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

Your name and organisation

Name	Privacy of natural persons
Organisation (if applicable)	Orion New Zealand Limited
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 do not consider the proposed approach of relying on Privacy Act protections where possible is appropriate as this results in an inconsistency under the consumer data right framework between the treatment of customer data which is also personal information under the Privacy Act and other customer data (e.g. data relating to businesses). Currently under the draft Bill, the Privacy Act protections would apply in the case of customer data which is personal information under the Privacy Act. However, the draft Bill covers all customer data, which includes information about non-natural persons (i.e. businesses). The protections in the Privacy Act would not extend to such customer data, leaving an inconsistent approach between the types of customer data, depending on whether or not the data comprises personal information. For example, under the Privacy Act, access to data about individuals can be refused in some cases including if the data holder has reasonable grounds to believe that the request is made under the threat of physical or mental harm. Under the draft Bill, data holders may refuse access to data for individuals, for the reasons set out in the Privacy Act but there are no grounds under which the data holder may refuse access for non-natural persons (even though a director or senior manager of a business could be under threat of physical or mental harm). We consider the relevant protections from the Privacy Act should be set out in the draft Bill (as with the Australian framework) so that the protections extend to both individuals and non-natural persons, to ensure a consistent approach. This would ensure data holders and accredited requestors are only required to adopt one approach to customer data, regardless of the identity of the customer. See also our further comments at items 8, 19 and 23 below.
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 consider there should be a maximum duration for customer consent, with such period being at least 15 months (broadly similar to that in Australia). There is a significant administrative burden imposed on data holders under the framework and we consider any shorter period would be onerous for data holders, accredited requesters and customers and add to this administrative burden. Furthermore, electricity distribution businesses have a 14 month wash-up cycle for reconciling electricity consumption and therefore, it makes sense for the customer consent to cover the reconciliation period.
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?*

	We agree that customer consent should automatically expire on a customer ceasing to be a customer of the relevant data holder and on an accredited requester's accreditation being revoked or suspended.
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?*
	Currently under the draft Bill, before providing data or performing an action, the data holder must check that the customer has authorised the request (including checking that the action requested is within the scope of the authorisation given by the customer) and verify both the customer's and the accredited requestor's identity. We do not consider this an appropriate allocation of risk where an accredited requestor is involved. We consider the data holder should instead be able to rely on evidence provided by the accredited requestor as part of the request to confirm such authorisation and identity, particularly given the accredited requestor must go through a rigorous accreditation process. If the onus does sit with the data holder, it is also not clear how the above checks and verifications would be completed. We consider this should be clarified in the draft Bill. See also our comments below at item 30 in relation to the closed register.
Care during exchange: standards	
7	*Do you think the procedural requirements for making standards are appropriate? What else should be considered?*
	We agree with the requirement in clause 88 of the draft Bill to consult with affected parties and the public before making standards. However, under clause 89, when creating new standards or incorporating existing standards into the framework, we consider the chief executive should also be required to have regard to any existing frameworks, regime, legislation, standards or guidelines already in place in the relevant industry. For example, under the Electricity Industry Participation Code 2010, there are existing protocols regarding the provision of metering information between industry participants under the Code.
8	*Do you think the draft law is clear enough about how its storage and security requirements interact with the Privacy Act?*
	As noted above at item 1, we consider the relevant protections from the Privacy Act (including in relation to storage and security requirements) should be set out in the draft Bill to ensure a consistent approach.

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 consider the Account Information API standard could be suitable for use in other sectors where account information is being requested. However, currently this standard does not envisage an automatic expiry for consent (which will need to be updated if the draft Bill includes such an automatic expiry). In addition, the standard does not cover "write operations" (i.e. action initiation), only read access, which may need to be updated to reflect that the draft Bill also envisages "action initiation". The Payment Initiation API standard may be less relevant given it governs the making of electronic payments. In addition, the standards currently envisage a process for API Providers (i.e. data holders) to be required to confirm the customer's authorisation. As noted at item 6 above, where a request is being made by an accredited requestor, we consider the onus of this should sit with the accredited requestor (with the data holder being able to rely on the information provided by the accredited requestor). To the extent these standards are used in other sectors however, we consider regard should be had to any existing frameworks, regime, legislation, standards or guidelines already in place in the relevant industry.
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?*
	We consider there should not be a separate class of accreditation for intermediaries. Instead, any third party dealing with consumer data or product data should be required to be an accredited requestor.
12	*Should accredited requestors have to hold insurance? If so, what kind of insurance should an accredited requestor have to hold?*
	We agree that accredited requestors should be required to hold insurance. However, we consider the draft Bill should clarify what type of insurance is envisaged (in particular, to ensure the type of insurance envisaged is generally available in the NZ market at a reasonable cost).
13	*What accreditation criteria are most important to support the participation of Māori in the regime?*

[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.

	-
14	*Do you have any other feedback on accreditation or other requirements on accredited requestors?*
	See our comments at item 6 above in relation to the onus for confirming customer authorisation and customer / accredited requestor identity where a request is made by an accredited requestor.
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.*
	-
16	*What are specific use cases which should be designed for, or encouraged for, business (including small businesses)?*
	A possible use case would be to develop customer personas to better aid our understanding of electricity consumption. The recent Electricity Authority Issues paper[2] referred to in footnote 2 below summarises the different uses of data and potential uses looking forward. These uses should be taken into account when developing the consumer data right framework.
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?*
	We do not consider accredited requestors and data holders should be required to receive consent from customers before their data is de-identified (and used for other purposes) or

[2] See the recent Electricity Authority Issues paper: Updating the Regulatory Settings for Distribution Networks December 2022 at https://www.ea.govt.nz/documents/1743/Issues-paper_-Updating-the-regulatory-settings-for-distribution-networks.pdf . See paragraphs 4.26 to 4.28.

	used in an anonymous form for research, infrastructure or general business planning or statistical purposes. The Privacy Act limits the use of personal information to the purpose for which it was collected. However, there are exceptions so personal information can be used for other purposes without the individual's consent, including if it is used in a form that does not identify individuals or is used for statistical or research purposes and won't be published in a form which would reasonably identify the individual. This is because the information, once de-identified or anonymous, is no longer information about an identifiable individual. We consider the same approach should be adopted in relation to the consumer data right, with data holders and accredited requestors being able to use customer data that is de-identified or anonymous for other purposes (including research or statistical purposes) without the customer's consent, as the de-identified information would no longer be information about that customer. Otherwise, this would be inconsistent with the Privacy Act. As noted at item 1 above, we consider the safeguards in the Privacy Act should be set out in the draft Bill to ensure a consistent approach across all types of consumer data. This would also ensure that the use of customer data which relates to non-natural persons (e.g. businesses) is also limited to the purpose for which it is collected (subject to the relevant exceptions in the Privacy Act). We consider the draft Bill should require accredited persons to act 'efficiently, honestly and fairly' when dealing with customer data or initiating actions (as is proposed under the Australian CDR amendment Bill).
20	*Are there other ways that ethical use of data and action initiation could be guided or required?*
	-
Preliminary provisions	
21	*What is your feedback on the purpose statement?*
	We agree with the purpose statement.
22	*Do you agree with the territorial application? If not, what would you change and why?*
	We agree with the territorial application.
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?*
	As noted at item 1 above, we consider the relevant protections from the Privacy Act should be set out in the draft Bill so that the protections extend to both individuals and non-natural persons, to ensure a consistent approach. This should include the reasons under the Privacy Act for a data holder refusing access to customer data (including if the data holder has reasonable grounds to believe that the request is made under the threat of physical or mental harm). These reasons should also extend to declining a request to perform certain actions under the action initiation regime where such circumstances exist.

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?*
	We think the draft Bill should expressly state that the record keeping requirements do not require the storage of the customer data itself.
26	*What are your views on the potential data policy requirements? Is there anything you would add or remove?*
	It is not clear what these policies would be required to contain. We consider the draft Bill should clarify this.
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	*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 Minister should also be required to have regard to any existing frameworks, regimes, legislation, standards or guidelines already in place in the relevant industry before recommending designation. Otherwise, we agree with the matters to be considered.
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?*
	-
30	*What should the closed register for data holders and accredited requestors contain to be of most use to participants?*
	As noted at item 6 above, we consider the data holder should be able to rely on evidence provided by the accredited requestor as part of the request to confirm the relevant customer's authorisation and identity. However, to the extent this onus remains with the data holder, we consider this closed register should also include information about customers' authorisations (including the scope of such authorisations), to assist data holders to check on the register whether customers have authorised requests for data without having to separately verify this with

	the customer. The data holder should be able to rely on the accredited requestor to provide this information for the register.
31	*Which additional information in the closed register should be machine-readable?*
	-
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 agree the yearly reporting date of 31 October for the period ending 30 June is suitable.
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?*
	So long as the technology is able to readily support this type of reporting and the information is helpful and relevant for the sector concerned, then real-time reporting maybe appropriate. Before this type of reporting is introduced, it should be considered on an sector by sector basis.
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 agree that the amount of customer redress should be capped (but that the cap can be reviewed and adjusted by the Minister of Commerce and Consumer in line with the Consumer Price Index, as with the approach taken in the Financial Reporting Act 2013). We consider this requirement to have a cap should be set out in the draft Bill (but that the regulations could specify the amount of such cap). See also our comments in relation to loss or damage to customers at item 39 below.
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 agree that disputes should be dealt with through existing industry dispute resolution schemes, with the Disputes Tribunal as a backstop. For example, certain industry participants under the Electricity Industry Act 2010 are already required to be part of the dispute resolution scheme under that Act. If a different dispute resolution scheme was imposed on those participants under the framework, this would create inefficiencies and duplication.

Other comments

Please see our additional comments on various aspects of the draft Bill below.

	Definition of data
36	We consider the definition of data is too broad.

The term 'data' is not defined in the draft Bill, with the draft Bill only providing that data includes information (including personal information under the Privacy Act 2020).

The MBIE discussion document states the intention is for the term 'data' to include derived data, and data derived from derived data. This is a very broad definition of data. This may compromise data holders' intellectual property (e.g. where data is derived through the application of internal analysis or enhanced using other intellectual property of the data holder) and could extend to data derived by an organisation for their own competitive advantage. We consider the definition of data should be limited to exclude derived data.

In particular, it is vital for Orion to innovate and seek out ways to support Central Canterbury's rapid growth, deliver on our commitment to confronting the climate emergency and respond to our customers' increasing desire for control over their energy choices. The proposed wide definition of data may impact on our ability to do so.

Outsourced providers – 'all reasonable steps'

37 Currently under the draft Bill, a data holder must take all reasonable steps to ensure that any outsourced provider it engages complies with the outsourced provider's obligations under the legislation.

We think the draft Bill should clarify what taking 'all reasonable steps' includes. In our view data holders should be deemed to have taken 'all reasonable steps' if they put in place adequate contractual arrangements with the relevant outsourced provider (including requiring the outsourced provider to comply with the legislation where applicable).

Outsourced providers – information to be provided to customers

38 The draft Bill provides that regulations made under the legislation may also require a data holder to provide information to a customer about outsourcing arrangements.

We consider the draft Bill should be clarified to outline what information will be required to be provided to customers and to clarify that data holders will not be required to provide the commercial terms agreed between the data holder and outsourced provider as part of this information.

Loss or damage suffered by customers

39 Currently under the draft Bill (clause 56), if a data holder contravenes a duty imposed by the legislation and a customer has suffered, or is likely to suffer, loss or damage because of the contravention, the data holder must take the steps prescribed by regulations to avoid, mitigate or remedy that loss or damage.

We consider that the threshold in this provision should instead require the customer to suffer, or be likely to suffer, *serious harm* (instead of just any loss or damage), which is the threshold under the mandatory breach reporting regime in the Privacy Act.

Express and informed consent

40 Under the draft Bill, consent must be express and informed consent. We consider the draft Bill should clarify what 'informed' consent will require from a data holder (including what information the data holder will be required to provide to customers to discharge this obligation).