MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT
HĪKINA WHAKATUTUKI

Response to submissions on the exposure draft Customer and Product Data Bill

Summary of changes and where changes were not made in response to feedback

- The Customer and Product Data Bill (**the Bill**) is currently before Parliament, and aims to establish an economy-wide framework to enable greater access to, and sharing of, customer and product data between businesses. This is commonly referred to as a "consumer data right". The Bill gives customers (including both individuals and entities) in designated sectors greater control over how their customer data is accessed and used, promote innovation and facilitate competition, and facilitate secure, standardised, and efficient data services.
- In June 2023, the Ministry of Business Innovation and Employment released an exposure draft of the Bill. Submitters broadly supported the approach and objectives of the Bill, however, they provided feedback on a range of specific issues. You can view the submissions here.
- This document summarises:
  - the significant changes that were made to the Bill in response to feedback
  - some of the key themes from submission that did not result in changes to the Bill.

SUMMARY OF SIGNIFICANT CHANGES

Commercial information

Clause 100(2) of the Bill adds new restrictions to what product data can be required to be shared (e.g. data holders' do not have to share product data that is not ordinarily publicly available).

This change responded to concerns about the lack of limits on the range of information that may be required to be disclosed, such as commercially sensitive data or data that has been produced or enhanced by the application of proprietary analysis.

For product data, it was not the policy intent for the Bill to generally require data holders to produce and disclose new, non-public information. The Bill was therefore changed to clarify what data can be designated, to ensure that the scope of powers to make secondary legislation are clear and appropriately constrained.

Removing outsourced providers

The exposure draft Bill included provisions for dealing with 'outsourced providers', which are persons to which an accredited requestor or data holder has contracted out the performance of a duty or power they hold under the regime.

The concept of 'outsourced providers' has been removed from the Bill. This was removed to simplify the Bill. We consider the approach of leaving any issues around outsourcing to be

addressed by participants in the system and general legal principles, rather than by the Bill, is more appropriate.

Declining requests

Some submitters raised that there are a range of valid reasons to decline requests that were not included in the exposure draft Bill. These include where the request is part of a cyber-attack, or a customer is known to have been subject to identity theft. For designated actions, it also includes situations where, for example, a person has insufficient funds in their bank account to make a payment.

We agree with this feedback and therefore have amended the Bill to provide for circumstances where data holders may or must decline requests.

Clause 16(1) and 20(1) of the Bill adds circumstances where data holders may decline requests for designated data or actions (e.g. in the interest of preventing harm to an individual or the public).

Clause 16(2) and 20(2) of the Bill add new requirements for data holders to refuse requests where they have reasonable grounds to believe that the request is made under the threat of physical or mental harm.

Customer redress

Most submitters opposed placing a cap on the amount of compensation that could be made available to customers in the event of a breach of the Bill. A reason for this, among others, was that it unfairly and unduly limited the ability for customers to seek redress. We agree with this and have amended the Bill to:

- provide that where a data holder or accredited requestor has breached obligations, that any person may apply to a court for compensation for loss or damage (see clause 80).
- remove the cap on compensation, and allow for regulations to set processes for resolving breaches between data holders, accredited requestors and customers (see clauses 59 to 63).

Dispute resolution

Clauses 50 and 51 of the Bill provide that data holders and accredited requestors can now be required to be members of existing dispute resolution schemes. Clause 95 of the Bill provides that the Disputes Tribunal may be used by customers. The Disputes Tribunal can therefore be used where data holders or accredited requestors are not members of an industry dispute resolution scheme.

Procedural requirements

Submitters raised various suggestions for improvements to the consultation requirement provisions, particularly the need for procedural requirements in relation to the making of other regulations. Submitters were also broadly supportive of means to support Māori participation in the regime. We agree with these suggestions and have amended the Bill to give effect to this.

The Bill now extends the consultation requirements to the development of all relevant regulations (of which previously only applied to designation regulations). This includes that the Minister must consult, among others, 1 or more people who have expert knowledge of te ao Māori approaches to data. See clause 131.

Standards

The exposure draft Bill did not provide for circumstances where the chief executive could make or change the standards without consulting. This was an issue as the chief executive may need to make urgent or minor amendments to existing standards without consultation (e.g. to address security issues or to ensure the ongoing operation of the regulated data services).

To address this, the Bill has been changed to allow the chief executive to make urgent or minor and/or technical amendments to existing standards without consultation (see clause 134(3)).

Secondary users

The exposure draft Bill did not provide for requests or authorisations to only be given by secondary users in certain circumstances. This was an issue as there may be circumstances where, in the interest of the customer, requests should only be given by secondary users (e.g. where customers are under 18 years old, or customers are under guardianship or power of attorney).

To address this, the Bill has been changed to provide a new regulation making power that can require requests or authorisations only be given by secondary users (see clause 25).

Offences and penalties regime

The Bill now has an offences and penalties regime that was not included in the exposure draft Bill.

The table below provides an overview of the offences and penalties regime in the Bill.

Penalty	Breach
Infringement notice of up to **$20,00.** Infringement offence of up to **$50,00.**	Failure to meet: • disclosure requirements (clause 35) • record-keeping requirements (clauses 45 and 46) • certain policy requirements (clause 58) • annual reporting requirements (clause 114).
For a body corporate, a fine of up to **$300,000.** For an individual, a pecuniary penalty of up to **$100,000.**	Failure to test electronic system when requested by MBIE (clause 30). Failure to supply information requested by regulator (clause 58).
For a body corporate, a pecuniary penalty of up to **$600,000.** For an individual, a pecuniary penalty of up to **$200,000.**	Data holder fails to provide regulated data service to customers and accredited persons.

	Failure to meet a number of requirements to support the performance of the regime (e.g. technical standards, annual reporting). A person fraudulently holds out that they are an accredited requestor. See clause 75 of the Bill for more detail.
For a body corporate, a pecuniary penalty of up to **$2,500,000.** For an individual, a pecuniary penalty of up to **$500,000.**	Data holder fails to: • operate an appropriate electronic system (clause 27) • verify identity of who makes request (clause 44). A person requests regulated data services when they are not permitted to (clause 42).
For a body corporate, punishable on conviction by a fine of no more than **$5,000,000**. For an individual, punishable on conviction to imprisonment of no more than 5 years, a fine of up to **$1,000,000**, or both.	A person knowingly makes a request for regulated data services they are not permitted to make (clause 43).

The general approach taken for the offences and penalties regime is for various minor contraventions of the Bill to be defined as infringement offences and for penalties to escalate in harshness based on risks to the regime for non-compliance, incentives for non-compliance, and where the conduct is particularly egregious or harmful.

Clause 91 provides for general defences for person in contravention of a civil liability provision and clause 92 provides a defence for contravention due to a technical fault in an electronic system.

Information sharing

Clauses 123 to 125 provide new powers that the chief executive may share information, subject to certain conditions, that they hold under the Bill with certain other people and agencies (e.g. the Privacy Commissioner, the Commerce Commission, or the Ministry of Justice).

This gives effect to the Cabinet decision that the CDR Bill, among other things, enable information sharing or collaboration with other regulators [DEV-22-MIN-0151 refers].

Privacy Act 2020

The Bill now specifies that:

- a customer's request for data is not an IPP 6[1] request under the Privacy Act 2020, however, if a data holder breaches certain requirements the data holder must be treated as being in interference with the privacy of an individual for the purposes of Parts 5 and 6 of the Privacy Act 2020 (clause 52).
- certain contraventions relating to storage and security are to be treated as breaching IPP 5[2] (clause 53).

In line with the purpose of the Bill, these provisions were added as they seek to enhance the access that customers otherwise have to their personal information, by facilitating secure, standardised efficient data services.

SUMMARY OF ISSUES RAISED WHERE CHANGES WERE NOT MADE

Duration of authorisation

Submitters had mixed views about whether there should be a maximum duration on authorisations.

We agree with submitters who raised that some use cases may require ongoing authorisation, and that concerns about ongoing authorisation can largely be addressed through periodic prompts or reminders to confirm authorisation. We also agree with submitters who raised that, even where a maximum authorisation is appropriate, consideration should be given to the wants of individual customers.

Further, we consider that such detailed authorisation requirements are more appropriate for regulations than the Bill. Accordingly, we did not make any changes to the Bill relating to the duration of authorisation.

Customer requests

Some submitters suggested that providing customers with direct access to customer data might be impractical or introduce unnecessary security risks, and therefore that this should be removed from the Bill.

We consider that providing for direct customer access to data will help to future proof the Bill, and the potential benefits outweigh the potential risks. Therefore, no change was made regarding customers' ability to make direct requests to data holders.

Safe harbour provision

Some submitters thought there should be safe harbour provision in the Bill to protect participants from liability insofar as they comply with their obligations under the Bill.

[1] IPP 6 is information privacy principle 6 in the Privacy Act 2020. This principle provides that an individual is entitled to receive access to their personal information from an agency, upon request.
[2] IPP 5 is information privacy principle 5 in the Privacy Act 2020. This principle provides storage and security and obligations on agencies that hold personal information.

We do not consider it necessary to include a safe harbour provision because:

- clause 18(1)(c) provides that a data holder only needs to perform an action on request where it would ordinarily do so in the course of its business.
- clauses 16(1), 16(2), 20(1), 20(2) provide for circumstances where data holders may or must decline requests, including where this may result in breaches to other laws.

Therefore, a safe harbour provision has not been added to the Bill.

For more information, please visit http://www.mbie.govt.nz/cdr.