Xero Submission

New Zealand's Consumer and Product Data Bill

24 July 2023

External(np)

Please reconsider printing me unless absolutely necessary the environment will thank you

Xero Submission

Consumer and Product Data Bill

24 July 2023

24 July 2023

Consumer Data Right Project Team
Commerce, Consumers and Communications
Ministry of Business, Innovation & Employment
NEW ZEALAND

ONLINE SUBMISSION:
consumerdataright@mbie.govt.nz

Dear Consumer Data Right Project Team

XERO SUBMISSION REGARDING THE DRAFT CONSUMER AND PRODUCT DATA BILL

The role of Xero is to make life better for people in small business and their advisors. Therefore, our role is to act in the best interests of small business and on that basis Xero welcomes the opportunity to comment to officials on the proposed *Consumer and Product Data Bill*.

Open data systems lie at the heart of the digitisation of our economy which, in turn, can drive the related productivity gains that have so far eluded New Zealand. Given the importance that small business plays in the New Zealand economy, we are encouraged that the Government has drafted the *Consumer and Product Data Bill* that proposes a framework to realise the value of certain data for the benefit of individuals and society; promote competition and innovation for the long-term benefit of customers; and facilitate secure and efficient data services in certain sectors of the New Zealand economy.

Xero commends the proposed Bill's approach to align with New Zealand's existing Privacy Act.

However, we do have some specific concerns that we have noted in our submission in response to the Discussion Document's questions. In particular, we are concerned that:

- The proposed legislation does not define 'data' - we think this should form an important component of the draft legislation.
- We should learn from the Australian Consumer Data Right experience regarding 'derived data' which resulted in downstream data transfers creating burdensome requirements and efficiency loss. New Zealand legislation/regulation should not include any reference to 'derived data'.
- The proposed legislation will have multiple regulators that will add layers of complexity to managing the enforcement of draft Bill.

External(np)
Please reconsider printing me unless absolutely necessary the environment will thank you

- With regards to administration and governance activities (such as accreditation, decision making on standards, regulation setting and enforcement), we advocate that these activities should be overseen and governed by an independent arm's length government entity in order to mitigate any potential conflicts of interest and ensure equitable access for consumers and businesses.

We also note Xero's disappointment regarding timing: firstly, the timing of the consultation period was not foreshadowed in advance to industry participants; secondly, the timeframes being extremely compressed given the nature and size of the documents; and thirdly, the consultation timing being over a school holiday period. Such an approach limits the abilities of external parties to provide extensive and informed comments on such an important piece of draft legislation.

Additionally we acknowledge that our submission can be shared publicly and released under the Official Information Act and that Maureena van der Lem, Head of Government Experience for Xero, NZ Privacy of natural persons is the appropriate contact person for Xero.

Yours sincerely

Privacy of natural persons

Bridget Snelling
Xero Country Manager, New Zealand

1. Introduction

1.1. About Xero

1.2. Xero is a global small business platform with 3.7 million subscribers which includes a core accounting solution, payroll, workforce management, expenses and projects. Xero also has an extensive ecosystem of connected apps and connections to banks and other financial institutions helping small businesses access a range of solutions from within Xero's open platform to help them run their business and manage finances. Xero currently operates an extensive data sharing network in New Zealand at high quality, reaching the vast majority of financial institutions in the country.

1.3. Consumer and Product Data and Xero's Responsible Data Use

1.4. At Xero, we're committed to using data responsibly. As a global platform for small businesses, we know we have an obligation to collect, manage and use customer data in a responsible way to benefit small business owners, their advisors and their community. Therefore, we align with the proposal that respect, care, trust and the enabling of the future sit at the heart of New Zealand Consumer and Product Data (CPD) legislation. At Xero we are of the opinion that customer data belongs to the customer.

1.5. Xero's Responsible Data Use commitments are:

1. Data security and privacy

We are committed to keeping data secure and protecting privacy at all times, and supporting customers with product features and information to help customers do the same.

2. Benefits small business

We are committed to using the data we hold for the benefit of small businesses.

3. Customer control and consent

We are committed to giving customers control over their data by providing the tools to manage their consent for each product or service that uses their data.

4. Open and honest

When customers sign up for one of our products or services, we are committed to letting them know what the benefits are, how their data will be used, if we're providing their data to someone else, and who that is.

5. Fees we collect

We are committed to never charging anyone a fee to access customer's data without getting their consent first and explaining to customers the nature of the fees charged. We may charge a fee for products or services containing anonymous data without allowing an opt out for this.

6. Data-driven decision bias
We are committed to doing everything we can to get rid of unfair biases in data and our algorithms that might negatively affect customers.
7. Trusted partners
We expect our trusted partners to approach responsible data use the way we do, and are committed to bringing our partners on this journey with us.
8. Accountant and bookkeeper enablement
We are committed to supporting our accountants and bookkeepers by providing useful data and insights to help small businesses thrive, and to use data in a responsible way.

2. Six policy principles for consideration

2.1. Transparency

2.2. Transparency enables trust. It is essential that the CPD legislation enables trust by creating a transparent regime that protects the data rights of consumers/customers. This includes appropriately defining key terms such as 'data' in the legislation.

2.3. Innovation

2.4. At Xero, we believe that it is crucial that the CPD enables and does not overly constrain innovation and the use of new technologies or approaches. Access to data needs to be flexible - it is important that the CPD regime provides a data access framework for the purposes of testing and product/offer development.

2.5. Simplicity

2.6. In order to maximise compliance, the proposed CPD legislation needs to provide clarity and be simple to follow to avoid loopholes, complexity and overbearing compliance costs for industry participants. Any wider applications beyond the banking sector, should endeavour to be system applications rather than sectoral fixes which would result in a patchwork approach to data regulation.

2.7. Productivity

2.8. The proposed CPD legislation should enable individual and small business efficiency and effectiveness - saving time, providing real-time insights into cashflow and business performance - thereby enabling productivity output growth.

2.9. Interoperability

2.10. To derive the benefits of the CPD the legislation needs to enable alignment and, where possible, standardisation across a number of sectors and industries in the New Zealand economy.

External(np)
Please reconsider printing me unless absolutely necessary the environment will thank you

2.11. Good governance

2.12. Good governance and oversight are crucial to any regime. Xero proposes that any entity overseeing the administration and governance of the CPD legislation be independent of data holders or accredited providers to ensure minimal conflicts of interest.

3. Lessons from other jurisdictions

3.1. We note that the Discussion Document notes differences from the Australian Consumer Data Right (CDR) primarily around the proposed New Zealand legislation relying on the existing New Zealand Privacy Act which applies across the economy. Xero supports this approach.

3.2. Other lessons from the Australian CDR include:

i. The regime created tension between data transferred under the CDR regime and outside of it by inserting privacy principles into the CDR that exceed privacy legislation. This tension had the effect of incentivising data transfers outside the CDR.

ii. The inclusion of 'derived data' in the legislation, which resulted in downstream data transfers of data derived from (or derived from derived) CDR data having CDR rules and protections applied to it. This included CDR protections and restrictions applying to a small business which wanted to share its payrun information with its accountant for example.

iii. Rules stipulating the deletion of all CDR data upon a lapsed consent. This would require Xero to delete a customer's subscription in the event of an administrative oversight, which in many cases is a small business's sole trusted system of record, required to meet record keeping obligations.

3.3. The unworkable nature of the Australian CDR for non-individuals means today, very few small business services are available. As a result, next to no small businesses can utilise the CDR regime, while existing data transfer mechanisms continue to thrive. For Xero, our small business customers continue to access their financial data through commercially negotiated feeds. For the minority of accounts which don't have direct feeds, small business customers can access their data via screen scraping (or manual uploads).

3.4. In contrast to Australia, the Open Banking regime in the United Kingdom (UK) now has over 7 million regular users including over 750,000 small businesses (with Open Banking having a 16% penetration rate for businesses versus an 11% rate for consumers).[1]

3.5. The latest data shows that UK Open Banking has been disproportionately adopted by small businesses and the gap between the businesses and consumers is widening. This is largely down to more small businesses using cloud accounting software that uses Open Banking to import transaction data. Small business use is dominated by data-driven account information services which allow firms to see

[1] https://www.openbanking.org.uk/news/uk-reaches-7-million-open-banking-users-milestone/

multiple accounts in one place, providing real-time insights for cash flow and forecasting. This accounts for 79% of business use.[2]

3.6. In contrast, UK consumers are using more payment initiation services, which allow them to move money, for example, to top up wallets, or to pay tax or credit card bills.

3.7. However, one challenge that the UK regime has faced is ineffective penalties where participants do not meet the required standards. It is positive to see the steps taken in this regard for New Zealand's proposed CPD legislation.

3.8. Xero also notes onward sharing is increasingly a topic of interest for UK regulators. As with the proposed CPD legislation, the UK system envisages there are clear consumer benefits to allowing third party access to their data.

4. Responses to discussion document questions

4.1. **Question 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?**

4.2. Xero notes that industry participants will need clarity about how the Bill will interact with the Privacy Act. Whilst much may remain to be determined by regulations and standards, the current draft Bill goes beyond the requirements of New Zealand's existing Privacy Act in many areas, including requirements relating to consent, secondary data use, data deletion and accreditation. This will create complexity, particularly given one dataset may well contain data types that include both personal and non-personal data.

4.3. With regard to the deletion of data, Xero would like to ensure the Bill avoids a situation where two different statutory data deletion processes are required to run in parallel, that is, one under the Privacy Act, and one under draft CPD Act. Xero recommends consistency in approach, including, for example, statutory timelines and grounds for refusal.

4.4. We also note that the two regimes have potential to create different rules for us for personal data and non-personal data. New Zealand's existing Privacy Act, in contrast to privacy legislation overseas such as the EU's General Data Protection Regulation (GDPR), is not generally express or explicit consent-based. Under the Privacy Act, some industry participants could arguably have broader rights to use data for a wider range of purposes than they would under a consent-driven CDR regime.

4.5. Xero notes that it does have some concerns regarding the multiple regulators managing enforcement. The legislation will have to be very clear, regarding carving out responsibilities to ensure that there is no overlap, for example, to reduce the potential risk that industry participants may need to engage

[2]https://www.finextra.com/newsarticle/42066/uk-small-businesses-embrace-open-banking#:~:text=Open%20banking%2Denabled%20products%20are,an%2011%25%20rate%20for%20consumers

with two regulators over the same issue (for example, the failure to delete data upon customer request) who have different timeframes, different expectations and different powers of enforcement. On the basis of the discussion document, it is Xero's understanding that the Privacy Commissioner oversees individual data privacy breaches and MBIE oversees non-individuals, that is, companies and trusts. The proposed CPD sets out that MBIE will separately monitor compliance and enforcement of obligations beyond those which would be covered in the Privacy Act to ensure the integrity of data exchange, that is, MBIE will enforce compliance of the CPD for data holders and recipients regardless if personal or company data is being shared.

4.6. Xero has some concerns regarding the Memorandum of Understanding (MOU) framework between MBIE and the Office of the Privacy Commission. We recognise that the proposed framework allows for agility and flexibility, however, it is often difficult for government entities to create, abide and enforce these agreements between government parties. Therefore, we propose that any MOU framework needs to ensure public transparency of the document on the respective government entities' websites and to ensure accountability be endorsed and signed by the respective portfolio Ministers.

4.7. Additionally, at Xero we are of the view that excluding the AU CDR rules around deletion is appropriate, particularly in scenarios when data is transformed, enhanced or derived into new data.

4.8. Question 2: Should there be a maximum duration for customer consent? What conditions should apply?

4.9. A right to data deletion is an important privacy feature for small businesses and individuals, but its intersection with other laws and obligations, including business record keeping, creates complexity in its implementation. At Xero we are of the view that a maximum duration for customer consent creates too much disruption and friction for customers that rely on continuous data flow to run their businesses, often leading to monetary loss. We note that for 'repeating payments' the monetary loss is potentially higher if a consent expires and payments are missed.

4.10. Additionally, a maximum duration period has the potential to undermine productivity as well as create a negative customer experience of deleting or de-identifying data required to fulfil statutory record keeping obligations absent an express instruction from a customer to do so. For example, if lapsed consents required data deletion (as under the Australian CDR) this would require industry participants to delete or de-identify all CPD and CPD derived data, meaning small businesses would lose hours of reconciliation and years of statutory business reports, exposing the business to significant risk of non-compliance.

4.11. At Xero we believe that a better solution for consumers is for data holders to provide an easily visible/findable online dashboard which shows customers which third parties have access to their data. This, coupled with a data holder issued reminder, should negate the need to re-consent. Data

holders sending reminders to their customers detailing their connected apps/recipients, not to reauthorise, but instead to advise them how to remove access is sufficient to ensure customer management of data sharing while mitigating the risk of the cost and inconvenience of reauthorising, or, worse, inadvertently failing to do so.

4.12. **Question 3: What settings for managing ongoing consent best align with data governance tikanga?**

4.13. Xero is of the view that managing ongoing consent should be consistent with the principles of the Treaty of Waitangi.

4.14. **Question 4: Do you agree with the proposed conditions for authorisation ending? If not, what would you change and why?**

4.15. As outlined in our response to Question 2, Xero is of the opinion that there should not be proposed mandatory time periods for authorisation. We believe that the data holder should provide consumers with an easily visible/findable online dashboard which shows which 3rd parties have access to their data. This, coupled with a data holder issued reminder to consumers, should negate the need to re-consent and negate the needs for maximum periods of time in the CPD legislation. We are of the view that the accreditation framework for recipients, the Privacy Act and MBIE regulations should provide sufficient safeguards for consumers/customers.

4.16. **Question 5: How well do the proposed requirements in the draft law and regulations align with data governance tikanga relating to control, consent and accountability?**

4.17. As outlined in our response to Question 3, Xero is of the view that proposed requirements in the draft law should be consistent with the principles of the Treaty of Waitangi.

4.18. **Question 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?**

4.19. From Xero's perspective, it is important that the primary CPD principles are legislated (as opposed to regulated) to ensure that they are enduring. This is important to ensure the obligations of the recipient and data holder are clear when the secondary legislation is designed. Our view is that, in its current form, the draft law does not impose sufficient obligations on the data holder to disclose information so

that the customer is 'expressly informed' to enable their decision to 'authorise' the data holder to share their data with an accredited recipient. As a consequence, Xero would like greater clarity regarding the proposed consent procedures, such as the specificity of consents. We recommend that the focus is on the outcome for the consumer/customer, that is, so that they understand what data is being shared and used for.

4.20. Xero would also recommend that secondary uses of data are permitted in line with privacy protections, that is, that they are fair and reasonable, would be anticipated by the individual, rather than being restricted to prescriptive consent requirements. There may be important security or public interest justifications for allowing industry participants to use data for additional purposes, such as fraud prevention. Limiting uses to only those explicitly authorised may create gaps or lead to limitations for industry participants in applying or offering best-practice security controls.

4.21. Xero is of the view that the proposed obligation of the data holder to seek 'confirmation' of the data recipient authorisation does not ensure the data holder provides enough disclosure to their customers to ensure they are well informed of their decision to share data, their own T&C's/privacy policies, and how they can revoke access via their own systems in need.

4.22. We would recommend that MBIE revisit the fundamental structure of consent and authorisation in the draft legislation so that customers are better informed of how their data will be shared, and both data holder and recipient are responsible for ensuring customers are well informed. This will also afford data holders and recipients with more protection against liability for customer disputes regarding unconsented data sharing. This process is well documented and accepted by the banking/payments industry in the PaymentsNZ CX guidelines. Also accessible here via the API Centre.

4.23. Xero is also of the view that the primary method for authorisation should be standardised in terms of the information provided – albeit not prescriptive in how it should be presented.

4.24. From a Xero technical perspective, best industry practice requires adherence to OAuth2 standards, whereby the data holder implements/owns the authorisation protocols, that is, the data holder enables the data sharing and not the recipient. So from a technical perspective, a proposed move to place the burden of authorisation on the data recipient would go against generally accepted industry standards and create additional complexity to engineer a solution.

4.25. Further, regarding section 33 of the Bill, the primary legislation should ensure that the data holder has systems/technical standards in place to ensure that the data recipient is accredited as part of their authorisation process.

4.26. We note section 26 of the Bill which limits the Act to only apply to data shared via an electronic system. We would strongly encourage MBIE to ensure the CPD only incorporates the sharing of data via internationally accepted methods of data transfer via secure API protocols. It should not cover non-digital requests for data sharing as this is largely covered by the Privacy Act. Our key concerns are

the inability to capture and audit the consent and authorisation obligations under the CPD and confirm its been provided in accordance with primary and secondary legislation.

4.27. Regarding joint accounts, the proposed CPD states that both data holders and data recipients should have systems in place to deal with joint/multiple party authorisation. Applying our Xero recommendations above in relation to authorisation, only data holders should have an obligation to manage single or joint authorisation or revocation of data sharing. From a data recipient's point of view, only the customer or joint customer who has authorised access to their data should be permitted to change, add or revoke access to their data within the user roles of the data recipient's service. We note, from the Australian CDR regime, that joint accounts have been problematic regarding authorisation (as under the CDR regime, the data holder requests the joint account holders to nominate only one party which means the other account holders are unable to manage the data). We do not believe this model attribute should be replicated in the CPD.

4.28. With regards to notification of consent, Xero would recommend that notification of consent or revocation of consent is provided either in the digital user journey at the time of consent or revocation, or via an easily accessible connection dashboard at both the data holder and data recipient digital customer interface. We do not recommend either party should send email confirmation of consent or revocation as this will lead to consent fatigue and customer friction.

4.29. **Question 7: Do you think the procedural requirements for making standards are appropriate? What else should be considered?**

4.30. Xero is of the view that the security standards and reference to an appropriate universal benchmark should be outlined in the primary legislation. There may be standards that should apply to all designated sectors and incorporated upfront into the primary legislation to avoid disparate standards across different industries.

4.31. With regards to the definition or scope of standards for secondary legislation, Xero is of the view that these should incorporate technical API standards for data exchange, but also customer and operational standards that should be met.

4.32. A critical consideration from a governance perspective is how standards are established and managed. Section 84 of the Bill implies that the MBIE's Chief Executive could outsource or delegate these responsibilities to an industry body. We are of the view that MBIE should adopt an industry consultation framework and with that enable the development of technical standards (which could be led by an industry body).

4.33. However, with regards to administration and governance activities (such as accreditation, decision making on standards, regulation setting and enforcement), Xero strongly advocates that these

activities should be overseen and governed by an independent government controlled entity in order to mitigate any potential conflicts of interest.

4.34. To this end, the regulatory framework should be robust enough to ensure compliance with the legislation and avoid the shortcomings of self regulation or the data holder industry predetermining the standards required for data sharing. Therefore, we would encourage MBIE to recruit the appropriately qualified personnel to design and implement the secondary legislation with high levels of industry consultation and balanced recognition of both data holder and data recipient feedback.

4.35. **Question 8: Do you think the draft law is clear enough about how its storage and security requirements interact with the Privacy Act?**

4.36. NZ has an opportunity to establish some minimum security requirements that are interoperable across all aspects of the data economy. The proposed CPD could capture multiple participants under this legislation and potentially other data sharing arrangements, for example, the IRD and other government departments and vendors. As a consequence, Xero is of the view that the primary CPD legislation should go further to establish minimum information security standards as part of its accreditation framework and these should be established by a lead agency, such as MBIE, and referenced in the legislation.

4.37. We note that security standards are often a major barrier to entry either by virtue of the standards being set too high, or variable across each data holder, thus inhibiting market coverage to enable successful third party services. Xero recommends that minimum security standards are incorporated into the primary legislation and are unambiguous to reduce the risk of third parties being rejected by data holders or not meeting accreditation.

4.38. The secondary legislation or sector designation rules may require additional security requirements but Xero recommends that these should only apply to 'write' transactions. For data holders, their regulatory obligations may require additional security standards.

4.39. Xero also recommends that organisations that already have met a high threshold of security accreditation such as ISO27001 and SOC2 accreditation should be fast tracked through the accreditation process given their proven capability and investment into information security.

4.40. **Question 9: From the perspective of other data holding sectors: which elements of the Payments NZ API Centre Standards are suitable for use in other sectors, and which could require significant modification?**

4.41. From Xero's perspective the API Centre technical standards are a good foundational step towards data sharing for other sectors, however, there are some shortcomings in their standards due to a range of factors and the complexity as well as cost in remediating their existing system architecture. Therefore,

while a good foundation, Xero recommends that the standards be reviewed from a broad perspective with 'fresh eyes' on future requirements across multiple sectors (with potential additions such as: a universal standard for single or multi person authorisation on data sharing and a standard for two way notifications).

4.42. **Question 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?**

4.43. From a high level perspective, if the technical, financial, certification or capital barriers are too high, Xero is concerned that new participants in the sector will be limited to global technology players, overseas institutions and digital service providers with significant financial backing from established financial institutions.

4.44. It is widely acknowledged that NZ banks' security standards and third party onboarding requirements are high barriers to entry, and often designed to be a high barrier to entry, and potentially disproportionate to the risks involved in a customer sharing their data with a third party. The same standards that apply to a software vendor providing services to a bank will often apply to a data recipient providing a service to a mutual customer, which is badly aligned given the data recipient is not providing their service to the bank, but to their mutual customer, and the bank's involvement is just limited to enabling the sharing of their mutual customers' data.

4.45. The issue of liability is very significant and in large part why bank security standards and third party onboarding requirements have been set so high under traditional vendor arrangements. However, under the CPD law, there should be no liability to the bank if they administer their obligations for informed consent appropriately and manage their proposed obligations for information security and accreditation appropriately (noting that banks/data holders do not have any obligations in the current draft law for information security or accreditation).

4.46. It is Xero's view that the liability for misuse of data once shared correctly with a data recipient, should lie with the data recipient. As it stands the draft CPD law is silent on liability.

4.47. **Question 11: Should there be a class of accreditation for intermediaries? If so, what conditions should apply?**

4.48. Xero's view is that in this respect the work of the API Centre is well grounded. If the intermediary is not providing services directly to the customer, and is only providing a data transfer service, the intermediary should be subject to the same accreditation rules as data recipients.

4.49. If an intermediary is providing a service to a third party to receive data, the intermediary should be liable for the actions of the third party in complying with the legislation. The third party would not be

subject to the proposed CPD legislation but would be bound by the Privacy Act and any contractual arrangements in place with an accredited intermediary.

4.50. **Question 12: Should accredited requestors have to hold insurance? If so, what kind of insurance should an accredited requestor have to hold?**

4.51. Xero is of the view that there should be no additional insurance requirements on accredited requestors (as there are no current insurance requirements for any holders or users of data).

4.52. **Question 13: What accreditation criteria are most important to support the participation of Māori in the regime?**

4.53. Xero has no comment on this question.

4.54. **Question 14: Do you have any other feedback on accreditation or other requirements on accredited requestors?**

4.55. Xero's view is that accreditation should remove any ambiguity or barriers to entry for a data recipient to develop their own innovative services to serve customers. It should focus on the scope of their services to their customers, and whether they provide services directly to their customers, or whether they are a data intermediary or intermediary/technical service provider.

4.56. **Question 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.**

4.57. Xero has no comment on this question.

4.58. **Question 16: What are specific use cases which should be designed for, or encouraged for, business (including small businesses)?**

4.59. Open data systems lie at the heart of the digitisation of our economy which, in turn, can drive productivity gains especially for our small businesses. From an overarching perspective, Xero's hope is that the proposed CPD legislation will be able to apply in a holistic manner across businesses enabling interoperability of data across multiple sectors in the New Zealand economy fuelling productivity growth.

4.60. As stated up front in our Submission, in Section 3: *Lessons from other jurisdictions,* Xero is mindful of Australia's experience with the negative consequences for small business of the inclusion of 'derived data' in the legislation, which had the adverse result of downstream data transfers of data derived from having CDR rules and protections applied as well as the issue of rules stipulating the deletion of all CDR data upon a lapsed consent that drive high compliance and administration costs. We note that the proposed 'Business Consumer Disclosure Consent' rule in Australia is a workaround required for the 'derived data' and 'data deletion' rules issues.

4.61. However, this is in contrast to the Open Banking experience in the UK. There, Open Banking is viewed as a secure tool that helps small businesses manage their finances more effectively – and become more resilient, productive and profitable. This is enabled by giving businesses access to up-to-date financial data at any time to enable them to understand and manage their money more effectively – including forecasting, applying for credit, or speeding up payments. Therefore, from Xero's perspective the proposed CPD legislation, appropriately constructed and implemented, has the potential to drive a number of key benefits for small businesses such as driving innovation and productivity output.

4.62. **Question 17: What settings in the draft law or regulations should be included to support accessibility and inclusion?**

4.63. Xero has no comment on this question.

4.64. **Question 18: In what ways could regulated entities and other data-driven product and service providers be supported to be accessible and inclusive?**

4.65. Xero has no comment on this question.

External(np)
Please reconsider printing me unless absolutely necessary the environment will thank you

4.66. **Question 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?**

4.67. In our experience, what constitutes ethical data use can be informed by the nature of the relationship between the individual and organisation; as opposed to embedding ethics in a regulatory framework. For instance, Xero has developed its own *Responsible Data Use Commitments* (as outlined in Section 1 of this Submission) which are tailored to the type of products and services that we provide.

4.68. Xero does not think that express consent should be required to de-identify data as this should be deemed a fair and reasonable secondary use.

4.69. **Question 20: Are there other ways that ethical use of data and action initiation could be guided or required?**

4.70. None other than Xero's Responsible Data Use policy that already has been identified in the prior question.

4.71. **Question 21: What is your feedback on the purpose statement?**

4.72. Overall, Xero supports the tenor of the purpose statement, however, we think it is very important for the draft CPD bill to define 'data' in the primary legislation. The core issue is that once a customer authorises their data is shared from a data holder to a data recipient, the data recipient will enable their customer to view, modify or transform their data within the parameters of the data recipients systems. Further, the data recipient (who may or may not be an accredited data holder) may enable their customers to share their data with a fourth party.

4.73. The legislation should be clear that any designation of data reflects the data that is held by a data holder. The instant it is shared with a data recipient, it no longer becomes a designated data set because of the ability of the customer or the data recipient to modify, transform, or enhance the data without any limitation from the original data holder. That is, the customer controls how their data is used by the data recipient via the consent model and terms and conditions of the data recipient, and any subsequent sharing of data will be undertaken with customer consent using either accepted industry practices or legislative requirements that may apply.

4.74. Xero is also of the view that the primary and secondary legislation should not include any reference to derived data, or impose any restrictions on a data recipient from enabling their customers to share their data with a fourth party unless the data recipients are themselves a designated sector/data holder.

4.75. Furthermore, the datasets that are designated under the secondary legislation for all sectors should reflect the transactional metadata that is created through electronic transactional records. The data

sets should not apply to data sets where human or electronic intervention has transformed a transactional record into an enhanced data point. From Xero's point of view, this act of transformation occurs when a bank statement transaction is imported into a customer's individual subscription. The customer (or their advisors who are invited into the subscription as secondary users) is able to modify this transaction without intervention from Xero. Nonetheless, regardless of whether the customer modifies the data that was originally received from the data holder, the fact that it has been transformed into data available via the Xero user interface would dictate that it is in fact now derived or enhanced data and should be excluded from the draft CPD bill and secondary legislation.

4.76. To take this example one step further, if the customer uses the data received from the data holder to create an accounting record via their Xero subscription, this new accounting data record is unique and transformed by either human or electronic intervention and should not be subject to any restrictions in the designated datasets for either banking or accounting software.

4.77. **Question 22: Do you agree with the territorial application? If not, what would you change and why?**

4.78. Xero notes that the proposed scope of the territorial application is aligned with the Privacy Act. However, we also note that the draft CPD Bill proposes the use of a 'carrying on business in New Zealand' threshold. In this regard, we understand that there is some need for caution in this application as Carrying on Business in New Zealand: an Uncertain Frontier in a Digital Age (NZBLQ Vol 27 Dec 2022 1, Kavanagh and Yang), has indicated that the test is problematic.

4.79. **Question 23: Do you think it is appropriate that the draft law does not allow a data holder to decline a valid request?**

4.80. From Xero's perspective, if a data recipient has met the accreditation requirements and has met the authorisation and consent requirements, a data holder should not be allowed to decline a valid request. Additionally, the data holder should ensure they provide enough disclosure to ensure their customers are making an informed authorisation/confirmation.

4.81. **Question 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?**

4.82. Xero has no comment on this question.

4.83. **Question 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?**

4.84. We would refer to our response in Question 21 which details how data is shared and intrinsically transformed at the instant is received by a data recipient. It is no longer the original data that was held by the data holder, but is now new data held by the data recipient and depending on the terms and conditions of the data recipient, can be modified or shared by the customer according to their instructions.

4.85. It is technically unfeasible to 'ringfence' data once imported from the data holder in its original format and populated in the data recipients customer interface. A customer should not be limited in their ability to modify or transform that data, nor share their data with other parties. Likewise, it is technically unfeasible for a data recipient to establish controls which would enable record keeping for modified data that is shared with fourth parties.

4.86. However, as part of an accreditation framework, a data recipient and data holder should be expected to maintain electronic records or API logs to meet clause 40 and 41 (1). In the case of 41 (b), this should only be expected if they were an accredited data holder, in which case clause 40 would apply and negate the need for 41 (b).

4.87. It is worth considering the role of intermediaries in this context. Please refer to Xero's position in Question 11.

4.88. **Question 26: What are your views on the potential data policy requirements? Is there anything you would add or remove?**

4.89. Xero agrees with the proposed standards for data governance and supports this requirement.

4.90. **Question 27: Are there any additional information gathering powers that MBIE will require to investigate and prosecute a breach?**

4.91. Xero has outlined responses in Question 1 on potential investigation/enforcement issues.

4.92. **Question 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?**

4.93. Xero believes that the draft legislation proposes an appropriately 'high bar' to those person/persons designated as data holders, in particular, the requirement for a Regulatory Impact Assessment given the significant investment required by data holders to comply with the draft law.

4.94. **Question 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?**

4.95. Xero has no comment on this question.

4.96. **Question 30: What should the closed register for data holders and accredited requestors contain to be of most use to participants?**

4.97. Our view is that the closed register should include up to date key contacts for all data holders and accredited requestors, as well as access to the technical details required to initiate a connection with those participants.

4.98. **Question 31: Which additional information in the closed register should be machine-readable?**

4.99. Xero's view is that if the register includes technical information required to onboard with participants these should all be easy to access in machine readable format.

4.100. **Question 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?**

4.101. Xero is of the view that this is an appropriate timeframe for reporting (the proposed four months post 30 June for yearly reporting).

4.102. **Question 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?**

4.103. Our view is that in the interests of competition and customer experience there should be real-time reporting that is transparent and publicly available. However, the real time reporting should be strictly limited and not onerous (given the reporting requirements associated with Question 32's annual reporting). We propose that real-time reporting is limited to complaints and API performance.

4.104. Additionally, the draft CPD Bill should also ensure enforcement penalties are in place for data holders who do not meet implementation deadlines, or quality assurance measures to ensure data recipients and their customers can rely on the data being shared by the data holder in a timely and accurate manner. If a data recipient invests in building their technical architecture and accreditation

External(np)
Please reconsider printing me unless absolutely necessary the environment will thank you

requirements under the proposed Bill, and a data holder is not able to provide the data recipient with a reliable service, the financial impact will be significant to the data recipient and should be reflected in the severity of enforcement penalties.

4.105. **Question 34: What is your feedback on the proposal to cap customer redress which could be made available under the regulations, in case of breach?**

4.106. Xero has already noted its concerns in our response to Question 1 regarding multiple regulators with differing enforcement powers and capabilities. A cap on customer redress adds another layer of complexity to the enforcement regime.

4.107. **Question 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?**

4.108. Xero notes that there is no specific dispute recognition scheme approach under the Privacy Act, instead the Privacy Commissioner has a broad range of options to seek to informally or formally settle disputes.

4.109. Therefore, Xero is interested in understanding the rationale behind the proposal regarding designation rules which would require participants to join a dispute resolution scheme and that non-privacy complaints would be dealt with by these schemes. How would MBIE deal with these complaints/infringements from an enforcement point of view? And would these enforcement rules deal with direct financial loss (we note the Banking Ombudsman only deals with claims of up to $350k)?

4.110. Xero would like to understand how the Privacy Act would govern in a scenario where ‘write’ or ‘action initiation/payment initiation’ results in customer loss.

4.111. Xero also has questions around what non-privacy issues would require cover for indirect losses not covered by other legislation? Xero notes that, as per the Discussion Document, it appears the business or individual would need to pursue damages via court action rather than a disputes tribunal to seek redress for their own damages - is this intentional? We note that this seems a high cost burden for small businesses to seek redress.

External(np)
Please reconsider printing me unless absolutely necessary the environment will thank you