Submission on discussion document: *Unlocking value from our customer data*

Your name and organisation

Name	Privacy of natural persons
Organisation (if applicable)	Privacy of natural persons
Contact details	Privacy of natural persons

[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 unless it is published anonymously.

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?*
	Yes the approach is sensible and means there are not two separate privacy regimes in place and avoids a fragmented approach to privacy in New Zealand.
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 that the customer should have the right to choose to give consent for the duration of the relationship (plus any regulatory periods post the end of the relationship). Customers are able to set time limits if they wish with the understanding that in doing so they will be required to re-consent if they wish to continue to rely on the service that utilises their data.
3	*What settings for managing ongoing consent best align with data governance tikanga?*
	As above, giving customers the right to choose the length of their ongoing consent aligns with governance tikanga. For some people the user experience and ease of giving consent will be more important, therefore we should avoid putting limitations for customers who wish to provide enduring consent for the lifecycle of the relationship with the accredited requestor.
4	*Do you agree with the proposed conditions for authorisation ending? If not, what would you change and why?*
	Yes the proposed conditions for authorisation ending make sense, however we are recommending that the maximum period be the length of the relationship between the customer and the accredited requestor.
5	*How well do the proposed requirements in the draft law and regulations align with data governance tikanga relating to control, consent and accountability?*
	The proposed requirements emphasis that the control of who receives and uses the data and product information sits with the customer as well as requirements for the accredited requestor to make it easy for the customer to remove or end their consent. This therefore aligns well with data governance tikanga and having sovereignty over your own data.
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?*
	The proposed obligations align with the customer being informed and having control over the consent process. We believe there should be a level of reasonable timeframes included, especially where there is an obligation to provide a non-automated digital solution as this requires companies to have teams set up to be able to respond to manual requests and this takes time and costs more.

Care during exchange: standards	
7	*Do you think the procedural requirements for making standards are appropriate? What else should be considered?*
	While not strictly related to the requirements around making the standards it is more of an observation that any standards will need to allow sufficient time for implementation.
8	*Do you think the draft law is clear enough about how its storage and security requirements interact with the Privacy Act?*
	The draft law clearly articulates the response to breaches as it relates to personal information but does not cover the event of a failure in storage of business information. This could impact the use/uptake from businesses who wish to enable data to be shared through this process as they do not have clear protections. We recognise however the balance required with not wishing to put a separate regime in place for managing breaches of personal information. It could well be that the complaints resolution process would be sufficient.
9	*From the perspective of other data holding sectors: which elements of the Payments NZ API Centre Standards[1] are suitable for use in other sectors, and which could require significant modification?*
	We have no feedback on this question.
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?*
	Setting the security standards to the level required for banking you effectively counteracts the purpose to promote innovation. Companies that are innovating are often start-up businesses that do not have the resources to maintain bank level security, nor should they need to for certain types of data (see question 11 below for a possible solution that would balance the need for security with enabling innovation). Other risks that need to be clearly understood relate to secure verification of users of the regime whether they be data holders, customers or accredited requestors, parties will need a safe and secure way of validating that they are dealing with the authorised party.
Trust: accreditation of requestors	
11	*Should there be a class of accreditation for intermediaries? If so, what conditions should apply?*
	Yes we believe that a sensible approach would be two pronged. First classify the data according to level of risk/sensitivity. Second risk rate the security level of the accredited requestor and authorise data access according to that risk level. Those accredited requestors who want to access the highest risk or most sensitive data will need to demonstrate the highest level of security (as required by the standards).

[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.

12	*Should accredited requestors have to hold insurance? If so, what kind of insurance should an accredited requestor have to hold?*
	No. Mandating insurance often means the price of that insurance premiums becomes higher and this can be cost prohibitive for new participants (and existing participants) in the market.
13	*What accreditation criteria are most important to support the participation of Māori in the regime?*
	We are not qualified to answer this question.
14	*Do you have any other feedback on accreditation or other requirements on accredited requestors?*
	For consideration, from experience conducting fit and proper person vetting on overseas directors and senior managers is difficult and much harder to do than for onshore directors as access to relevant agencies and databases can be challenging. Therefore this requirement disadvantages companies with offshore directors and senior managers and adds additional costs.
Unlocking value for all	
15	*Please provide feedback on:* • *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.*
	We have no feedback on this
16	*What are specific use cases which should be designed for, or encouraged for, business (including small businesses)?*
	We have no feedback on this
17	*What settings in the draft law or regulations should be included to support accessibility and inclusion?*
	We have no feedback on this
18	*In what ways could regulated entities and other data-driven product and service providers be supported to be accessible and inclusive?*
	We have no feedback on this
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?*
	We have no feedback on this
20	*Are there other ways that ethical use of data and action initiation could be guided or required?*
	We have no feedback on this
Preliminary provisions	
21	*What is your feedback on the purpose statement?*
	Suggest removing the term "long-term" and simply say "promote competition and innovation for the benefit of customers."
22	*Do you agree with the territorial application? If not, what would you change and why?*
	We have no feedback on this
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?*
	Yes, it is entirely appropriate. If data holders had the option to decline a valid request there is potential for mis-use and abuse of the system. Data holders would be able to prevent competitors from getting access to data by declining requests. If the accreditor requestor has been approved to request the data and the customer wishes to share that data with them and the data holder has the relevant data then no other approval should be necessary.
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?*
	We have no feedback on this
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?*
	We have no feedback on this
26	*What are your views on the potential data policy requirements? Is there anything you would add or remove?*
	The focus should not be on whether a policy exists but whether the right procedures and protocols are in place.
Regulatory and enforcement matters	

27	*Are there any additional information gathering powers that MBIE will require to investigate and prosecute a breach?*
	We have no feedback on this
Administrative matters	
28	*Are the matters listed in clause 60 of the draft law the right balance of matters for the Minister to consider before recommending designation?*
	We have no feedback on this
29	*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?*
	We have no feedback on this
30	*What should the closed register for data holders and accredited requestors contain to be of most use to participants?*
	We have no feedback on this
31	*Which additional information in the closed register should be machine-readable?*
	We have no feedback on this
32	*Is a yearly reporting date of 31 October for the period ending 30 June suitable? What alternative annual reporting period could be more practical?*
	Yes. This reporting period works.
33	*Should there be a requirement for data holders to provide real-time reporting on the performance of their CDR APIs? Why or why not?*
	Ideally this would be self-service real time dashboard reporting so that those that rely on its use can get instant notification if data is unavailable and could impact its own solution/service.
34	*What is your feedback on the proposal to cap customer redress which could be made available under the regulations, in case of breach?*
	We have no feedback on this
Complaints and disputes	
35	*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?*
	Yes. This would provide the public additional comfort that there is an independent body they can contact. Most data holders/accredited requestors will already be members of a disputes resolution scheme. Provided there is not a requirement to sign up to a new scheme set up for the purposes of this legislation then this would not be an issue. If data

holders/accredited requestors were asked to sign up to a new scheme this would mean they would be signed up to multiple schemes which becomes cost prohibitive and inefficient.

Other comments