Consumer Advocacy Council

24 July 2023

Consumer Data Right Project Team
Ministry of Business, Innovation and Employment
PO Box 1473
Wellington 6140

By email: consumerdataright@mbie.govt.nz

Submission on: Discussion paper "Unlocking value from our customer data: A draft law to set standards and safeguards for customer and product data exchange."

Introduction

1.1 Thank you for the opportunity to make a submission on "Unlocking value from our customer data: A draft law to set standards and safeguards for customer and product data exchange"

1.2 This submission is from the Consumer Advocacy Council, the independent advocate for residential and small business electricity consumers in Aotearoa New Zealand.

1.3 Our comments on the discussion document are set out in the submission form below. Given the short timeframe for making submissions, we have focused our responses on selected questions.

1.4 If you have any questions regarding our submission, please do not hesitate to contact:
Tammy Peyper, manager, Consumer Advocacy Council
Email: info@cac.org.nz
Phone: 021 829 931

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

Your name and organisation

Name	Tammy Peyper
Organisation (if applicable)	Consumer Advocacy Council
Contact details	By email: tamrynne.peyper@mbie.govt.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?
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?
The Council has some concerns about the reliance on Privacy Act protections and we recommend safeguards should be better aligned with the Australian CDR. In particular, protections should include the right for a consumer to request deletion of personal information and prohibition of the use of CDR data for direct marketing. We consider the addition of these rights would enhance consumer protection and trust in the CDR regime. We also note that consumer redress under the Privacy Act can be slow, particularly where cases are referred to the Human Rights Review Tribunal. Consideration therefore needs to be given to ensuring consumer complaints are investigated promptly. This is likely to require additional resourcing for the Office of the Privacy Commissioner and the Tribunal.
Consent settings: respecting and protecting customers' authority over their data
Should there be a maximum duration for customer consent? What conditions should apply?
The Council considers a maximum duration for customer consent should be included. Alignment with the 12-month expiry period in Australia may be appropriate. However, it is also essential the customer has the ability to nominate a shorter timeframe where, for example, they intend their interaction with the provider to be a one-off.
What settings for managing ongoing consent best align with data governance tikanga?
In the Council's view, processes for management of ongoing consent must be based on an 'opt in' approach; that is, providers must be required to gain specific consent from the customer rather than rely on the customer to opt out.
Do you agree with the proposed conditions for authorisation ending? If not, what would you change and why?
In principle, the Council agrees with the proposed conditions for authorisation ending outlined in para 65.
How well do the proposed requirements in the draft law and regulations align with data governance tikanga relating to control, consent and accountability?
Regulations must clearly set out providers' obligations for obtaining consent and acting promptly on customers' requests to withdraw consent. We recommend regulations should specify timeframes within which providers must act on requests from a customer to withdraw consent. Penalties must apply for failure to comply with specified timeframes.

	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?
	See comment above.
Care during exchange: standards	
	Do you think the procedural requirements for making standards are appropriate? What else should be considered?
	The procedural requirements seem appropriate. However, consideration should be given to how consumer participation in the development of standards will be supported. Consultation processes must ensure consumers are able to participate and that their views are represented.
	Do you think the draft law is clear enough about how its storage and security requirements interact with the Privacy Act?
	See our comments on the enforcement of the Privacy Act in response to question 1.
	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?
	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?
	High security standards are essential to provide effective consumer protection. We therefore do not consider high standards should be regarded as a barrier to entry.
Trust: accreditation of requestors	
	Should there be a class of accreditation for intermediaries? If so, what conditions should apply?
	The Council supports the approach in the draft law that businesses helping other businesses (i.e., intermediaries) to request designated data would be expected to become accredited requestors. To ensure adequate consumer protection, we consider the same rules and standards should apply to intermediaries.
	Should accredited requestors have to hold insurance? If so, what kind of insurance should an accredited requestor have to hold?

[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.

The Council supports requirements for accredited requestors to hold insurance. We agree this will increase the ability of customers to obtain redress or compensation for harm or loss. The approach suggested (para 105) where the accrediting agency will assess the adequacy of insurance cover seems appropriate.

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

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

The Council considers robust disclosure requirements must be placed on providers in relation to how data is used. To enhance consumer protection, we suggest data should only be used for other purposes (such as research or sale to third parties) where the customer has specifically 'opted in' to this use.

We note current disclosures under the Privacy Act about how customer data may be used are often contained in lengthy terms and conditions and fail to provide sufficient detail for consumers to identify how their data may be used. We therefore consider CDR regulations must contain specific requirements regarding the form and content of disclosure.

Unlocking value for all

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.*

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

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

The Council suggests consideration should be given to how organisations working with low-income consumers or disadvantaged communities may be able to enhance their services through participating in the CDR framework. As well as providing open access to 'good practice' resources, financial support may be needed for the non-profit sector.

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

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?

The Council supports requiring express consent for de-identification of customer data. Consumers should have control over how their data is used: this should be the starting point for designing ethical standards. A requirement for express consent is consistent with this and a necessary consumer safeguard.

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

Preliminary provisions

What is your feedback on the purpose statement?

In the Council's view, the purpose statement should specifically acknowledge the purpose of providing consumers with rights to access and control the use of their own data.

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

The Council agrees with the territorial application. This is consistent with other consumer protection legislation.

Regulated data services

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

We agree it is appropriate that data holders should not be able to deny a valid request. Requests should only be able to be denied where there are reasonable grounds to believe they are being made unlawfully or would result in harm.

Data holders will need to ensure they have appropriate processes in place in order to flag requests deemed to be invalid or unlawful and be able to justify their grounds for denying requests.

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

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?
The Council agrees record keeping requirements are essential to enable effective monitoring and enforcement. Requiring providers to keep records for a specified timeframe is therefore appropriate. We suggest this timeframe should be seven years, rather than five, to make it consistent with requirements for retention of financial records.
What are your views on the potential data policy requirements? Is there anything you would add or remove?
We consider the data policy also include information about provider's ownership and related parties (if any) to help inform consumers about the company and their decision on whether they wish to use its services.
Regulatory and enforcement matters
Are there any additional information gathering powers that MBIE will require to investigate and prosecute a breach?
Administrative matters
Are the matters listed in clause 60 of the draft law the right balance of matters for the Minister to consider before recommending designation?
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?
What should the closed register for data holders and accredited requestors contain to be of most use to participants?
Which additional information in the closed register should be machine-readable?
Is a yearly reporting date of 31 October for the period ending 30 June suitable? What alternative annual reporting period could be more practical?
Should there be a requirement for data holders to provide real-time reporting on the performance of their CDR APIs? Why or why not?

The Council considers a real-time reporting requirement would improve the ability of the regulator to monitor the market and the outcomes for consumers. We therefore support introduction of this requirement.

What is your feedback on the proposal to cap customer redress which could be made available under the regulations, in case of breach?

Our main concern with setting a cap on customer redress is that it may be difficult to identify a specific amount that will provide adequate compensation in every case where the provider's error or delay has caused financial loss to the customer.

Regulations could instead list the types of expenses for which providers will be liable (e.g., late payment fees incurred as a direct result of the provider's error) without stating the amount and without limiting consumers' rights to seek redress for other costs (as provided for in clause 58 of the bill).

Complaints and disputes

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?

The Council considers the Disputes Tribunal would not provide a sufficient backstop where a provider is not a member of an established dispute resolution scheme, such as the Banking Ombudsman or Utilities Disputes.

First, consumers who take cases to the Tribunal incur a filing fee, whereas the Banking Ombudsman and Utilities Disputes schemes are free.

Second, the threshold for taking cases to the Tribunal is low: $30,000. In contrast, the Banking Ombudsman can hear claims to up $350,000.

Third, few decisions of the Tribunal are published, reducing the opportunity for scrutiny of complaint decisions.

We therefore recommend membership of a free and independent dispute resolution scheme should be a requirement for accreditation.

Other comments