TELSTRA CORPORATION LIMITED

Submission to Treasury consultation on

Treasury Laws Amendment (Consumer Data Right) Bill 2018

Public version

12 September 2018

CONTENTS

01 Introduction

We welcome the opportunity to comment on the exposure draft of the legislation enabling the Australian Government's proposed Consumer Data Right (**CDR**).

We have previously expressed our in principle support for the Productivity Commission's recommendations regarding data availability and use in Australia. In doing so, we have focused on the proposed introduction of a CDR as a way to promote consumer interests and help drive competition and innovation across the economy. We are also very supportive of the government's regulatory reforms aimed at greater availability and use of government-held data.

We believe these data reforms could help establish and normalise a safe environment that is trusted by consumers, within which private and public enterprises can use data to the betterment of consumers and the economy. Improved use of consumer and government-held data has the potential to lead to the creation of new products and services, increased productivity, and new and more efficient ways for customers to interact with suppliers.

While there is a wide range of potential benefits to be derived from access to data, there are three key barriers to achieving these benefits:

- the availability of data itself, under existing legislative and regulatory frameworks;
  `
- prevailing safety and trust concerns, about the use, sharing and release of data, which are heightened by high profile cases involving data breaches and data misuse; and

- the availability of low cost ways for firms to participate (use data) in a safe and trusted environment (including ways that achieve the benefits associated with improved data availability while minimising the associated regulatory burden).

The CDR exposure draft legislation seeks to address the first barrier, by increasing the availability and portability of consumer data, and the second barrier, by providing for CDR privacy and data standards frameworks.

However, we have concerns about a number of aspects of the draft CDR Bill. It is overly complicated and broad in scope; even so, it does not adequately address the second and third barriers mentioned above, potentially undermining the benefits the exposure draft seeks to achieve.

The remainder of our submission is structured as follows:

- **Section 2**: considers the application of the CDR to the communications sector, including discussion on the process for designating sectors and the associated complexities;
- **Section 3**: explains why the CDR regime should **not** capture value-added data;
- **Section 4**: addresses the implied assumption in the CDR Bill that the CDR data holder is always the service provider;
- **Section 5**: explains our concerns regarding the proposed CDR privacy regime;
- **Section 6**: raises concerns with the proposed extension of the ACCC's section 155 powers for the purposes of the CDR regime; and
- **Section 7**: contains some additional recommendations to improve the implementation of the CDR regime.

02 Application of the CDR to the communications sector

2.1. Benefits of adding communications sector will be different from other sectors

The telecommunications sector already incorporates mechanisms for access to, and sharing of, data. Suppliers offer plans for broadband and mobile services that make the customer's choice between providers very simple. For example, many suppliers offer plans with simple monthly fees, often without the requirement to contract, and with minimal incremental transaction costs. Customers, including business and enterprise customers, switch regularly between suppliers, and even those who don't regularly make informed decisions to stay with their current provider after assessing competitive offers.[1]

Customers also have many mechanisms to receive the types of data envisaged under the CDR regime, in order to facilitate their decision-making. For example, customer bills already detail the user's consumption (calls, SMS, data usage) at a granular level, and this information can be taken or forwarded to other suppliers in the industry for the purpose of obtaining a competitive quote. Beyond this, individual and business customers often have access to more information about their telecommunications consumption than their providers do – for example, mobile phones store calling histories for calls made on the provider's network, as well as via apps like WhatsApp and Viber; they also store data usage information, including information broken down by different apps.

In addition, the telecommunications sector contains mature processes and regulation facilitating switching from one supplier to another, including number portability processes, and a range of ACMA and ACCC determinations underpinning a strongly competitive market in which switching between competitors is already high.

The telecommunications sector has undergone multiple policy, regulatory and commercial transformations over the last two decades that have led to a very competitive sector. In that context, the benefits of applying the CDR regime to the sector will lean more towards building trust in the sharing and use of data by public and private enterprises to enable the creation of new products and services, productivity improvements, and new and more efficient ways for customers to interact with suppliers.

2.2. The process for determining whether a sector is designated

The designation of sectors by the Minister is appropriate in this context. The ultimate decision to add a sector into the CDR framework could have significant consequences, and is one that must include Parliamentary oversight to take into account the broad range of economic and social factors that go beyond the scope and experience of any delegated regulatory authority.

There are additional issues in the draft legislation in relation to the designation process. These issues need to be addressed to protect customers and taxpayers against a situation where they ultimately incur the additional costs faced by their suppliers of participating in the proposed framework for little or no benefit relative to existing alternatives.

Firstly, the factors to which the Minister and ACCC must have regard in making or advising on a decision to designate a sector must include consideration of the cost to potential data holders of contributing data within the framework. While the draft legislation requires a number of factors to be taken into account, including the likely regulatory impact (section 56AD), this is a broad term and could potentially be satisfied with minimal consideration or analysis. Accordingly, the legislation should specifically require the ACCC to undertake a quantitative cost-benefit analysis for each sector. The ACCC is a very

[1] Switching is also supported by Government policy. For example, with the roll out of the Government's National Broadband Network (**NBN**), every customer migrating from Telstra's network to the NBN has a free and open choice as to which retail service provider they want to migrate to.

experienced economic regulator and is familiar with completing such analyses. Without a requirement to show that the quantified benefits outweigh the quantified costs, it would be difficult to establish or sustain that society is better or worse off with a specific sector designated. Additionally, given the potential complexity of the proposed CDR framework, a much better understanding of the cost of implementation is needed, to ensure no sector is subject to unnecessary cost for little benefit.

Secondly, customer- and industry-led alternative frameworks and customer applications that meet the objectives of the CDR regime already exist in some sectors, and should be considered by the Minister and the ACCC in any decision or advice to designate a sector. For example, the Telecommunications Numbering Plan[2] requires all carriers and carriage service providers to implement number portability for fixed and mobile services. This ensures that technical barriers to customers switching (a principal objective of the CDR regime) is already satisfied within the communications sector. The Telecommunications Consumer Protections (**TCP**) code requires suppliers to provide critical information summaries (short but detailed information plans) to customers at the time of sale. Further, in relation to CDR data itself, mobile devices already log all incoming/outgoing call/SMS/MMS details, both on native call/SMS/MMS applications and over-the-top (**OTT**) applications (e.g. WhatsApp™ and Facetime™), as well as logging data consumption, often on a "per application" basis. This level of detail far exceeds information that could be gathered by a service provider for compliance with the CDR regime, given the service provider has no visibility of calls/messages from OTT applications or of data consumption at a "per application" level of granularity. Consideration of pre-existing industry regulation and codes that meet the objectives of the CDR regime, along with technical alternatives (that could exceed the granularity of information able to be collected by a service provider) should be included in section 56AD.

Thirdly, it appears that there is no express obligation upon the Minister to publish supporting reasons for designating a sector (sections 56AD and 56AE) before making the instrument. While we acknowledge the instrument designating a sector is a disallowable instrument[3], the draft Bill should be amended to include a requirement that the Minister publish supporting reasons with sufficient period for comment prior to the instrument being tabled in Parliament. Supporting reasons should include details of the cost benefit analysis demonstrating that society is better off with a specific sector designated.

2.3. The proposed CDR framework will not keep up with changes in the communications sector

The communications sector is very competitive and fast-paced. The complex and static nature of the proposed framework, if had been applied even two years ago, would not have been able to adjust to changes that have recently occurred in this sector, and will not cope with future change. Nowhere else in the world has a CDR been applied to the communications sector, and we caution a much simpler approach is needed to achieve the stated objectives.

Below are just some examples of the changes in technology, services and customer plans that could directly impact a static implementation of the CDR:

- nbn has introduced speed tiers for broadband plans, and has recently varied those speeds for fixed wireless customers;
- Telstra is rolling out hybrid modems, so that customers get both fixed and mobile connectivity from their modems;

---

2 Telecommunications Numbering Plan 2015, ACMA. https://www.legislation.gov.au/Details/F2016C00283

3 Telstra understands that the Minister would be required to issue a Regulatory Impact Statement for any such designation: see Australian Government Guidance Note, *Australian Government Regulation Impact Statement Preliminary Assessment Form: Is a RIS Required*? dated September 2017, available at https://www.pmc.gov.au/sites/default/files/publications/003_AG_Preliminary_Assessment_Form_1.pdf

- Facebook™, WhatsApp™, Skype™ and other providers provide voice a higher volume of messaging than the traditional telecoms, and they also provide competitive voice calling services;
- the prices for calling and messaging are now zero for many plans in the market, and may no longer feature in the purchasing decisions of many customers; and
- streaming video and other value-added services are regularly bundled into plans.

We recommend that the draft legislation be reviewed to allow a much simpler approach to satisfy the requirements of the CDR for any designated sector. This could mean a customer- or industry-led framework for data sharing may be used as a substitute for the standards imposed by Data61. One way to achieve this is to formally recognise alternative frameworks and switch off parts of the CDR framework when an alternative exists. Another way is to make the standards a self-regulatory mechanism, with the ability for the standards to be imposed should the self-regulatory mechanism fail.

2.4. The right to data portability should not adversely affect the rights and freedoms of others

Telecommunications data potentially contains additional complexities not present in other sectors. There are two key scenarios:

- products and services in the telecommunications sector can involve a “one-to-many" or a “many-to-one" relationship between the “owner” of the service and the user(s); and
- products and services in the telecommunications sector may contain information related to third parties where transfer of that information could result in it being used for purposes not authorised by the third party.

In the first scenario, there can be a single owner with multiple users on a single service, such as a fixed-line broadband service in a family home or other multi-occupant dwelling such as university students sharing accommodation. Assuming the owner (purchaser) of the broadband service elects to become a CDR consumer by authorising the transfer of the CDR data for that service, then some of the CDR data will relate to third parties. The presence of multiple people at a single address is beyond the visibility and knowledge of the service provider and, as such, it is not possible to devise a mechanism to allow data to be segregated.

The reverse can also occur. There can be multiple “owners” with a single user, for example, an employer supplying an employee with a mobile phone. Often in this situation, employers allow employees some amount of personal use. Does the employer have to obtain the employee’s consent before authorising data related to that service to be transferred under the CDR regime? Alternatively, does the employee have to obtain their employer’s consent before authorising the contacts list stored in the phone to be transferred under the CDR regime to another application such as WhatsApp™? It would appear that **Privacy Safeguard 5** may be attempting to address this scenario by compelling a data holder to notify *each* CDR consumer who may be the subject of CDR data. However, when a mobile phone is supplied to an employee by their employer, the service provider is unlikely to have any knowledge that the “user” of the phone service (the employee) is different from the person who is the registered owner of the service (the employer), and so providing notification to the employee is unworkable. There are many other parallel examples, including people who purchase a mobile phone service in their own name for a child or an elderly parent.

In the second scenario, the potential for data portability to impact upon the rights of third parties exists where a CDR consumer creates a directory of contacts as part of their service, and authorises the transfer of the directory to a new service provider to facilitate switching to that provider. While parallels to this example exist in other sectors (for example, a CDR consumer may have created a directory of BSB/Accounts for entities they regularly transfer money to), we suggest that the risks of misuse of directory information (phone numbers, email addresses, etc) created in a telecommunications context is

potentially more susceptible to misuse for marketing purposes by a gaining data recipient. Again, it would appear that **Privacy Safeguard 7** is attempting to address this scenario. However, it only requires a valid consent to have been obtained from the *CDR consumer*, and not from any third party referenced by the CDR data. We suggest that this is an insufficient safeguard in this context, as the CDR consumer is not empowered to authorise the use of CDR data (for direct marketing purposes) when they are not the *subject* of that data. This was at the root of the Cambridge Analytica/Facebook controversy, where a Facebook user consented to their data being used for analysis, but in the process, Cambridge Analytica was able to obtain data relating to third parties known to/referenced by the consenting Facebook user.

03 The CDR should not capture value-added data

3.1. Value-added data is not required to facilitate competition

Value-added, inferred or derived data results from the intellectual, technological and financial investments companies make in their businesses, for a range of purposes such as improving products and services, identifying new product opportunities and markets, or to achieve business efficiency gains that lower costs. Ultimately, the benefits resulting from investments in data and its analysis accrue to consumers through more competitive offerings, or new products and services better suited to the needs of consumers.

Also, data of this type is not required to facilitate competition, or to facilitate transfer of data to applications such as accounting software, consumption tracking or household budgeting. The data required to achieve the objectives of the CDR regime is, at most, raw transaction data (and could be further limited to data that is required to facilitate competition and is not already available to and shared by consumers under an alternative framework). The EM states that it is necessary to include data "…*that has been derived from CDR data, such as financial reports compiled from transaction data*…".[4] The transaction data, inclusive of any service provider initiated transactions, is sufficient for an accredited data recipient to compile their own financial reports, or indeed, any other report or aggregation necessary.

The same applies in the telecommunications sector, where the transfer of transaction data (details about calls, SMS, data consumption) can be aggregated by the accredited data recipient to form an accurate understanding of the CDR consumer's consumption (for the purpose of competitive quotes), or can be directly loaded into analytical software for any other purpose as authorised by the CDR consumer.

3.2. Socialising value-added data with competitors will reduce business investment in data and analytics

Forced disclosure of value-added data (including derived and inferred datasets) to competitors, even on a "per consumer" basis, risks undermining investment by businesses in competitive markets, and will reduce investment in data and its analysis.

The Impact Assessment (**IA**)[5] for the UK midata scheme is a valuable point of reference for consideration when determining the scope of data that should be captured under Australia's CDR regime. The IA notes the consumer transaction data held by firms is valuable commercial information, and the existence of a power compelling firms to release this data "*may reduce their incentive to collect the information*". This is referred to as a potential "chilling effect". The IA states that, in order to minimise this risk, the proposed power will only refer to the disclosure of "*'raw' factual information*".

---

4 Treasury Laws Amendment (Consumer Data Right) Bill 2018, Exposure Draft Explanatory Materials, paragraph 1.47, in reference to schedule 1, item 1, subsection 56BB and 56BC of the legislative amendments.

5 Department for Business Innovation & Skills, Cabinet Office Impact Assessment for midata 2012. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/32689/12-944-midata-impact-assessment.pdf

04 The CDR should expressly contemplate solutions where the CDR data holder is not the service provider

There is an implied assumption in the draft Bill and associated EM that the CDR data holder is the service provider. Section 56AG(1) defines the CDR data holder as the person (or class of persons) nominated in the instrument used to designate the sector (as required under section 56AC). Paragraph 1.39 of the EM, in referring to section 56AG(1), states that: "*Generally speaking, a data holder will be the entity that generates or collects the initial transaction records or data*." While this does not prohibit an entity outside of the direct service provider being a CDR data holder, it does set an expectation that the service provider will be the CDR data holder.

As we noted in section 2.2 above, in the telecommunications sector, there is a variety of ways in which CDR data could be collected, and further, some of that data can only be collected from sources outside the visibility and control of a telecommunications service provider (e.g. from the OTT service provider, or via a third-party application resident on a device such as a mobile phone).

In addition to our recommendation in section 2.2 above (that section 56AD be amended to include consideration of industry regulation and codes and/or technical alternatives that satisfy the objective(s) of the CDR regime), we also recommend that section 56AG(1)(a) also be amended to note that the CDR data holder may not be the provider of the service specified in the instrument that designates a sector.

05 Parallel privacy regime will be difficult operationally, and confusing for consumers

The CDR Bill proposes to introduce a new set of Privacy Safeguards, which are similar to but more restrictive than the Australian Privacy Principles (**APPs**), cover a broader set of information than the APPs, extend to entities such as businesses (in addition to natural persons), yet only apply to CDR participants under certain circumstances.

Telstra is concerned having parallel privacy regimes in the *Privacy Act 1988* (Cth) (**Privacy Act**) and the *Competition and Consumer Act 2010* (Cth) (**CCA**) will be difficult to work with for data holders, accredited data recipients, and consumers. The relationship between the APPs and the Privacy Safeguards, and the way in which they work together, is unclear and will likely give rise to questions and uncertainties about which regime applies when, and the differences between the two.

In particular, we note the following issues:

- Whether the APPs or the Privacy Safeguards apply to particular data may change back and forth over time, as a result of decisions made by the CDR consumer. Example 1.14 in the EM provides a good case in point. In that example, Meeks Banking Services must initially treat George's CDR data in accordance with the Privacy Safeguards. However, when George closes her savings account with AnnaBank and opens a savings account with Meeks, Meeks is able to treat all new and historical data about George's savings account in accordance with the APPs.

- In isolation, this example may not seem overly complex. But it is not hard to imagine other scenarios that would give rise to more complex considerations about whether the APPs or the Privacy Safeguards apply. For example:
    - What would happen if George kept her savings account with AnnaBank, and opened another savings account with Meeks?
    - What would happen if Meeks collected data about George relating to five bank products, but George only switched to Meeks for one of those products?

- What would happen if George were a business customer, to which the APPs do not apply, but the Privacy Safeguards do?

- Whether the APPs or the Privacy Safeguards apply matters. This is because, while the Privacy Safeguards are drafted so as to be "comparable to the protections for individuals contained in the APPs"[6], the Privacy Safeguards contain more restrictive requirements than the APPs. This means that, at different points in time, more or less restrictive requirements may apply to exactly the same data sets.

- Consumers are also likely to find it difficult to navigate the different privacy regimes applying to information about them. To take an obvious example, Privacy Safeguard 1 requires CDR participants to have a clearly expressed and up-to-date policy about the participant's management of CDR data (see section 56ED(4)). We expect that there will be a high degree of duplication between a company's privacy and CDR policies, and there is a strong risk that customers will be confused about the distinction and differences between the two.

- Also, if companies want to inform consumers about their privacy rights and how those change, then there might need to be multiple communications about different privacy obligations that apply at different times and throughout their relationship with their supplier. This will be confusing for consumers (and suppliers).

In addition, as noted above, the CDR regime and its Privacy Safeguards are designed to cover a broader range of information than that to which the Privacy Act applies. For example, as the EM states in paragraph 1.52:

> *"For the CDR regime, CDR data is data that 'relates' to a CDR consumer. The concept of 'relates to' is a broader concept than information 'about' an identifiable, or reasonably identifiable person under the Privacy Act. The term 'relates' has a broader meaning than 'about' and is intended to capture, for example meta-data of the type found not to be about an individual in* Privacy Commissioner v Telstra Corporation Limited *[2017] FCAFA 4 (19 January 2017). As such, where information is primarily about a good or service, but may reveal information about a consumer's use of that good or service, it relates to the consumer."*

In our view, the breadth of the CDR regime will introduce a range of additional questions and uncertainties for CDR participants – including:

- While the term "relates to" is supposed to be broader than the term "about", the bounds of the former are unknown and potentially far-reaching. This will introduce uncertainty into the CDR regime, and it is not clear that any such broadening will help achieve the stated objectives of the CDR regime. To use the example from paragraph 1.52 of the EM (quoted above), it is not apparent why "meta-data of the type found not be 'about' an individual in *Privacy Commissioner v Telstra Corporation Limited"* would be relevant to a customer considering switching away from their existing telco provider. An example of this kind of meta-data might be an IP address assigned to a device for a specific communication, which would clearly not have any bearing on possible offers to the consumer from another communications service provider.

- The broader the reach of the CDR regime, the greater the possible compliance issues associated with some of the Privacy Safeguards. For example, Privacy Safeguard 10 provides that a *"CDR participant for CDR data must take reasonable steps to ensure that the CDR data is, having regard to the purpose for which it is held, accurate, up‑to‑date and complete when the CDR participant discloses the CDR data in accordance with subsection 56EI(1) or (2)"*. There may be difficulties with this safeguard if, for example, certain types of network data such as location information are captured by the CDR regime and the way in which they are collected is intermittent.

[6] Treasury Laws Amendment (Consumer Data Right) Bill 2018, Exposure Draft Explanatory Materials, paragraph 1.19.

- We have previously raised our concerns about the application of a CDR regime to the telecommunications sector, where one service or account may be used by multiple people (e.g. flatmates sharing a broadband service, or multiple family members having their mobile services on a single account). The CDR regime raises the possibility of data being transferred at the request of one consumer which relates not just to them but to other people who share a service or account.

Beyond the Privacy Safeguards already referred to (in this section and section 2.4 above), the content of some of the other proposed safeguards raises further possible issues. For example:

- In Privacy Safeguard 3, the concept of an accredited data recipient "soliciting" CDR data has the potential to confuse. In circumstances where an accredited data recipient receives CDR data from a data holder at the request of a CDR consumer, it is not immediately apparent how the concept of "soliciting" CDR data fits in.

- Similarly, Privacy Safeguard 4 provides that an accredited data recipient who receives but did not solicit CDR data must destroy the CDR data as soon as practicable. The way in which in this safeguard is framed seems to impose an additional requirement for solicitation which, if not met, means the relevant CDR data must be destroyed. Again, this concept of "soliciting" has the potential to confuse in the context of the CDR. If a data holder transfers CDR data to an accredited data recipient at the request of a CDR consumer, our understanding is that should be sufficient for compliance with the CDR regime.

Overall, we are concerned that the introduction of a new privacy regime for CDR data will add another layer of complexity to an already complex set of laws and regulatory requirements governing the collection, handling and storage of information and data. In the telecommunications space, Telstra must comply with the Privacy Act in respect of personal information, and with the *Telecommunications Act 1997* (Cth) and the *Telecommunications (Interception and Access) Act 1979* (Cth) for certain types of telecommunications data. The proposed Privacy Safeguards, and the ability of the ACCC to make additional rules regarding privacy requirements for the purposes of the CDR regime, give rise to serious concerns about implementation and management of an appropriate compliance regime to capture these additional requirements for CDR data.

At Telstra, the customer is at the centre of everything we do, and we fully acknowledge and support the importance of ensuring privacy is protected. We remain concerned the CDR regime will not achieve wide adoption without consumer confidence in data privacy, and confidence will be very difficult to establish under a regime that is complex to understand.

We are strongly of the view more extensive consideration and consultation is necessary to determine an appropriate privacy regime for the purposes of the CDR. We are particularly concerned that the proposed Privacy Safeguards follow from a feature of the design of the CDR framework that proposes CDR data holders must transfer consumer data to accredited data recipients. It seems much of the complexity and many issues around privacy could be avoided if the draft legislation recognised alternative (and in some cases existing) frameworks whereby suppliers provide data to consumers who then have complete control over who they provide that data to.[7]

06 Concerns about extension of the ACCC's section 155 powers

The ACCC has broad powers under section 155 of the CCA. We note that, under the CDR Bill, the ACCC could exercise its powers under section 155 in respect of designating CDR sectors, which represents an extension of the ACCC's section 155 powers. We recognise that the ACCC is more

[7] An example of this is messaging transaction records. Customers hold records of their messaging transactions on their mobile phones from many service providers. Indeed, as noted above, customers hold more data about their transactions than any of their individual suppliers. The customer has complete control over who they provide that data to, and an alternative framework could make it quite easy for the customer to send that data, without the need for the proposed Privacy Safeguards pertaining to the CDR framework.

familiar with using these powers than is any other regulator. Notwithstanding, each exercise of the ACCC's section 155 powers imposes a significant burden on the recipients of such notices.

We believe there should be greater clarity for businesses and consumers about the circumstances in which the ACCC might delegate these section 155 powers to the OAIC (and to ASIC) and how (and why) the OAIC would administer such powers delegated to it by the ACCC as is contemplated by the inclusion of section 26(4) of the CCA. It is not obvious why the OAIC would need such powers.

In addition, we do not believe it is appropriate to empower the ACCC to delegate its section 155 powers to any "other person" (as is proposed by the addition of section 26(5) of the CCA). Given their coercive nature, the potential impact on notice recipients and the consequences for non-compliance, we consider that the grant of these types of powers should generally be left to Parliament, not delegated by one agency to another as the former sees fit.

07 Other recommendations

7.1. Clear principles and objectives for each CDR purpose

Based on the exposure draft of the Bill, the EM and the roundtable sessions convened by Treasury during the consultation period, the CDR regime appears to be trying to fulfil a wide range of purposes, including:

- Enabling consumers to more effectively use data relating to them for their own purposes (EM paragraph 1.14);
- Increase competition and promote market efficiency (EM paragraph 1.33);
- Enable consumers to 'harvest' the value of their data (EM paragraph 1.33);
- Reduce the cost to consumers of accessing data (EM paragraph 1.20); and
- Foster innovation (EM paragraph 1.20 and 1.33).

The absence of a clear set of principles and objectives for each CDR purpose not only makes it difficult to define the important attributes of the CDR regime, but also makes it difficult to measure the success (or otherwise) of the regime in delivering to that purpose. Taking the purpose of enabling consumers to more effectively use data relating to themselves for their own purposes as an example, it is important to define the ways CDR consumers may use the data to derive benefit. Is the intention to allow consumers to 'download' data (e.g., energy consumption data, banking data) so that they can modify behaviours (household energy use, impulse spending behaviour, etc)? Or, is the intention to allow customers to derive benefit (i.e., use the data) by obtaining a competitive quote on a service? Once the purpose(s) of the CDR regime are clearly understood, objectives can be established that when measured, will show the success with which the CDR regime has met each purpose. For example, if the purpose is to allow consumers to 'download' data such as bank transaction data into a software package such as MYOB™, then objectives would include ease of exporting data, commonly accepted formats, etc.

We recommend the processes outlined in the draft Bill for designating a sector and creating the CDR rules include steps that require the purpose(s) to be clearly articulated, and that principles and objectives for each purpose be identified.

7.2. Review of the first sector before designating new sectors

Finally, we recommend that 12 months after the first sector is designated, a review of the CDR be completed. This would help identify aspects of the regime that have worked well, and areas for improvement, which could be factored into the designation of subsequent sectors to avoid repeating any mistakes made in the inaugural sector.