



Feedback on the Customer and Product Data Bill exposure draft and discussion document
Ministry for Business, Innovation and Employment (MBIE)
15 Stout Street, Wellington Central, Wellington 6011
[by email: consumerdataright@mbie.govt.nz]

24 July 2023

Re: AWS comments on the Customer and Product Data Bill exposure draft and discussion document

Dear Madam/Sir,

Amazon Web Services New Zealand Ltd. (AWS) is grateful for the opportunity to comment on the *Customer and Product Data Bill* consultation document including the exposure draft of the Customer and Product Data Bill ('the draft law') and accompanying discussion document.

We believe that forthcoming Customer and Product Data legislation has the potential to further enable New Zealand's digital economy. At the same time, careful consideration and thorough public consultation is always important when regulating in any area that impacts personal data.

As you may be aware, AWS is the cloud computing arm of Amazon.com, Inc. AWS has been operating in New Zealand for 10 years. We have offices in Auckland and Wellington and employ more than 150 New Zealand staff in roles such as solutions architects, account managers, sales representatives and professional services consultants. In September 2021, AWS announced that it would establish an AWS Region in Auckland in 2024, which will bring world-class cloud computing infrastructure onshore to New Zealand. The Economic Impact Study¹ that accompanied the AWS infrastructure announcement estimated that this investment of NZ\$7.5 billion will create around 1,000 new jobs and contribute approximately NZ\$10.8 billion to New Zealand's GDP over 15 years. This cloud computing infrastructure will enable our thousands of active customers in New Zealand – including large enterprises, governments, and small businesses already using AWS global infrastructure – to leverage our advanced cloud services to innovate and scale using highly secure and resilient infrastructure located in New Zealand. Online we have published a number of [case studies](#) showing how banks and other financial service providers have built solutions on AWS because of the scalability, cost effectiveness, and the services AWS offers for analysing large volumes of data.² From this experience we wish to provide some recommendations for the New Zealand government to consider as it chooses to regulate consumer and product data rights. Where our comments relate to specific provisions we note the section and page number.

We welcome the Ministry for Business, Innovation and Employment's (MBIE) intent to connect this initiative to the Digital Identity Services Trust Framework Act (2023). We support MBIE's aim to encourage interoperability and to align with consumer data rights in place overseas. Aligning the definitions in the draft legislation with similar Australian legislation will simplify and facilitate business between New Zealand and Australian companies working in both jurisdictions. With this in mind, below is a summary of

¹ [AWS, Economic Impact Study, New Zealand Region \(2021\)](#)

² AWS for Financial Services, accessed 13 July 2023 <https://aws.amazon.com/financial-services/>

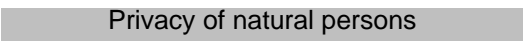


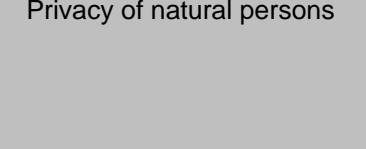
our initial recommendations on the exposure draft of the Bill. Additional detail and explanation on each of these recommendations is in **Appendix A**.

Recommendations on the exposure draft of the Bill

- **Recommendation 1:** Narrow the definition of “outsourced provider” in the exposure draft to subcontractors of data holders and accredited requestors that have been engaged to perform specified duties under the draft law (Section 23 of the draft law).
- **Recommendation 2:** Introduce a provision in the draft law equivalent to Section 11 of the Privacy Act 2020 (Privacy Act) to ensure that an entity cannot be classified as a data holder or outsourced provider in relation to data that it holds solely in its capacity as a service provider to another entity that actually controls that data. (As per discussion document question 1)
- **Recommendation 3:** Clarify that designated product data, designated customer data and designated actions can only include data or actions insofar as they relate to products or services (a) consumed in New Zealand, or (b) supplied to customers based in New Zealand (Section 11 of the draft law). (As per discussion document question 22)
- **Recommendation 4:** Clarify in the draft law that the Privacy Act only applies to the personal information that is included in any customer data requested in accordance with Sections 14 to 15 of the draft law. (As per discussion document question 1)
- **Recommendation 5:** Remove the “CPD storage and security requirements” in the draft law, as these topics are already covered by the Privacy Act. (As per discussion document question 8)
- **Recommendation 6:** Align the definition of product data in the draft law with the corresponding definition in the Australian [Competition and Consumer \(Consumer Data Right\) Rules 2020](#). (As per discussion document para 45)
- **Recommendation 7:** Introduce the concept of “materially enhanced information” (as defined in the Australian [Consumer Data Right \(Authorised Deposit-Taking Institutions\) Designation 2019](#)) in the draft law. As per discussion document para 45).

Additional detail on our recommendations and comments on the exposure draft of the Bill (**Appendix A**) and also some broader comments on open data, public cloud and data for good (**Appendix B**) are attached. Also for reference on AWS services as it relates to the New Zealand Privacy Act, the AWS White Paper on [Using AWS in the Context of New Zealand Privacy Considerations](#) is available online.

Thank you again for the opportunity to provide recommendations and comments. We would be pleased to elaborate further on our submission and look forward to remaining engaged in future consultations. In the event anything in our submission is unclear or if you would like additional detail, please do not hesitate to contact me on  Privacy of natural persons

Yours sincerely,
 Privacy of natural persons

Paul Keating
Head of Public Policy, New Zealand
Amazon Web Services New Zealand



Appendix A: Specific comments on the Exposure Draft of the Customer and Product Data Bill ('the draft law')

Definition of “outsourced provider”: Section 23

The definition of “outsourced provider” under Section 23(4) of the draft law is very broad and risks capturing outsourced providers that would not have the necessary access, visibility or ability to comply with the draft law. Under the draft law, a company is an outsourced provider if a data holder or accredited requestor has subcontracted the performance or exercise of a duty or power under the draft law to the outsourced provider. The discussion document outlined that an outsourced provider might be an entity which helps a data holder connect its data systems to enable regulated data services to be provided. This definition could accidentally capture third parties, like cloud service providers (CSPs) and other data processors, that do not have any control, access or visibility of regulated customer or product data and would not be able to comply with the customer request provisions in the draft law. As described in the [Using AWS in the Context of New Zealand Privacy Considerations](#) whitepaper³, customers using AWS maintain control over their content within the AWS environment. AWS does not access or use customer content without the customer’s consent, except as required to comply with a valid and legally binding order. AWS has no contact with the individuals whose personal information is included in content that a customer stores or processes using the AWS services. Therefore, even though AWS services may provide the underlying computing infrastructure that data holders use to store their customers' data, we would not be able to assist customers to comply with their duties under the draft law.

Recommendation 1: We recommend that the definition of outsourced provider should be narrowed to include only a provider that has been specifically engaged to assist a data holder or accredited requestor to perform or exercise its duties under the draft law. Specifically, we recommend the following amendment to Section 23(4):

“(4) In this section,—

(a) a person (A) is an **outsourced provider**, in relation to a data holder or an accredited requestor (B), if B ~~subcontracts~~ ~~contracts out~~ to A the performance or exercise of a **specified** duty or power under this Act:

(b) the **outsourced duty or power** is the **specified** duty or power **under the Act** that the data holder or accredited requestor has subcontracted to the outsourced provider to perform or exercise ~~has been contracted out.~~”

Recommendation 2: We recommend that government introduce into the draft law a provision equivalent to [Section 11 of the Privacy Act](#), which clarifies that where entity A holds customer or product data solely for and on behalf of entity B, and does not use it for its own purposes, then that data is treated as being “held” by entity B and not entity A. A similar clarification would be appropriate in the context of the draft law, to ensure that an entity cannot be classified as a data holder or outsourced provider in relation to data that it holds solely in its capacity as a service provider to another entity that actually controls that data. Further, this language would more closely align the draft law with leading international privacy

³ Available online at:

https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_New_Zealand_Privacy_Considerations.pdf



regulations, such as the European Union’s General Data Protection Regulation (GDPR), that draw clear distinctions between the roles and responsibilities of “processors” and “controllers”.

Territorial application: Section 11

We understand that the draft law is proposed to apply to New Zealand or overseas agencies carrying out business in New Zealand in line with Section 4 of the the Privacy Act. We believe an additional important nexus should exist – the draft law should only apply to products or services (a) consumed in New Zealand, or (b) supplied to customers based in New Zealand. Without these additions, the breadth of Section 11 of the draft law might require data holders to provide designated customer data to customers based outside of New Zealand or capture New Zealand technology companies that offer products exclusively to customers in overseas countries. This would be unduly onerous for both New Zealand entities exclusively serving customers internationally, and organisations who have limited operations in New Zealand and offer some services exclusively to customers outside of New Zealand.

Recommendation 3: We recommend that Section 11 be redrafted to clarify that designated product data, designated customer data and designated actions only include data or actions insofar as they relate to products or services (a) consumed in New Zealand, or (b) supplied to customers based in New Zealand.

Privacy Act considerations: Sections 44-48

It is our understanding that the draft law aims to enable individuals to access their data in a secure environment that is consistent with the Privacy Act and that Privacy Principle 6 (“**IPP 6**”) is proposed to apply to personal information included in any customer data requested under the draft law. We are supportive of this approach; however, we believe the current drafting of Sections 44 to 47 does not clearly articulate MBIE’s intention and may unintentionally create the impression that IPP 6 applies to *all* customer data. If MBIE seeks to extend the application of the Privacy Act to include other data, or decides to include “action initiation” in the draft law, we believe MBIE should engage in further public consultation to assess the very significant implications and consequences of these steps.

Recommendation 4: We recommend that Section 44 should be deleted, and Sections 45 to 47 should be amended to clarify that these provisions only apply to personal information that is included in any customer data requested in accordance with Sections 14 and 15 of the draft law.

Recommendation 5: We recommend that Section 48 should be deleted as it may cause unintentional confusion. The discussion document outlines that the draft law is not intended to change broader legal settings regarding collection, storage or security of personal information. We believe that introducing “CPD storage and security requirements” in Section 48 creates undue complexity in the legislation, given that any breaches of the Privacy Act relating to these topics will already be handled under Parts 5 and 6 of the Privacy Act.

Definition of “product data”: Section 9

The definition of “product data” in Section 9 of the draft law is very broad, i.e. “data that relates to a data holder’s products”. We understand that the data holder’s designated regulations will specify the categories of product data that are relevant to a particular industry, but this very broad language in the draft law might unintentionally create the risk of a data holder being asked to share product data that contains proprietary or confidential information or trade secrets, thereby potentially undermining a data holder’s ingenuity and investment in proprietary products.



Recommendation 6: We recommend that MBIE narrow the definition of product data in line with the Australian [Competition and Consumer \(Consumer Data Right\) Rules 2020](#) (“**CDR Act**”) to include only information about products that is publicly available. Under the CDR Act, data holders are only required to disclose product data that is not linked to a customer where it is (a) specific to a product, (b) held in digital form, (c) about the eligibility criteria, terms and conditions, price, availability or performance of a product, and (d) is publicly available if the data relates to availability or performance.

Recommendation 7: We recommend that MBIE apply the concept of “materially enhanced information” (as defined in the Australian [Consumer Data Right \(Authorised Deposit-Taking Institutions\) Designation 2019](#)) to customer data in the draft law. In Australia, data holders are not required to disclose information that is wholly or partly derived through the application of insight or analysis to customer data and that renders the data significantly more valuable as a result.



Appendix B: Comments on public cloud, open data and using data for good

Public cloud is an enabler to open data

Public cloud can empower data holders to unlock the value of their data at scale. Financial sector (FS) organisations hold vast amounts of data but struggle to extract value from this data at scale. By unlocking the value of data, FS organisations can deliver deeper and more personalised offerings, insights, and support to their customers and partners. The unlocked value can also help FS organisations quickly expose inefficiencies in current processes from capital markets to manufacturing operations, while providing prioritised insights into areas that require optimisation.⁴ From a single cloud interface, organisations can find and subscribe to a variety of financial data, such as insurance claims, consumer spending patterns, personal income data, customer demographics, ESG (environmental, social, and governance) ratings, and Financial APIs. For example, globally a number of banks are building open banking platforms in response to new regulations and customer demands.

Other international examples

In addition to other case studies that MBIE has considered, there are two case studies on open data which MBIE may wish to consider when reviewing its wider open data policy initiatives. These are both taken from the AWS whitepaper “Open Data on AWS”.⁵

The Government of Iceland leveraging ‘API and Open Data’

Digital Iceland accesses commercial technology skills by making a lot of its data open so developers can use it to innovate services. Open data feeds are shared via a unified API, which allows the aggregation and integration of data from different sources and in different formats. In turn, the developers share what works for them.⁶

The National Data Sharing and Accessibility Policy (NDSAP) in India

The NDSAP is applicable to all shareable, non-sensitive data that is generated by various ministries, departments, subordinate offices, organisations, and agencies of the federal and state governments of India. The objective of this policy is to facilitate access to Government of India–owned shareable data through a wide area network, thereby permitting a wider accessibility and usage by the public.⁷

Data for good initiatives

AWS has built data exchanges to help facilitate finding public datasets, registering datasets and sharing data through the cloud so more time can be spent on data analysis rather than data acquisition. Data exchange programmes like this make data available to encourage greater collaboration and innovation among a variety of industry participants. In New Zealand, Figure.NZ is taking New Zealand’s public data in its current form, extracting it and standardising it so it is easy to find and use. This is then published in charts, maps and tables for free access. This is a good example of opening up data for the benefit of all.⁸

⁴ [Unlocking the value of your data at scale in the financial services industry](#), AWS, September 2022

⁵ Open Data on AWS, 30 March 2022

https://d1.awsstatic.com/whitepapers/compliance/Open_Data_on_AWS_Cloud_2022.pdf

⁶ Ibid.

⁷ Ibid.

⁸ Use Figure.NZ “Publish your data”, accessed 11 July 2023 https://tohu.figure.nz/external/use_figurenz/#use-our-data