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

Your name and organisation

Name	Karen McWilliams, Sustainability and Business Reform Leader at Chartered Accountants Australia and New Zealand Keddie Waller, Senior Manager – Public Practice, Financial Planning and Ethics Policy at CPA Australia
Organisation (if applicable)	Chartered Accountants Australia and New Zealand CPA Australia
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 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 proposal to rely on the Privacy Act protections wherever possible when developing the draft law and believe the right parts of the Privacy Act have been considered. This approach should result in reduced costs and compliance obligations on business, which should in turn encourage and support smaller participants to engage in the new regime. Where the implementation of this regime creates gaps in the protection of personal data, we recommend that amendments are made in the Privacy Act to ensure consistency in the approach to regulating personal information. However, given the Privacy Act is only limited to personal information, consideration will need to be given to how non-personal information outside the scope of the Privacy Act, such as business data, will be covered by appropriate protections in the future regulations.
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 note that 'consent' is not provided for in the proposed Bill and make our comments in relation to a customer's authorisation. We support a maximum period for a customer's authorisation, at which time the data holder or accredited requestor can seek confirmation to roll over the authorisation for another maximum period, or action a request to withdraw the authorisation. This process should also include advising a customer of the impact of withdrawing their authorisation. If a customer does not respond to enquiries by a data holder or accredited requestor, then the authorisation must expire. While we do not have a firm view of a maximum period, we would suggest annually is reasonable for individuals and not more than three years for businesses.
3	*What settings for managing ongoing consent best align with data governance tikanga?*
	No comment.
4	*Do you agree with the proposed conditions for authorisation ending? If not, what would you change and why?*
	We support the proposal in the draft Bill that an authorisation will automatically end if a customer closes an account with a data holder or when an accredited requestor's accreditation is suspended or cancelled (section 31). We recommend that amendments are made to this section so that ending an authorisation is not significantly harder than giving an authorisation. However, we are concerned with the proposal to facilitate the withdrawal of authorisation by email or phone by a customer. The intent of the draft Bill is to create an electronic system and requires regulated data services to be provided using an electronic system (section 26)

	and for data holders and accredited requestors to have systems in place to enable the customer to view authorisations (section 34). Allowing authorisation and its withdrawal in a non-digital form exposes the customer to potential risks such as impersonation. It will also increase the resources needed by accredited requestors and data holders to capture non-electronic authorisation in an electronic system for no additional benefit to a customer. We recommend that only the electronic system should be used by customers to give, modify or withdraw their authorisation and as proposed, an accredited requestor or data holder must outline any consequences (if any) of doing so. With the heightened risks of cyber and identity fraud with voice, email and post it is critical to have a centralised record, such as a dashboard, of all activities relating to customer authorisation documented.
5	*How well do the proposed requirements in the draft law and regulations align with data governance tikanga relating to control, consent and accountability?*
	No comment.
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?*
	We consider the proposed obligations on data holders and accredited requestors to be appropriate, provided the electronic system is the only means by which customers can withdraw their authorisation. Please refer to our response to question 4 for further details.
Care during exchange: standards	
7	*Do you think the procedural requirements for making standards are appropriate? What else should be considered?*
	We support the proposed procedural requirements for making standards, including to consult people and groups that will be affected by the issue of the proposed standard. However, we note the absence of a specific reference to data holders and accredited requestors within this list of consultation groups. While it may be implied, we suggest consideration be given to including these groups specifically. Consideration should also be given to the time needed for data holders and accredited requestors to develop the software and implement processes to implement the standards. Based on the experience in Australia, frequent changes to the standards can disproportionally increase the costs for participants in comparison to the actual or perceived benefits to customers. We suggest that new standards or changes to existing standards should be implemented in blocks, and not more than biennially. This approach acknowledges that each change requires the participants to update their systems and processes, which can take significant time and resources.
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 is clear on how the storage and security requirements of personal information interact with the Privacy Act.

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?*
	No comment.
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?*
	When developing the new regime, we believe it is important to consider the following: • Data flow – how data currently flows between customers, intermediaries, data holding businesses, including for example digital service providers. • Customer – ensuring that the customer understands the purpose, benefits, relevant considerations, and their rights within the regime. • Intermediaries – the role of intermediaries and how they support customers. • Equitable access - all data holders should be able to participate in the regime to ensure accessibility for all customers and to prevent large businesses from gaining an unfair advantage. Using banking as an example, if small banks cannot afford to participate, their customers will be disadvantaged and may lead to customers moving to a larger bank. Further, as outlined in our response to question 7, regular changes would also create challenges for those participating and should therefore be avoided.
Trust: accreditation of requestors	
11	*Should there be a class of accreditation for intermediaries? If so, what conditions should apply?*
	We are concerned that the draft law penalises non-accredited requestors as an accredited requestor does not have to action their request. This may create a barrier for the professionals who provide services to customers, such as professional accountants, who need accounting data to service and support their clients. It is not possible at this stage to comment if seeking Class Two accreditation is feasible, as the costs and requirements for this level of accreditation are currently unknown. However, we are concerned that any form of accreditation to ensure requests will be actioned will disrupt existing trusted relationships for example, between a professional accountant and their client. We request clarity of the expected class of people that could be brought into the regime as secondary users, in particular, section 22 (4) which may capture professionals accountants, including members of Chartered Accountants Australia and New Zealand and CPA Australia. Further, we are also concerned that section 36, Identity, of the draft Bill does not talk to these secondary users.

[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?*
	We consider it appropriate for accredited requestors to have adequate insurance for customers to be properly compensated for any loss arising from a breach of their obligations under this regime.
13	*What accreditation criteria are most important to support the participation of Māori in the regime?*
	No comment.
14	*Do you have any other feedback on accreditation or other requirements on accredited requestors?*
	No comment.
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.*
	No comment.
16	*What are specific use cases which should be designed for, or encouraged for, business (including small businesses)?*
	We suggest that it is important to identify other related existing and proposed obligations on business and how they may be leveraged in developing the new regime. For example, as the corporate registry identifier and beneficial ownership reforms plans progress, look for ways to leverage from work being carried out as part of these reforms.
17	*What settings in the draft law or regulations should be included to support accessibility and inclusion?*
	No comment.
18	*In what ways could regulated entities and other data-driven product and service providers be supported to be accessible and inclusive?*
	No comment.
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 consider it is appropriate for ethical requirements to form part of the safeguards for the use of customer data, however such a test should be subjective not objective. We therefore support option 2: requirement to get express authorisation from customers for de-identification of designated customer data. To ensure efficiency and avoid authorisation fatigue, the authorisation should form part of a customer giving or modifying their authorisation to access data. However, the request for this authorisation must be a separate and distinct section from authorisation to access data.
20	*Are there other ways that ethical use of data and action initiation could be guided or required?*
	No *comment.*
Preliminary provisions	
21	*What is your feedback on the purpose statement?*
	In our view, the purpose statement is appropriate for the new regime.
22	*Do you agree with the territorial application? If not, what would you change and why?*
	We agree with the territorial application, as it ensures consistent application and customer protection.
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?*
	In our opinion, the draft Bill does not prevent a data holder from declining a request. As sections 17(1)(c) and 18(1)(d) state, data holders need only action a request if they would ordinarily perform that action. Therefore, where a data holder would not normally provide information to protect a vulnerable customer, they would not need to provide information in response to a request received through this regime. With that view, we consider sections 17 and 18 are appropriate.
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?*
	No comment.
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?*
	No comment.

26	*What are your views on the potential data policy requirements? Is there anything you would add or remove?*
	We consider it appropriate for accredited requestors to have a customer data policy. Commonly, people rarely read policy documents which may lead to customer being overwhelmed when seeking key information. Therefore, we suggest accredited requestors should ensure that key information can be easily found on their portal, in particular, how to lodge a complaint. We recommend considering amendments to section 43 of the draft Bill to incorporate this obligation.
Regulatory and enforcement matters	
27	*Are there any additional information gathering powers that MBIE will require to investigate and prosecute a breach?*
	We have not identified any additional information gathering powers that MBIE may need, however we recognise the importance of appropriately resourcing MBIE to take on these additional responsibilities.
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 consider the matters listed achieve the right balance.
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?*
	No comment.
30	*What should the closed register for data holders and accredited requestors contain to be of most use to participants?*
	No comment.
31	*Which additional information in the closed register should be machine-readable?*
	No comment.
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?*
	We welcome more information on the benefits that will arise from the planned annual reporting and call for MBIE to articulate the purpose of these reports, including the purpose of any proposed metric, as well as what outputs MBIE may produce from data collected in these reports. Importantly, reporting should not be overly burdensome. To support accredited requestors efficiently build their electronic systems to capture the required reporting metrics automatically, the specific requirements of what they will be required to report on must be detailed as soon as practical in the regulations.

	Alongside this, MBIE should ensure its own technology systems enable efficient online reporting lodgement that aligns with the electronic systems accredited requestors will be required to build themselves as part of participating in the regime. MBIE should also recognise that reports lodged via the online reporting platform are likely to be subject to internal review and sign off by an accredited requestor's compliance function. Therefore, MBIE should cater for this process in the build of its online reporting platform. For example, the full report should be visible in a printable format to assist those preparing the reports to plan and review in advance of submission. It should also enable the accredited requestor to retain a copy of any reports lodged for their own record keeping purposes. We refer you to the Ministry of Justice, which changed its reporting platform in response to feedback from reporting bodies under the *Anti-Money Laundering and Countering Financing of Terrorism Act 2009* to leverage their experience.
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?*
	No comment.
34	*What is your feedback on the proposal to cap customer redress which could be made available under the regulations, in case of breach?*
	No comment.
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?*
	We understand the only disputes that can arise for data holders and accredited requestors is where a customer considers they have breached their obligations under the proposed regime. That is, the release and transfer of data. Where this is not already covered by existing complaints processes under the Privacy Act, we suggest the regulator of regime, MBIE, should sit as the complaints body.

Other comments

We believe the proposed customer and product data regime has the potential to deliver tangible benefits to individual and business customers. However, a key consideration in building the new regime will be ensuring that any compliance obligations and associated costs are balanced with real benefits for customers. In our view, it is important to set metrics to measure the success of the regime in advance of implementation.

In Australia, we have seen truncated timeframes for consultation and implementation, coupled with creating new compliance obligations rather than leveraging those in existence. This has resulted in a complex regime with significant costs, acting as a barrier to entry for small data holders and potential accredited data recipients. We believe there is the opportunity to learn from this and other global experiences in the successful development and implementation of the new regime for New Zealand.

It is also important to consider how the design of the broader framework will apply to different sectors, to avoid creating barriers to entry for potential participants. For example, while the banks in New Zealand have been preparing for this for a number of years, other sectors will most likely not

yet be considering these changes. As outlined in the previous responses, it is important that the regime supports smaller businesses to engage, and we suggest that this cohort should be front of mind at all stages of development.

We note that the many elements of the new regime, such as accreditation, will be implemented through regulations and look forward to participating in these consultations and urge that a minimum period of 8 weeks is provided for these consultations.