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

Your name and organisation

Name	Jane Brown
Organisation (if applicable)	Te Kāhui Inihua o Aotearoa/The Insurance Council of New Zealand (**ICNZ**)
Contact details	Privacy of natural persons

Thank you for the opportunity to submit on MBIE's Unlocking value from our customer data discussion document (**discussion document**) and exposure draft of the Customer and Product Data Bill (**Bill**).

By way of background, ICNZ's members are general insurers and reinsurers that insure about 95 percent of the Aotearoa New Zealand general insurance market, including about a trillion dollars' worth of Aotearoa New Zealand assets and liabilities. ICNZ members provide insurance products ranging from those usually purchased by individuals (such as home and contents, travel and motor vehicle insurance) to those purchased by small businesses and larger organisations (such as Product and Public Liability, Business Interruption, Professional Indemnity, Commercial Property and Directors' and Officers' insurance).

This submission is provided by ICNZ on behalf of itself and its members, noting that members may also choose to submit individually.

The submission is in two parts:

- Overarching comments on the consultation, and
- Responses to discussion document questions.

Overarching comments

Consultation process

ICNZ is appreciative of the opportunity to engage on an exposure draft Bill but note the limited duration of this consultation (one month, compared to the over two months provided for feedback on the initial CDR options paper in 2021) and its timing (coinciding with school holidays). We appreciate that it is likely there are timing pressures during an election year but point out that such limited consultation timeframes can affect submitters' ability to thoroughly consider and discuss a topic, particularly for member organisations such as ICNZ.

Aotearoa New Zealand should take learnings from other CDR regimes

ICNZ broadly supports a consistent approach with the consumer data right (**CDR**) in Australia so that lessons can be learnt from their implementation to simplify ours, and interoperability between the two countries' regimes can be enabled. However, in order to ensure that the regime in Aotearoa New Zealand does not recreate issues already experienced in Australia, there must be flexibility provided for in our legislation. This is particularly so noting the recent slowdown and 'consolidation'

phase taking place in Australia which illustrates that the original system has not necessarily worked as envisaged.[1]

The CDR regime that is developed with the banks must also apply to other sectors

Because work on open banking is already underway, the CDR regime is essentially being built around the banking sector. While we agree that this is a logical place to start given use cases have been identified there, it is essential that the CDR regime is not structured in a way that works for banking and then is expected to apply across other sectors while not being specifically built to accommodate them. The regime must be constructed in a way that will recognise the differences and intricacies of other sectors such as general insurance.

Insurance is fundamentally different from banking in a range of ways. This includes:

- the diversity of products that are offered (there are many different insurance products and variations in each product between individual insurers – this variation in product also means that there is a lack of uniformity in the data held by insurers),
- the data held (data held by insurers often relates to the insured asset, rather than to the individual and therefore only remains relevant while the individual retains the asset),
- customer interactions (insurer-customer interactions are relatively infrequent and tend to focus on claims or annual renewal), and
- the nature of within-sectoral interactions (e.g., the use of different types of intermediaries and different distribution arrangements).

For completeness, and consistent with ICNZ's previous position, we reiterate that we do not believe that insurance should be considered for designation until the CDR regime is properly formed and understood, and preferably, until the equivalent regime has been implemented in Australia, with time to learn from its implementation. There does not appear to be a pressing need for insurance to be one of the next designations, as we believe that the barriers to shifting insurer mentioned in the previous consultation, are low. As general insurance policies are renewed on an annual basis, customers are essentially provided with a yearly prompt to consider the pricing and appropriateness of their insurance arrangements.

For further details on why we do not consider insurance is appropriate for designation before the regime has had time to mature and why other sectors should be prioritised, please refer to ICNZ's 2020 submission on MBIE's Options for establishing a consumer data right in New Zealand.[2]

Designations beyond the banking sector

Consistent with the above, before any further designations beyond banking are made, there needs to be clear use cases that demonstrate that the CDR regime is delivering benefits to customers, having regard to wider and specific impacts. There will need to be a positive cost/benefit analysis overall (which includes the impact of implementation costs) and careful consideration must be given to potential risks or adverse outcomes that could result from further designation.

It is essential, when considering further designation, that the sector is provided sufficient time to engage on the documentation of the requirements, the development of the rules, standards and guidelines, and to build and implement the necessary enhanced functionalities to ensure effective management of risks and quality solutions for consumers. For the general insurance sector, this comment should be read in the context of the increased and changing regulation already affecting the sector, which will require extensive reviews and the implementation of new processes.

---

[1] The Australian Government's statement in response to the Statutory Review of the Consumer Data Right released in June 2023 states that the system should be allowed to "mature" and improving CDR functionality and data quality within the already designated banking and energy sectors should be prioritised.

[2] ***https://www.icnz.org.nz/wp-content/uploads/2023/01/ICNZ_submission_on_Consumer_Data_Right_071020.pdf***, specifically page 17 onwards.

A CDR regime will create risk as well as benefits

It should also be noted that with complex changes of the nature of the CDR, there are almost always downsides that will need to be carefully considered and managed. While it may seem obvious that opening up the sharing and use of data will improve financial inclusion for some people, there may be other parts of society who suffer detriment, or are excluded from financial advancement, under such changes. A report from EIOPA[3] identifies obvious risks such as data breach, misuse of data, and fraud, as well other more specific risks like financial exclusion, market fragmentation, an undue focus on headline prices over quality, and lock-in risks for consumers with certain platforms.

[3] European Insurance and Occupational Pensions Authority 'Open Insurance: accessing and sharing insurance-related data', available at: ***https://www.eiopa.europa.eu/consultations/open-insurance-accessing-and-sharing-insurance-related-data_en#reference-%20documents***.

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?*
	In principle, ICNZ is supportive of utilising the Privacy Act, as opposed to creating a parallel regime under the Bill, as was required in Australia. However, we are not convinced that the Privacy Act is entirely fit for purpose, for the proposed functions under the Bill (for example, see our comments about the ability for a data holder to refuse a data request and the proposed penalties below). It is essential that there is full confidence in the Privacy Act's ability to interact with any CDR regime so that a need to revise the privacy legislation doesn't arise. Any revision of the privacy legislation at the same time as the implementation of the CDR regime would be problematic for participants with increases in the cost and complexity of implementation, as well as the likely creation of delays. We note that Aotearoa New Zealand's Privacy Act falls some way behind the protections provided by the likes of the European GDPR. We therefore question whether consideration has been given to how the CDR will impact on New Zealand businesses who deal with citizens of the EU. To ensure that the interaction and overlay of the Bill and the Privacy Act are fully understood, we encourage MBIE to consider the creation of guidance on how certain Information Privacy Principles apply. For example, if a data holder receives a request to share a customer's personal information, does the data holder have an obligation under IPP 8 to first check the accuracy of that information before sharing. Guidance should also explain what should happen in the instance of any inconsistency between the Bill and the Privacy Act, and which legislation should supersede the other.
Consent settings: respecting and protecting customers' authority over their data	
2	*Should there be a maximum duration for customer consent? What conditions should apply?*
	ICNZ's view is that a maximum duration for customer consent of 12 months would be appropriate. We agree that the 12-month period used in Australia would be more workable than the 90-day period in the UK and that longer than 12 months would risk a 'set and forget'-type situation for consumers. Twelve months therefore appears to provide a balance of being a reasonable time period for a consent to last while not being administratively burdensome on either the data holder, requestor or customer. ICNZ agrees with the proposal in paragraph 65 of the discussion document that when a customer closes an account with a data holder or when a service relationship ends, associated consents should expire.
3	*What settings for managing ongoing consent best align with data governance tikanga?*
	While ICNZ does not have any specific feedback on managing ongoing consent, we would be supportive of settings that encourage customers to engage with the CDR regime and to take active management of their consents. That way, use of the CDR by customers will be more meaningful and they will be able to retain greater control of their data.

4	*Do you agree with the proposed conditions for authorisation ending? If not, what would you change and why?*
	We believe that the proposed conditions for ending authorisation appear broadly appropriate. However, going forward, it will be necessary that the regulations recognise different relationships in different sectors beyond the holding of "an account", which appears to be language that would largely relate to banking.
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 comments.
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?*
	ICNZ generally agrees that the proposed obligations under the draft law and regulations are appropriate. In particular, we support clause 34 of the draft Bill relating to customer control of authorisation. It will be important that the giving of consent does not legitimise wide use of data beyond what a customer would expect. While recognising the obligations relating to use of personal information in the Privacy Act, it may also be helpful to have a specific standard under the CDR regime relating to reasonable use of customer data. We note that it is possible that practical issues could arise when implementing some of the obligations. For example, requiring data holders to notify requestors of withdrawal of consent will be simple where there is only one requestor. However, the process could become more complex and onerous if there are multiple requestors involved, which will often be the case. Clause 34(3) of the draft Bill provides that "The data holder or accredited requestor must ensure that the systems are able to give effect to a withdrawal of an authorisation with immediate effect". We consider "with immediate effect" should be amended to "as soon as practicable" for practical purposes, for example, with digital channels such as email, requests after hour requests or that are not within business days cannot always be actioned with immediate effect.
Care during exchange: standards	
7	*Do you think the procedural requirements for making standards are appropriate? What else should be considered?*
	ICNZ is supportive of the proposed procedural requirements for the setting of standards. Our only recommendation would be that clause 88(1) should make it clear that the persons "substantially affected by the issue of the proposed standard" includes sectors that will be subject to the standard. This should include both data holders and the sectors envisaged to be material users of that data as usage may impact on the functioning of competitive markets.
8	*Do you think the draft law is clear enough about how its storage and security requirements interact with the Privacy Act?*
	ICNZ has a strong preference for the Privacy Act's storage and security requirements to also apply to the CDR regime, rather than there being two parallel regimes. However, we would

	have to defer to any assessment or advice from the Office of the Privacy Commissioner (**OPC**) as to the practical effectiveness of the existing requirements.
9	*From the perspective of other data holding sectors: which elements of the Payments NZ API Centre Standards[4] are suitable for use in other sectors, and which could require significant modification?*
	No specific comments, further consultation on technical standards would be required with impacted sectors at the time consideration is given to applying the CDR to them.
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?*
	Refer to answer to question 9 above.
Trust: accreditation of requestors	
11	*Should there be a class of accreditation for intermediaries? If so, what conditions should apply?*
	ICNZ is comfortable with the explanation in paragraphs 93 and 94 of the discussion document that unlike Australia, a special class of accreditation for intermediaries is not required under Aotearoa New Zealand's CDR regime.
12	*Should accredited requestors have to hold insurance? If so, what kind of insurance should an accredited requestor have to hold?*
	ICNZ would not support any mandatory requirement for accredited requestors to hold insurance but would be open to the inclusion of a non-prescriptive requirement for requestors to have suitable arrangements in place to cover civil liabilities that may arise. It is important to allow for a degree of flexibility as some entities may not be able to obtain insurance, while others may be in a position to self-insure, or choose to use other financial instruments (such as guarantees) instead. It is also important to consider the role of insurance and its limitations. For example, we presume that MBIE anticipates that the most appropriate type of insurance for an accredited requestor might be professional indemnity or statutory liability insurance. It should be noted that the primary purpose of these lines of insurance is to provide protection for those providing the advice or service. They should not be seen as a surety of compensation for the customers or users of a requestor. When considering feedback on this question, we recommend that MBIE look to the equivalent Australian legislation which states "*A person who is accredited at the "unrestricted" level must have adequate insurance, or a comparable guarantee…"*.[5] We believe that this would be appropriately flexible wording to adopt (and potentially with the addition of "adequate insurance, if available"), rather than mandating the holding of insurance only, or a particular type of insurance.

[4] 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.

[5] Competition and Consumer (Consumer Data Rights) Rules 2020, s 5.12(2)(b).

13	*What accreditation criteria are most important to support the participation of Māori in the regime?*
	No comments.
14	*Do you have any other feedback on accreditation or other requirements on accredited requestors?*
	ICNZ is supportive of the idea of a fast-track to accreditation for businesses with similar processes for other domestic schemes. We believe that this could include other sectors with strict eligibility requirements under legislation such as the Insurance (Prudential Supervision) Act 2010 and the Financial Markets Conduct Act 2013. Allowing a fast-track obligation will help to minimise compliance costs for entities under the CDR regime.
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.*
	In relation to the potential defining of 'Māori data' under the Act, the definition of this and its application would need to take account of the ability of data holders to apply such differentiations and the potential consequences of doing so. We note for example that it is highly unlikely any business within the insurance industry would be doing this today. When it comes to implementation of the regime, it would also be helpful for MBIE to identify Māori data sovereignty experts who would be able to support designated industries in correctly applying specific requirements relating to Māori or Māori data. This would help to ensure that entities are able to apply the CDR in a way that best helps meet the needs of Māori.
16	*What are specific use cases which should be designed for, or encouraged for, business (including small businesses)?*
	No comments.
17	*What settings in the draft law or regulations should be included to support accessibility and inclusion?*
	No comments.
18	*In what ways could regulated entities and other data-driven product and service providers be supported to be accessible and inclusive?*
	It should be recognised that the CDR regime is not going to be attractive or usable for some parts of the community, particularly those with low technological and/or financial literacy. We would support efforts to support inclusion and accessibility such as those 'data for good'

	initiatives referenced in paragraph 129 of the discussion document and recognise these may need to have sector specific elements.
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?*
	ICNZ supports the idea of ethical requirements for accreditation in principle, but notes that this in itself, would not be sufficient to avoid adverse outcomes for some customer groups. In relation to the two options for additional safeguards on the ethical use of customer data: • Option one is ICNZ's preferred approach: general insurers are already (or will be) subject to potentially related legal obligations which could also be applied in the CDR setting. • Option two risks creating barriers to access and additional cost: paragraph 145 of the discussion document recognises that if the participation requirements on participants in a regime are too high or costly, a law will not be able to achieve its purpose. ICNZ agrees with this sentiment and believes that option two would necessitate more input than customers would be willing to provide and could lead to them disengaging with the regime. • It should also be noted that data holders are often able to derive value from the data they hold in a de-identified manner which can subsequently be used to create value that is passed onto customers. It would not be beneficial to establish additional barriers to the creation of value for customers, such as by having to seek individual consent to de-identify data, particularly without a clear description of any problems with the current approach to de-identified data.
20	*Are there other ways that ethical use of data and action initiation could be guided or required?*
	Consistent with our response to question 19 above, some sectors will already be subject to legislation and guidelines/codes with obligations that extend to the use of data. In addition to the Financial Markets (Conduct of Institutions) Amendment Act 2022 conduct obligations referred to in paragraph 142 of the discussion document, which insurers are also subject to, ICNZ's members must adhere to the Fair Insurance Code which contains overarching requirements relating to transparency, honesty, fairness and utmost good faith.[6] More generally, across designated sectors, impact assessments could be used to guide the ethical use of data.
Preliminary provisions	
21	*What is your feedback on the purpose statement?*
	The draft purpose statement seems appropriate for the intent of the legislation.
22	*Do you agree with the territorial application? If not, what would you change and why?*

[6] ***https://www.icnz.org.nz/wp-content/uploads/2023/01/Fair_Insurance_Code_2020.pdf***.

	ICNZ supports aligning the territorial application of the draft Bill with the Privacy Act. We also agree that it is important that the CDR regime applies equally to entities carrying on business in Aotearoa New Zealand regardless of whether they have a physical presence in the country. If that is not the case, it could allow a competitive advantage to offshore entities.
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?*
	ICNZ agrees that Privacy Act protections for not giving access to information, such as that in section 57(b) should be maintained, and potential fraud should also be included as a reason for declining a request. It is possible that it would also be appropriate to include further reasons to decline a request and note the situations where the Australian law means that a data holder must refuse or not disclose CDR data. Rule 4.7 of the Australian CDR Rules allows the data holder to refuse to disclose data where: • the data holder considers it to be necessary to prevent physical, psychological or financial harm or abuse • the data holder has reasonable grounds to believe that disclosing some or all of the CDR data would adversely impact the security, integrity or stability of the Register of Accredited Persons or the data holder's ICT systems • the CDR data relates to an account that is blocked or suspended, or • it is provided for in the data standards.[7]
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 comments.
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 comments.
26	*What are your views on the potential data policy requirements? Is there anything you would add or remove?*
	We do not agree that the names of any outsourced providers used by an entity will be of interest or use to customers, nor does it seem relevant if the entity remains responsible for compliance with the CDR regime. All entities are likely to have numerous outsourced providers and providing a list of those via a customer data policy may be unhelpful and create confusion.

[7] ***https://www.oaic.gov.au/consumer-data-right/consumer-data-right-guidance-for-business/privacy-obligations/guide-to-privacy-for-data-holders#consumer-data-request-services***.

Regulatory and enforcement matters	
27	*Are there any additional information gathering powers that MBIE will require to investigate and prosecute a breach?*
	No comments.
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?*
	ICNZ agrees that the factors in clause 60 are appropriate and also suggests inclusion of the following: • The risks and downsides associated with enabling data sharing: including the risk of potentially adverse outcomes for customers in relation to, for example, the supply or pricing of products (i.e. the risk that customers who do not engage with CDR (because they do not have data to share or because they are not technologically capable of doing so) will often end up with a worse outcome than those who can and do).
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 comments.
30	*What should the closed register for data holders and accredited requestors contain to be of most use to participants?*
	No comments.
31	*Which additional information in the closed register should be machine-readable?*
	No comments.
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?*
	ICNZ supports a yearly reporting date of 31 October for the period ending 30 June, but strongly urges that reporting requirements are set to the minimum amount of information required to administer the regime so as to minimise compliance costs and time requirements for entities. We note that for some sectors, such as general insurance, these reporting requirements would come on top of an increasing number of annual reporting requirements.
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?*
	ICNZ strongly opposes any suggestion of a requirement for data holders to provide real-time reporting on the performance of their CDR APIs. This would create an additional level of compliance and operational costs that would not appear to be outweighed by the benefit of doing so.

34	*What is your feedback on the proposal to cap customer redress which could be made available under the regulations, in case of breach?*
	If there is to be a cap on the possible amount to be repaid for customer redress, it would be appropriate to be tied to CPI. However, we note that specifying refunds or redress in regulations may limit an entity's ability to apply other, more appropriate redress options, depending on the circumstances. It may also set an expectation of financial compensation in any instance of error or delay.
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?*
	ICNZ believes that it would be preferable in principle to align dispute resolution processes under this regime with existing mechanisms, rather than creating a new scheme. Further development may be required to operationalise this. We note that the 'Overview of the complaints system' diagram on page 54 of the discussion document is complex and would require new agreements and systems to be put in place in order to operationalise.

Other comments

Definition of data

It would be helpful to have greater clarity around what type of data it is expected would be shared under the regime. For example, while it can be assumed that "data" includes structured customer details, account details, and transaction details such as payments and claims, would it also include unstructured data, all interactions with a customer, and internal data (call recordings, any investigations, emails, metadata, etc.)? We are also cognisant that for example in relation to insurance claims there will be data about the customer but also potentially others (the details in a claim might relate to the person at fault for the motor vehicle claim, which could be an authorised driver of the person holding the policy or details of someone at fault that is not the policy holder or user of the policy holder's vehicle) and these will need to be considered in any future application of the regime.

There is also limited explanation provided in the discussion document about the purpose of extending the Bill to "Product Data" as well as "Customer Data". We would appreciate if MBIE could provide further information on the reasons for doing so, particularly as the definition of "Product Data" in clause 9 of the Bill is extremely broad and could potentially be onerous to comply with.

Interim orders under clause 51

We note that the High Court has the ability under clause 51(2) to make an interim order preventing the use of the powers under clause 49 to supply information, produce documents, or give evidence. It appears that there is a high threshold to be met before an order can be made (cl 51(2)(b) the applicant would suffer substantial harm from the exercise or discharge of the power). Noting that the effect of an interim order is merely to pause the exercise of the clause 49 powers temporarily until there is a final decision made on the proceedings brought by the applicant, we recommend that a lower threshold of harm is allowed for.

Proposed penalties

We note that the provisions relating to infringement offences, compensation orders, pecuniary penalties and criminal offences will be drafted after the main obligations and protections are finalised, but that the discussion document includes proposals for these. We believe that there is an unjustified disconnect between the potential penalties under this regime and that of the Privacy Act when so many protections under CDR are reliant on the privacy legislation. It seems inconsistent for the possible penalties under the CDR regime to be significantly higher than those under the foundational privacy legislation.