameters should be increased to ensure they align with existing industry practices. The Rules should not specify what terminology must be used when communicating to the consumer that a product is a trial product - just that the description must make clear that it will serve the purposes of a trial product and that CDR data in relation to the product may not be available (rule 1.10E(1)(b)(i)). This is because it is common to use a variety of other terminology in product development like beta, limited release, internal testing. It is our view that this should be extended to all current and future designated sectors, not exclusively to banking.

The Government should also consider how the Rules could be amended to allow small providers to more easily trial ideas and build proofs of concepts using CDR data through limited access to the system. Many innovators looking to explore CDR are small and do not necessarily have the capital to devote to proving their conformance against the CDR's bespoke and non-mutually recognised requirements. In many cases, these providers are forced to abandon the CDR in favour of other data access models like screen scraping. Rules changes to the CDR Representative model could facilitate this by requiring a Principal to ensure that their Representative meets the controls set out in Schedule 2 only after the Representative has received a certain number of consents, has been in the system for a specified period of time or intends to publicly offer a CDR service (whichever comes first). In such a case, the Principal's third-party management framework should need to include details of how they would minimise risks relating to any CDR Representatives offering such trial products. The Principal would remain responsible for all technical communication with the register and any Data Holders, meaning risks to other participants or the overall CDR system would be limited. The CDR Representative would also need to clearly communicate the potential risks to any consumers prior to the consent process. Permitting such an approach would allow prospective data recipients to understand whether the CDR would support their business model, while limiting risks to consumers and the system at large. CDR does not exist in a vacuum and unless there is a way for smaller players to use the system to innovate, there will continue to be demand for screen scraping.

CDR Telecommunications:
Adatree is excited to see the CDR continue to be extended to new sectors, and welcomes the draft CDR Telecommunications Rules at Schedule 5.

We are broadly supportive of the types of data that will be included under the relevant data clusters. We do however think that there needs to be some increased clarity around how information about bundled products will be included, given the importance of this information for use cases like comparison services and switching. Our current understanding is that basic details about other products bundled with a 'relevant product' (e.g. hardware like a phone, additional benefits like Foxtel, etc) would be included under *billing data* and *product specific data*. We think it will be necessary for there to be a level of specificity required around how information about bundled products must be provided (either in the Rules or Standards). For instance, it will be vital that I understand the make and model of any hardware included in a bundle, not just that the bundle includes 'a phone'. We also understand that the detail provided around these bundled products will be limited. For instance, the fact that a consumer's internet plan comes with Foxtel would be apparent, but no details would be provided around how often this service is actually used. While we consider that it would be beneficial for consumers to have additional information on these bundled products included, we note there may be limitations around what is permitted under the existing designation instrument.

It is our view that eligibility for CDR telecommunications being limited to those with an associated account spend below $40,000 is too restrictive and will likely exclude a significant number of small and medium sized businesses from benefiting from CDR. A business seeking to provide phones to as few as twenty five employees could be put over that limit. This is particularly the case given our understanding that all spending on bundled services will be included as part of the customer's total account spend. We suggest that this threshold be raised to $200,000 per annum in order to better service more customers.

We also argue that the proposed de minimis threshold of 30,000 services in operation is too high and should be reduced. Maintaining this threshold will mean that a substantial number of consumers will not be able to benefit from sharing their telecommunications data. Additionally, as consumer data sharing increases the ability for smaller providers to become more competitive and win new customers, it will be important that any consumers who do switch remain able to share their data. We therefore argue that a threshold of 10,000 services in operation would be more appropriate.

It is also not immediately clear from the Rules or explanatory materials how those providers who operate as a secondary brand or any whitelabelled product

providers of an initial carriage service provider (CSP) - such as iiNet for internet services or Kogan Mobile for mobile - are intended to be incorporated into the system. As with Open Banking, it is our view that the best consumer experience will be achieved through customers engaging with the brand with whom they have a relationship - rather than the underlying parent provider. We also consider that it would be appropriate for some larger brands of initial CSPs to be included in the tranche 1 date alongside their parent company, such as Vodafone.

We note that rule 3.2(1)(c) refers to 'partnership accounts'. We seek to confirm that this will include all kinds of business/corporate accounts, noting the importance of CDR being available to businesses as well as individuals. (We understand this to be the intention of the rule and that this terminology appears to be in line with what has been used in the Banking Sector under Schedule 2 rule 3.2, but we think that in this instance it is necessary to confirm this).

We also note that there appears to be a typo in rule 5.6(3), with large CSPs needing to commence their Part 4 obligations from the tranche 1 date, rather than the tranche 2 date.

Additional issues and comments:

- The changes to the Rules appear to clarify that a Principal will be responsible for any breach of the Privacy Safeguards by their OSP, however the way this is done is not appropriate. The proposed changes to the Privacy Safeguard rules will mean that, for an OSP with multiple Principals, every Principal will be equally liable for a breach by an OSP. This is not appropriate as an OSP may fall foul of the Rules due to the actions of a single Principal - for instance an OSP may unknowingly be provided and use data containing government identifiers by a non-complaint Principal (breaching Privacy Safeguard 9). In such an instance, only the relevant Principal should be considered to be in breach.
    - The structure of these amendments appear to replicate the shared liability structure for CDR Representatives. A CDR Representative can only ever have one Principal though, meaning that the issue of multiple Principals being able to be indicted would not apply.
- Rule 7.12(2) requires CDR Reps and OSPs to direct any other 'person' who has received CDR data to delete it. This breadth is inappropriate, as it includes those that the consumer has explicitly allowed the data to be shared with, including TAs and CDR insight recipients
- The Rules relating to CDR Representatives and CDR OSPs should require that they delete any CDR data they have received should their CDR arrangement with their Principal terminate. This should be viewed as being equivalent to the treatment of an accredited person who has had their CDR accreditation revoked (rule 5.23(4)).
- Additional professional classes should be eligible to receive CDR data as Trusted Advisers. Consideration of which classes should be added should take into account their existing need to access equivalent data and the benefits to consumers from having this enabled through the safer CDR channel. Classes for immediate consideration should include lenders and other ACL holders beyond mortgage brokers, as well as APRA regulated providers like ADIs and general insurers. Data Holders for a specific sector should also be classified as a TA to enable them to securely receive data relating to that sector without needing to become accredited.
- The CDR Insights model needs to be reworked to make it more fit for purpose. Key requirements are that it needs to be sector agnostic, commensurate to the risk posed, and not whitelist acceptable use cases. The Rules should be changed to have only two classes of CDR insights - 'verification insights' for sharing factual information that a consumer could reasonably understand and provide themselves (e.g. their name, address, BSB, account balance, energy usage over a quarter, current rate), and

'assessment insights' for recommendations, scores, and other derived data which is created through ADR analysis and which the consumer could not reasonably recreate themselves (e.g. a credit score, a recommendation, an eligibility assessment, a ranking). Any limitations on acceptable use should be incorporated through a black list of banned use cases (such as rule 1.10A(3)(b)), rather than a white list of permissible use cases. This guarantees CDR insights are sector agnostic and don't need to be updated for each new sector. Disclosing CDR data as a CDR insight should remain consent driven, but this consent process should be commensurate to the risk of the data being disclosed. ADRs should equally be able to receive and use CDR insights 'outside' the restrictions imposed through the CDR.

- Many of the issues raised during the Treasury's Rules discussion forum focused on how to best enable better consent management. Empowering a consumer to choose how they manage their consent data could:
    - allow business consumers to have full visibility of the data shared by their nominated representatives, even when these consents have different timeframes;
    - provide a consumer driven way to maintain visibility of all the consents they have given to different ADRs (and not requiring that this information automatically be disclosed to Data Holders); and
    - enable consumers to more easily track their consents as CDR extends to more sectors.

  If changes to improve consent management are to be progressed, it will be important to ensure that it is done so in a way that does not put undue stress on CDR participants.