AGL Energy Limited
T 02 9921 2999
F 02 9921 2552
agl.com.au
ABN: 74 115 061 375

Level 24, 200 George St
Sydney NSW 2000
Locked Bag 3013
Australia Square NSW 1215

31 December 2019

**Select Committee on Financial Technology and Regulatory Technology**

AGL Energy (**AGL**) welcomes the opportunity to provide comment to the Select Committee on the Financial Technology (**FinTech**) and Regulatory Technology (**RegTech**) Issues Paper (Issues Paper).

AGL is one of Australia's leading integrated energy companies and the largest ASX listed owner, operator and developer of renewable generation. AGL is a significant retailer of energy and provides energy solutions to over 3.5 million customers in New South Wales, Victoria, Queensland, Western Australia and South Australia.

AGL has actively participated in the Consumer Data Right (**CDR**) consultation processes run by Treasury, the Australian Competition and Consumer Commission (**ACCC**) and CSIRO's Data61 group over the last 18 months, providing insights into the energy sector and our customers. A key and guiding principle that has informed AGL's active engagement in the CDR consultation processes has been ensuring the customer is at the centre of this consumer rights framework.

Service digitisation is redesigning market structures across industry sectors. Established mature markets are being disrupted by the enthusiastic take-up of innovative services by digitally enabled proactive consumers. Achieving the best outcomes for consumers in this environment requires customer-centred, principle-based regulation that allows industry the flexibility to find the most efficient solution to achieve the desired outcome for consumers. AGL is embracing digital solutions in service delivery by enhancing our digital solutions for customers. We see the CDR as just one part of a way that businesses in Australia can harness service digitisation to improve customer experiences.[1]

The primary objective of the CDR is consumer access and use of data about themselves in a way that fosters informed decisions regarding products and services. We support this premise as a way of empowering customers and allowing them to direct data to accredit third parties in a way that prioritises consumer privacy and expectations.

While the issues paper is focused on opportunities and barriers for FinTech and RegTech generally, we would caution the Committee against any changes to the CDR for this purpose without proper evaluation on how it will impact the operation of the CDR from a consumer perspective. This will allow decision-makers to identify any unintended consequences that may impact or inhibit consumer engagement and trust in the framework.

AGL has provided our views on how to balance FinTech compliance with the CDR while also maintaining consumer engagement and confidence in accessing and using the CDR below.

[1] For more information on our digital solutions visit the AGL Investor page (p.57-61).

**Purpose of the CDR**

The primary purpose of the CDR is to give consumers the ability to access and use more information about themselves, and about their use of goods and services, in a way that allows informed decision making about both the good and services they use.[2]

This primary purpose is reflected strongly through the Explanatory Memorandum for the CDR legislation, including emphasising consumer control:

- The CDR provides individuals and businesses with a right to efficiently and conveniently access information held by businesses about the transactions they enter into as consumers and to authorise secure access to this data by trusted and accredited third parties.
- CDR is designed to give consumers more control over their information leading, for example, to more choice in where they take their business, or more convenience in managing their money and services.
- Strong privacy and information security provisions are a fundamental element of the CDR. These protections include privacy safeguards.[3]

AGL supports this customer centric purpose. A well-constructed framework that consumers trust should encourage industry innovation, which is one of the pillars of the CDR framework. We therefore consider that it is important to keep this purpose at the forefront of decisions impacting the way CDR is to operate.

**Importance of CDR structure**

Throughout the CDR process there has been a strong emphasis by both government and many stakeholders on the importance of getting the consumer protections framework of the CDR right.

The CDR framework is therefore developed, in line with the above primary purpose, to ensure security and access to consumer CDR data is appropriately protected. Treasury determined that a new privacy regime (known as the Privacy Safeguards), rules on accreditation and consent, and the consumer data standards, were all integral to a functioning and effective CDR regime. These principles were balanced by decision-makers with business needs/efficiencies, interoperability of the CDR framework across different sectors and costs.

The importance was summed up well by Mr Andrew Stevens, of the Data Standards Body who stated that, *the consumer data right is about making a data transfer safer and fully consent based... The consent regime would be stronger, and the protections would be greater, than consumers enjoy today.*[4] This importance has been highlighted by AGL, for example in our appearance at the Senate, Economics Legislation Committee, AGL's representative stated that '*It's extremely important to get the framework right because, firstly, consumers and their data absolutely need appropriate protections—that is the fundamental belief of AGL—and the CDR regime will only work properly if the public has confidence in the framework'*.[5]

---

[2] Treasury Law Amendment (Consumer Data Right) Bill 2019, Explanatory Memorandum Chapter 1
[3] Ibid.
[4] The Senate, Economics Legislation Committee, Treasury Laws Amendment (Consumer Data Right) Bill 2019 [Provisions], March 2019 - Mr Andrew Stevens, Interim Chair, Data Standards Body, Committee Hansard, 6 March 2019, p. 38.
[5] The Senate, Economics Legislation Committee, Treasury Laws Amendment (Consumer Data Right) Bill 2019 [Provisions], March 2019, p.49.

**Consumer expectations**

It is important that consumer expectations are met under the CDR. It is therefore important to understand what consumer expectations are when it comes to the CDR and how it operates in terms of services, products and data control. The right regulatory framework considers both the costs and benefits to industry and the community to find the right balance. Consumer protections are an integral pillar to regulatory frameworks, but it is an obligation of decision-makers to balance these against the benefits of competition, innovation and market flexibility.

To understand what consumer expectations were, Data61 commenced work in 2018 through their Consumer Experience (**CX**) workstream. The CX workstream aims to help organisations to provide consumers exercising their rights under the CDR with a trusted and usable consent experience[6], by understanding consumer expectations. This work was done to facilitate Treasury and government support of the broad CDR framework it had developed.

Throughout this work, it was found that **trust and safety** were priorities to consumers. Data61 participants needed to be able to trust the process and all entities involved. One participant stating, *"I would rather that this is developed from a consumer point of view, than the purchaser point of view."*[7]

We note that FinTech Australia are aligned to the needs of the customer and thus privacy and security are core operating principles and that the privacy and security measures for CDR are broadly supported.[8]

Consumers also valued repetition and emphasis on ability to revoke consent. Most participants felt reassured by the knowledge that they could easily revoke their consent whenever they wanted.[9] Knowing that there were multiple options to revoke consent, including a way to revoke consent through the data recipient's app, was important to users.

Consumers expect that their data will be stored and handled appropriately, with security and privacy at the forefront of businesses minds. To achieve this outcome, effective Rules and standards need to be in place to achieve consistency and transparency for consumers.

**CDR compliance costs**

The Issues Paper highlights a key concern of FinTech organisations about the CDR is the compliance costs. They estimate that compliance cost will be around $50,000 - $100,000 per year. The more businesses that participate in the CDR, the more successful we believe it will be – as consumer trust and knowledge of their rights grow. However, it is not a compulsory requirement to participate in the CDR regime unless the business is designated as a data holder – it is an opt-in for those who seek to become accredited data recipients.

[6] Data61 Consumer Data Standards Phase 2 Consumer Experience Report; Consent flow, p.2.
[7] Ibid.
[8] The Senate, Economics Legislation Committee, Treasury Laws Amendment (Consumer Data Right) Bill 2019 [Provisions], March 2019 - FinTech Australia, Submission 17, p. 6.
[9] Data61 Consumer Data Standards Phase 2 Consumer Experience Report; Consent flow, p.8.

We encourage the government to consider the compliance figures in the context of the strong privacy and security needs under the CDR (as a right for consumers and the management of their data), as well as comparatively against the broader costs of participants.

Treasury estimated that the CDR framework will increase compliance costs in the banking sector and for accredited parties by an average of $86.6 million per year, and in the energy sector by an average of $9.9 million per year[10], on an annualised basis (with common accreditation costs not duplicated in the latter figure).[11] Treasury ultimately concluded that the benefits of the CDR as proposed would still exceed these costs.[12]

It is our understanding that to estimate the financial costs in the banking sector, Treasury relied heavily on confidential submissions provided by Australian banks. We understand that the submissions showed a wide variance in cost estimates due to the differing starting points between entities. As the banks considered their regulatory costs as highly commercially sensitive (noting that they may reveal information regarding their internal systems), Treasury did not release this information publicly.

Treasury did not calculate a bottom up estimate as they did not receive detailed breakdowns of cost calculations. In calculating the compliance estimate, Treasury also incorporated actual United Kingdom (**UK**) implementation costs for Open Banking which were between GB150m to 200m for all nine banks not including ongoing costs.

The impact of compliance costs was also considered by the Productivity Commission report on Data Availability and Use in 2017. The report concluded that compliance costs could be greater for small data-holder businesses to large businesses, in part, because larger businesses would tend to have greater opportunities to harness economies of scale, however the overall benefit of consumer access to data was determined to be paramount.[13]

We also note that in a submission to the Productivity Report, Fintech Australia rejected the notion that the costs of APIs would be prohibitive, noting that banks in other markets are undertaking 'open API' projects without being compelled by government.[14]

As the CDR rolls out into other sectors of the economy, accredited data recipients, including FinTechs, will be able to harness the benefits of economies of scale through diverse data access.

[10] AGL have previously submitted that the energy assessment required more rigorous assessment due to the lack of information regarding the energy framework, see our previous submission to the Senate Committee, or our submission to the Australian Competition and Consumer Commission Banking CDR Rules (p.20).
[11] Treasury Law Amendment (Consumer Data Right) Bill 2019, Explanatory Memorandum,p.3.
[12] Ibid.
[13] Productivity Commission Inquiry Report – Data Availability and Use, March 2017, p.218.
[14] Productivity Commission Inquiry Report – Data Availability and Use, March 2017