Ms Deborah Anton
Interim National Data Commissioner
Office of the National Data Commissioner
1 National Circuit, Barton ACT 2600

Verifier Pty Ltd

Submission to The Office of the National Data Commissioner Exposure Draft Data Availability and Transparency Bill 2020

About Verifier

Verifier is a consumer-driven, consent-based data sharing platform built on Privacy-by-Design principles. Our goal is to put the consumer in the driver's seat with respect to their data – to enable them to access that data and to use it to get better outcomes. We respect the information security needs of consumers, our data sources and our clients. Our clients include banks and non-bank financial institutions.

Verifier is a RegTech pioneer and thought leader in data-portability, and we are currently in the final stages of becoming an Accredited Data Recipient in the Consumer Data Right regime.

About the Authors

Lisa Schutz is Verifier's founder and CEO. Verifier is a founding member of The RegTech Association. Lisa is a founding director of that organisation, formed in 2017, with the goal of establishing a centre of excellence in Australia for RegTech, for the benefit of the community and commerce.

Lisa is also a member of both the Data Standards Body Advisory Committee for Banking and the Data Standards Body Advisory Committee for Energy - under the Consumer Data Right regime.

Debra Kruse is Verifier's Head of Legal and Commercial. Debra is an experienced lawyer whose expertise includes privacy law and the Consumer Data Right regime.

Lisa and Debra have spent significant time and effort in the consultation process leading to the Consumer Data Right regime and its application to Open Banking.

Purpose of Verifier's submission

Verifier welcomes the opportunity to make this submission in respect of the Exposure Draft Data Availability and Transparency Bill 2020 (the **Exposure Draft Bill)** and the Accreditation Framework Discussion Paper (the **Accreditation Discussion Paper**).

The purpose of our submission (and therefore the focus of our submission) is to advocate for the implementation of regulation that promotes consent-driven data portability, is efficient and fair, and which embodies competitive neutrality.

Verifier's comments on the Exposure Draft Bill:

Control of the data sharing

The Exposure Draft Bill does not compel Commonwealth Data custodians to share data they hold. Instead, each Data custodian is responsible for assessing each request for data to be shared, and if the Data custodian determines that:

(a) the sharing is for one of the three permitted purposes, and

(b) the risks of sharing can be managed,

then the Data custodian may share data, notwithstanding applicable Commonwealth, State or Territory non-disclosure laws[1].

In this construct, the Data custodian has control over the data sharing. Contrast this with both:

(a) the Consumer Data Right, which gives the consumer (the subject of the data) the right to authorise sharing their data for any purpose, and

(b) Australian Privacy Principle 12, which gives individuals the right to access their data – and share it with others as they see fit.

Verifier's recommendation

We commend the government's move towards making data about individuals and business entities (each a **data subject**) that is held by its agencies available to be used for purposes designed to achieve outcomes which are in the public interest.

However, in our view, the 'permitted purposes' for data sharing should include a mechanism that permits Data custodians to share data at the request of the data subject) for a non-government purpose which might result in a better commercial outcome for the data subject.

A mechanism that should be considered to enable the data subject to access their data for a commercial purpose might be similar to the Ministerial 'designation' of sectors and data types employed in the Consumer Data Right regime.

Introducing an appropriate mechanism would:

(a) empower the data subject to use their data to get better outcomes,

(b) advance the consent driven, digital first principles of data portability, and

(c) enable government, the National Data Commissioner, and Data custodians to ensure the safety and security of data sharing.

[1] Section 13(1) and section 15.

Verifier's responses to Accreditation Discussion Paper questions:

Q3: Are there circumstances when it should be mandatory to use an Accredited Data Service Provider for a data sharing project?

Yes. Given the sharing of public data has traditionally been limited, Data custodians are unlikely to have the experience or internal expertise or resources required to enable efficient data integration or data sharing.

Q4: What would those circumstances be?

Every data sharing project assessment should include the assessment of the Data custodian's data integration or data sharing capabilities.

Each assessment should also include consideration of accredited data service providers' capabilities – including those who may not currently be on government service provider panels – but who are experienced and proven RegTech organisations whose core business is data integration and data sharing.

In short, where an accredited data service provider's data integration and data sharing capability is greater than the capability of the relevant Data custodian, use of the accredited data service provider should be mandatory.

Q7: Should the accreditation process recognise other frameworks, standards or processes that have assessed an element of data capability? If so what standards/processes might be appropriate to recognise?

Yes. To the greatest extent possible, the accreditation process should be harmonised with the accreditation process and standards adopted by the Consumer Data Right regime – to avoid inconsistency and unnecessary regulatory complexity.

Q10: Are there further ways we can streamline the accreditation process?

Yes. Entities that are accredited under the Consumer Data Right regime should be streamlined to accreditation.

Q11: Do the timeframes to renew accreditation, every 5 years for Accredited Data Service Providers and every 3 years for Accredited Users, seem reasonable?

No. It is not clear why those renewal periods should differ. This will introduce unnecessary complexity for those entities who are accredited as both Users and Data Service Providers.

Finally, we would be happy to discuss any aspect of our submission with you or your staff. Please contact Debra Kruse in the first instance by email at debra.kruse@verifier.me.

Sincerely
Lisa Schutz and Debra Kruse
Verifier