

Submission on discussion document: Unlocking value from our customer data

Your name and organisation

Name	Irene Peter
Organisation (if applicable)	Sharesies Limited
Contact details	Privacy of natural persons and legal@sharesies.co.nz

[Double click on check boxes, then select 'checked' if you wish to select any of the following.]

The Privacy Act 2020 applies to submissions. Please check the box if you do not wish your name or other personal information to be included in any information about submissions that MBIE may publish.

MBIE intends to upload submissions received to MBIE's website at www.mbie.govt.nz. If you do not want your submission to be placed on our website, please check the box and type an explanation below.

I do not want my submission placed on MBIE's website because... [Insert text]

Please check if your submission contains confidential information:

I would like my submission (or identified parts of my submission) to be kept confidential, and **have stated below** my reasons and grounds under the Official Information Act that I believe apply, for consideration by MBIE.

I would like my submission (or identified parts of my submission) to be kept confidential because... [Insert text]

Responses to discussion document questions

How will the draft law interact with protections under the Privacy Act?

1 *Does the proposed approach for the interaction between the draft law and the Privacy Act achieve our objective of relying on Privacy Act protections where possible? Have we disapplied the right parts of the Privacy Act?*

We support the interaction with the Privacy Act and how this Bill proposes to lean on the established body of law for protection of personal data.

Consent settings: respecting and protecting customers' authority over their data

2 *Should there be a maximum duration for customer consent? What conditions should apply?*

We believe consumers don't expect to have to continually reconfirm their consent and will be disadvantaged when they lose access to services while re-consent is sought.

We believe it is sensible that legislation requires a clear, accessible and simple process for withdrawal of consent.

3 *What settings for managing ongoing consent best align with data governance tikanga?*

4 *Do you agree with the proposed conditions for authorisation ending? If not, what would you change and why?*

5 *How well do the proposed requirements in the draft law and regulations align with data governance tikanga relating to control, consent and accountability?*

6 *What are your views on the proposed obligations on data holders and accredited requestors in relation to consent, control, and accountability? Should any of them be changed? Is there anything missing?*

In order for the identified benefits of the CDR to be realised, legislation must seek to ensure a low friction and easy to understand consent process. International experience shows that where data holders are not held to account for ensuring a good consent experience, the benefits of the CDR are not as readily realised.

Consumers will be deterred from participation in the CDR if the consent process provided by data holders is difficult to access or difficult to complete. We should consider clear and simple standardised wording for consent in the standards. This would ensure that the consent process is deliberately succinct and clear, and that data holders do not feel the need to protect themselves (or take the opportunity to protect their place in the status quo) with complex consent processes that undermine consumer confidence and deter consumer participation. In the UK specific customer journey and experience guidelines were developed following the launch of open banking "so that the customer journey can be low friction, speedy and simple."

We strongly support safeguards for giving consent that do not create an inconvenient or burdensome customer experience so that the intended benefits of the CDR are truly realised.

Care during exchange: standards

7

Do you think the procedural requirements for making standards are appropriate? What else should be considered?

8

Do you think the draft law is clear enough about how its storage and security requirements interact with the Privacy Act?

9

From the perspective of other data holding sectors: which elements of the Payments NZ API Centre Standards¹ are suitable for use in other sectors, and which could require significant modification?

10

What risks or issues should the government be aware of, when starting with banking for standard setting? For example, could the high security standards of banking API's create barriers to entry?

Trust: accreditation of requestors

11

Should there be a class of accreditation for intermediaries? If so, what conditions should apply?

12

Should accredited requestors have to hold insurance? If so, what kind of insurance should an accredited requestor have to hold?

The case for specifying insurance cover under the legislation is not clear. There is no minimum insurance requirement for parties holding or processing personal data under the Privacy Act and it's not clear that the CDR risk profile is different.

When would the insurance respond? For example, if an accredited requestor suffered a data breach under which data subjects suffered harm:

- the data holder(s) who provided data to the accredited requestor should not be liable under the Law (it was not their breach), the data holder will not have suffered loss and should not have any need to claim against the accredited requestor
- the data subject(s) may have suffered loss and could claim against the accredited requestor directly, that data subject has agreed to the accredited requestor

¹ New Zealand API standards to initiate payments and access bank account information. They are based on the UK's Open Banking Implementation Entity standards but tailored for the New Zealand market. Market demand has driven development and led to the creation of bespoke functionality for New Zealand.

accessing and using its data and so this would appear to be no different to a consumer relationship in relation to data already covered by the Privacy Act.

13 *What accreditation criteria are most important to support the participation of Māori in the regime?*

14 *Do you have any other feedback on accreditation or other requirements on accredited requestors?*

Unlocking value for all

Please provide feedback on:

- 15
- *the potential relationships between the Bill safeguards and tikanga, and Te Tiriti/the Treaty*
 - *the types of use-cases for customer data or action initiation which are of particular interest to iwi/Māori*
 - *any specific aspirations for use and handling of customer and product data within iwi/hapū/Māori organisations, Te Whata etc, which could benefit from the draft law.*

16 *What are specific use cases which should be designed for, or encouraged for, business (including small businesses)?*

17 *What settings in the draft law or regulations should be included to support accessibility and inclusion?*

18 *In what ways could regulated entities and other data-driven product and service providers be supported to be accessible and inclusive?*

Ethical use of data and action initiation

19 *What are your views on the proposed options for ethical requirements for accreditation? Do you agree about requirements to get express consent for de-identification of designated customer data?*

20 *Are there other ways that ethical use of data and action initiation could be guided or required?*

It's not clear that there is public interest in adding additional express consent for de-identification. Notably this extends beyond the rights attributed to personal information

under the Privacy Act. We know from experience that the addition of a further tick box can have a more than minor deterrent effect (and often an outsized impact) on customer engagement and process completion. Further express consent requirements should not be added without clear consumer interest.

Preliminary provisions

21 *What is your feedback on the purpose statement?*

22 *Do you agree with the territorial application? If not, what would you change and why?*

Regulated data services

23 *Do you think it is appropriate that the draft law does not allow a data holder to decline a valid request?*

Accommodation should be made for compliance with other laws - for example the FMA under s44 of the Financial Markets Authority Act 2011 can make broad confidentiality orders. In a future state, if Sharesies were required to send transaction history under a CDR designation and could not decline a request, then it could end up in breach of a confidential order in relation to the same information. There will be other examples of similar conflicts. In instances of conflict, relief should be provided from one of the obligations.

24 *How do automated data services currently address considerations for refusing access to data, such as on grounds in sections 49 and 57(b) of the Privacy Act?*

Protections

25 *Are the proposed record keeping requirements in the draft law well targeted to enabling monitoring and enforcement? Are there more efficient or effective record keeping requirements to this end?*

26 *What are your views on the potential data policy requirements? Is there anything you would add or remove?*

Regulatory and enforcement matters

27 *Are there any additional information gathering powers that MBIE will require to investigate and prosecute a breach?*

Administrative matters

28	<i>Are the matters listed in clause 60 of the draft law the right balance of matters for the Minister to consider before recommending designation?</i>
29	<i>What is your feedback on the proposed approach to meeting Te Tiriti o Waitangi/Treaty of Waitangi obligations in relation to decision-making by Ministers and officials?</i>
30	<i>What should the closed register for data holders and accredited requestors contain to be of most use to participants?</i>
31	<i>Which additional information in the closed register should be machine-readable?</i>
32	<i>Is a yearly reporting date of 31 October for the period ending 30 June suitable? What alternative annual reporting period could be more practical?</i>
33	<i>Should there be a requirement for data holders to provide real-time reporting on the performance of their CDR APIs? Why or why not?</i>
	Yes. We support positive pressure to ensure a well functioning and well maintained API.
34	<i>What is your feedback on the proposal to cap customer redress which could be made available under the regulations, in case of breach?</i>
Complaints and disputes	
35	<i>In cases where a data holder or requestor is not already required to be member of a dispute resolution scheme, do you agree that disputes between customers and data holders and/or accredited requestors should be dealt with through existing industry dispute resolution schemes, with the Disputes Tribunal as a backstop? Why or why not?</i>

Other comments

We are supportive of the Bill and support the focus on unlocking data for the benefit of people and their organisations. We are hopeful that the legislation will encourage investment in more secure and efficient alternatives to the existing data sharing methods used by some in the New Zealand financial services landscape.

We believe that subordinate legislation will likely need to address the scope of data holders to charge for these services, if the CDR is to meet its full potential innovators cannot be priced out of access.

There is significant demand for data held by government agencies. It would be good if government sectors had the opportunity to lead by example. For example passport and driver licence data are requested in most AML Customer Due Diligence processes. The DIA and NZTA could be early target sectors for designation.

We look forward to opportunities to innovate (and to partner with others) as we continue to democratise access to wealth development opportunities in New Zealand. New Zealand is well behind the rest of the world in our data and digital financial services capability, we must catch up and at pace, this legislation is an essential step to unlocking that potential.