Mr Daniel McAuliffe
Structural Reform Group
The Treasury
Langton Crescent
PARKES ACT 2600

Dear Mr McAuliffe

Response to Consultation on Consumer Data Right

On behalf of SISS Data Services we thank Treasury for the opportunity to respond to the request for submissions into the proposed Consumer Data Right Bill.

About SISS Data Services (SISS)

SISS is an Australian enterprise that provides data management services for the professional and financial services industries and has provided 'Open Banking' related data transfer and compliance services to over 80% of Australian banks since 2010. Through direct contractual arrangements with banks, building societies, credit unions, fund managers, stock brokers and others we provide authorised access to third parties – such as FinTech enterprises - to consumer data through our proprietary Application Programming Interfaces (APIs).

Our API's interface directly with both financial institutions and third parties to seamlessly provide access to data in standardised formats using robust security processes that are currently being certified against ISO 27001.

We have more then eight years experience in providing these services. Our enterprise is an example of the innovation that the CDR is intended to facilitate. It enables us to provide Treasury with a unique perspective on potential or unintended problems that the CDR Bill might create.

Executive Summary

Key Issues

- We are concerned that the proposed CDR framework with multiple rule making and accreditation processes will result in costly, disproportionate and complex compliance burdens that will inhibit new market entrants from participating in the CDR.

- The accreditation processes established under cl 56AG of the Bill do not provide sufficient clarity and are likely to mean that accreditation is not undertaken in an efficient and timely manner.

Our Recommendations

- Remove sectorial limitations on CDR, particularly for Finance as we should not be reflecting the UK Open Banking model with includes security for payments. We recommend introducing a "lighter touch" compliance approach that can be operationalised quickly, efficiently and economically
- Revise participation approaches by replacing the technical rules-based system with principles and guidelines that are in place from the outset in a 'one size fits all' approach.
- Reduce to scope of information covered by the CDR to exclude derived and associated information

Comments

One of the main difficulties we have had in attempting to assess the potential impact of the CDR legislation on objectives such as encouraging competition in the financial services and other markets and in supporting innovation is that much of its detail – and thus its regulatory impact – is left to decision-making by organisations such as the ACCC and new bodies such as the Data Recipient Accreditor (DRA) and the Data Standards Body (DSB).

The CDR Bill's approach is overly complex and technical. For example, it would be impractical, expensive and disproportionate to require FinTech's to complete ISO 27001 or equivalent certification in order to become data recipients. SISS estimates that for the CDR to produce its intended innovation and competition dividends entry level compliance costs should be around $2000 per entity.

An ISO 27001 approach disregards varying levels of security risk and assumes that it is an appropriate approach to security across a variety of sectors and across a variety of security risk postures. The consequence of mandating a requirement such as ISO27001 is that this will favour information incumbents. This means that regulatory rules will be shaped to reflect their risk profile, which will not be the risk posture of new market entrants.

We do not believe that an ISO 27001 requirement around security is necessary or desirable. Certainly, this requirement will be out of the reach of most start-up enterprises. In addition,

The CDR's intent to encouraging innovation will be offset by leaving decision-making by organisations such as the ACCC and new bodies such as the Data Recipient Accreditor (DRA) and the Data Standards Body (DSB). We question whether these

new bodies will have the knowledge, budgets, experience or appetite to provide such vast and specific range of accreditations services, which are the core business of operators such as SISS, in a timely manner. Moreover these entities appear to have an unrestricted scope to develop legally binding rules that will largely determine how the CDR is operationalised.

On our reading of the CDR Bill, they are free to establish and impose rules that do not adequately balance each of the CDR's policy objectives. For example, the DRA might choose to require all data recipients to be certified to comply with the security requirements of ISO 27001 before they can receive consumer data. Under this scenario the DRA might decide that a consumer must be accredited to that standard before she or he could receive her or his own data under the CDR scheme. This would be an absurd outcome but seems to be an open possibility under the CDR Bill.

Based on our experience we recommend the accreditation criteria for a 'light touch' compliance regime would seek to cover the following 5 key areas:

a. Know Your Client (Disclosure)
b. Data Breach Process (Data Breach Notification & Management)
c. Risk Management (Proactive Risk Management of data security risks)
d. Environment Management (Regular Internal & External Vulnerability Scans)
e. Insurance (Cyber Insurance – relevant to the business model)

We believe that this could be achieved through a not for profit body (possibly auspiced by the ACCC) being established to undertake accreditation based on principles set out in the legislation.

Equally, the CDR legislation does not contain control, transparency or oversight mechanisms that hold rule-making bodies to account or that ensure that decisions are made in a timely manner.

We are concerned that the CDR adopts a piecemeal, sector-by-sector approach. This is a consequence of the highly complex nature of the regulatory scheme which seems to have been modelled on the UK's Open Banking initiative. This is the wrong model on which to base the CDR because it is designed to support payment and remittance systems. This functionality extends beyond the CDR which is designed to facilitate information sharing, not payments.

That said, we do not support a CDR system that is modelled exclusively on the data portability provisions of the EU *General Data Protection Regulation* (GDPR). The GDPR light touch approach does not leave scope for appropriate and necessary consumer protection safeguards such as necessary security safeguards for personal data in transit between a data controller or processor and individuals.

Our preferred approach is for the sectoral limitations on the CDR to be removed so that it applies to all of the private sector from the outset. Instead of leaving rule

making about accreditation and standards to separate bodies like the ACCC, DSA and DSB, a principles-based regime should be embodied in the legislation that provides adequate guidance to all of the CDR participants about their obligations and participation requirements so that they can be in a position to be part of the CDR system from the outset. These principles can be augmented by guidelines and recommendations made by (say) the ACCC and/or the OAIC supplemented by the activities of the not-for-profit entity referred to earlier in this submission.

We do not support the extended definition of CDR data in sub-clauses 56AF(2) and (3) of the CDR Bill. These extend the definition of data covered by the CDR to directly or indirectly derived CDR data and data that is associated with CDR data. These categories of data will cover value-added data, such as insights and recommendations that are produced by data holders and other participants in the CDR system that are a product of their own activities and which embody their own intellectual property.

We consider that the multiple tiers of privacy protection that would apply to the CDR such as the consumer data rules, the privacy safeguards and the APPs are unnecessary. Again, these multiple and potentially overlapping requirements are likely to produce regulatory complexity and uncertainty, particularly as some can apply differentially sectors, classes of data, classes of persons within designated sectors and different classes of persons to whom CDR data may be disclosed. A single set of rules –preferably the APPs in conjunction with the proposed broader definition of personal information that extends to information that 'relates' to an individual would be preferable.

It is important that Treasury be mindful that this regime will apply to many different participants, some of whom may have access the skills and resources to work with the level of complexity of the CDR Bill but many, particularly those who are new market entrants will not. For all participants there is significant benefit in simplifying and streamlining the regulatory framework via ready-formed intermediaries.

Finally, we recommend that the practice of screen scrapping be prohibited to provide an even playing field, for Open Banking (everyone accessing data the same way), which is also conducive to reducing cyber risks for consumers.

We would be happy to provide any further information or clarification if required.

Yours sincerely
SISS Data Services Pty Limited

Grant Augustin
Managing Director