MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT
HIKINA WHAKATUTUKI

Discussion document

Unlocking value from our customer data

A draft law to set standards and safeguards for customer and product data exchange

June 2023

newzealand.govt.nz

Permission to reproduce

Important notice

The opinions contained in this document are those of the Ministry of Business, Innovation and Employment and do not reflect official Government policy. Readers are advised to seek specific legal advice from a qualified professional person before undertaking any action in reliance on the contents of this publication. The contents of this discussion paper must not be construed as legal advice. The Ministry does not accept any responsibility or liability whatsoever whether in contract, tort, equity or otherwise for any action taken as a result of reading, or reliance placed on the Ministry because of having read, any part, or all, of the information in this discussion paper or for any error, inadequacy, deficiency, flaw in or omission from the discussion paper.

ISBN 978-1-991092-32-8 (online)

Contents

Minister's Foreword

The ability for New Zealanders to allow the use of their data to enable real-time information on products and pricing has the potential to make us all better off – and your views about how we achieve this are important.

This legislation provides a framework in which customers are given the power to require entities (like banks) to share information. This will unlock the ability for customers to compare products in real time, manage accounts across different providers simultaneously, and switch between providers seamlessly. Providing this power to customers is at the heart of the Customer and Product Data Bill (the **draft law**) which brings in a consumer data right for Aotearoa New Zealand (**CDR**).

It is truly exciting to imagine the possibilities that will emerge. The draft law will enable innovators in our economy to develop new products and services and increase competition, which, in turn will benefit customers by leading to reduced prices and improved product offerings.

The Aotearoa / New Zealand landscape is unique. This proposal builds on international experience and adapts it for our unique communities and aspirations. This is a new law for everyone and can create opportunity and improve inclusiveness. Together, this will help us grow a productive, high wage and low emission economy.

Critical to any data sharing is trust. At the heart of this new law is the setting of standards so that customers can be sure that their data is safe, and the parties who are accessing it are accredited as trustworthy, competent, and secure. This is a vast improvement on existing approaches to data sharing, which can pose risks to customers and which may need revisiting.

I congratulate those businesses which have already made great strides to allow customers to use and share their own data in innovative ways and encourage them to continue. Government has an important part to play in facilitating and accelerating the creation of a workable and consistent platform for the sharing of data – but this is work that must be completed in close collaboration with industry participants, consumer and iwi representatives and technical specialists.

The banking sector will be the first cab off the rank for standardised data exchange. In the future we will be looking for areas where the greatest gains can be made for everyday New Zealanders. These may include the energy, finance, insurance, and health sectors.

Our Government is committed to ensuring that customers are informed, empowered, and protected in their interactions with businesses. The release of this draft law represents a key milestone in New Zealand's journey to a safe and prosperous digital future.

To make sure the regulatory settings do this well, it is important we hear the valuable perspectives on this draft law from all interested parties. I look forward to hearing your views on this essential digital infrastructure for the future.

As the Minister of Commerce and Consumer Affairs, I am pleased to present this draft Customer and Product Data Bill for public consultation.

Hon Dr Duncan Webb
Minister of Commerce and Consumer Affairs

Executive Summary: Unlocking value from our customer data

When businesses like banks, power companies and mobile phone companies provide us with services, data is created – for example, account histories, transactions or usage. This is 'customer data'. It is held by businesses and is protected by business security measures, as well as the Privacy Act 2020 in the case of personal information.

Customer data holds enormous value and opportunity, but only if customers are able to make full use of it and connect it with digital applications, or with collectives they trust. For example, electricity usage information can help people find the cheapest power company and plan, or reduce their carbon emissions. Bank records can provide insights into household expenses or streamline the process of applying for a loan.

People can already ask for their data to be provided to their accountants, banks or others – but there are problems. Businesses don't have the same rights as individuals to access their data, and the way it is accessed can be inefficient and insecure.

The draft Customer and Product Data Bill (the **draft law**) unlocks the value of data for people and their businesses by:

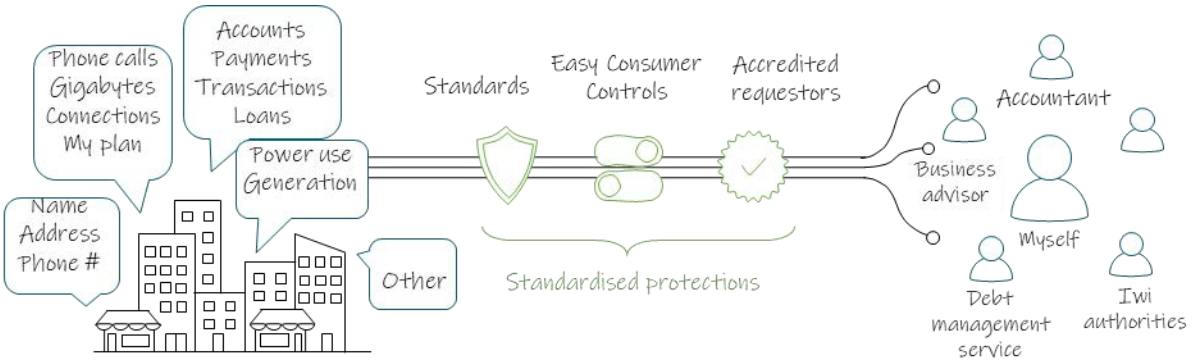
- improving customers access and control of their own data
- standardising how data is exchanged
- ensuring those who request access to data are accredited as trustworthy.

The draft law will also require businesses to make information about their products available in ways that can be automatically processed by a computer. This will make it easier to compare and switch.

The aim is to help innovators in our economy create new products and services and increase competition. This in turn will benefit customers by leading to reduced prices, improved product offerings, and greater productivity. There are also opportunities to support by-Māori, for-Māori data initiatives, business-to-business applications, and improved accessibility and inclusion.

The rules will apply to banking first. Other sectors will be included in future.

Currently, it is generally difficult for consumers to access or exchange data held about them. The draft law will complement existing Privacy Act protections and data security measures.



We want your feedback on how this new system should work. Below are the key issues that we would like to hear from submitters on, but feedback is welcome on all aspects of the system.

Respect
for customer authority

What should the requirements be to ensure that consent to data exchange is express and informed?

How might tikanga values make these rules stronger?

Care
of data during exchange

How do we decide which customer and product data to bring into the system?

What should the process be for setting the more detailed rules about data exchange?

How do we build on industry work to date, while making sure the standards work for diverse data holders and customers?

Trust
of those who access our data

Who can be accredited to connect to data holders?

The Future
We want to hear:

How unlocking product and customer data could help meet the aspirations of people, iwi, businesses and others?

What concerns you might have about the ways data is (or could be) used?

Introduction

1. When businesses provide us with goods and services, data is created. For example, banks, power companies and mobile phone companies hold our account histories, transaction data and product usage information. This is 'customer data'.

2. Customer data holds enormous value and opportunity for individuals, businesses, iwi and hapū, and our broader economy and society. By enabling customers to access and exchange their data with other businesses of their choice, it can be used to enhance overall customer experiences and meet individual, business and social needs.

3. For example, new and innovative services can use customer data and digital connections to:

    - make it easier for customers – including small businesses – to shop for services, such as banking, electricity, and telecommunications. For example, electricity usage information can help people to find the cheapest power company and plan. Bank records allow customers to compare financial products and services using personalised data, and then streamline the process for applying

    - offer tailored advice and insights or product recommendations, which could boost productivity and efficiency for businesses and save individuals time and effort

    - action customer decisions, like opening new accounts or switching providers.

4. We are seeking feedback on the draft law which aims to make this potential a reality. It does this by giving customers more access to and control over their data, standardising methods of exchanging that data, and accrediting those who are trusted to request or edit customer data.

5. Customer consent and control over access will remain central. The draft law strengthens Privacy Act protections and extends some of the protections to all designated customer data.

6. If the customer consents, the draft law will require businesses that hold designated customer data (data holders) to provide that data to accredited requestors, subject to privacy and security safeguards. The draft law will also require product data to be made available electronically on request. It will require businesses to perform actions in response to electronic requests, such as opening accounts or changing customer plans.

7. The draft law will support innovators in our economy to create new products and services and increase competition. This in turn will benefit customers by leading to reduced prices, improved product offerings, and greater productivity. The draft law also creates

opportunity to support by-Māori, for-Māori data initiatives, business-to-business applications, and improved accessibility and inclusion.

8. Once the draft law is passed, specific data can be brought under the new law one sector at a time. Banking data will be brought in first.[1]

9. The Ministry of Business, Innovation and Employment (**MBIE**) is seeking feedback on how the overall system should work (Chapter One). We also want feedback on the draft law itself (Chapter Two). We ask questions throughout the document and page 61 sets out how to make a submission. Your feedback will inform the design of the draft law as well as future regulations, and the standard setting processes.

How is customer data and product data currently exchanged and used?

10. There are already innovative products and services that use customer data to benefit customers by helping them manage their finances, compare product offerings, or more easily switch from one provider to another. However, the way that customer data is accessed at present has problems.

11. In the banking sector, customers currently use their bank data and make payments in a variety of ways which can be insecure and inefficient. For example, when people want to provide their bank transaction records to another business (eg a lender or financial adviser), they can:

    - Download statements of their transactions (eg PDF or CSV spreadsheets) and e-mail or upload them. These require customers and often receivers to undertake many manual steps. The resulting information may not be in a standard format and can be tampered with. It is only provided at a point in time and quickly falls out of date.

    - Enable 'screen scraping' by sharing their online banking credentials (eg login and password) with the receiver. Providing login details to a third party generally is a breach of a customer's banking terms and conditions and is also a significant privacy and security risk. The receiver uses special software to capture transactions from an internet banking website or mobile banking system and convert them to a format which can be absorbed into their own software system.

    - Ask the bank to send the transaction details securely, in a standard format that integrates directly with the receiver's software (ie using an Application Programming Interface[2] or **API**). Financial technology (**fintech**) businesses offer products and services

[1] In due course, there will be a dedicated engagement process to explore what data, and which data holders in the banking sector should be designated.
[2] A good explanation of an Application Programming Interface is in this video: ***https://www.youtube.com/watch?v=s7wmiS2mSXY***.

that support a lender or adviser receiving details in this manner. However, this requires fintechs get agreements with each individual. It also requires the bank to have invested in their data systems.[3] Only limited numbers of customers currently have access to this option.

12. A number of sectors have been developing standards for safe and efficient data exchange, and the Privacy Act already protects personal information.[4] However, progress within individual sectors has been relatively slow and has not delivered the full range of potential benefits available for customers. The current regulatory settings, or lack thereof in some cases, is holding back electronic access to customer data and product data in standardised and secure formats.

What will the draft law improve?

13. The draft law seeks to make direct, secure and standardised transfer of customer and product data from one organisation to another available to all customers. The draft law seeks to standardise privacy protections for data exchanged using the draft law, make these standards enforceable, as well as provide a pathway for redress if things go wrong. The aim is to build upon existing innovation while also accelerating standard, secure, efficient ways for customers to:

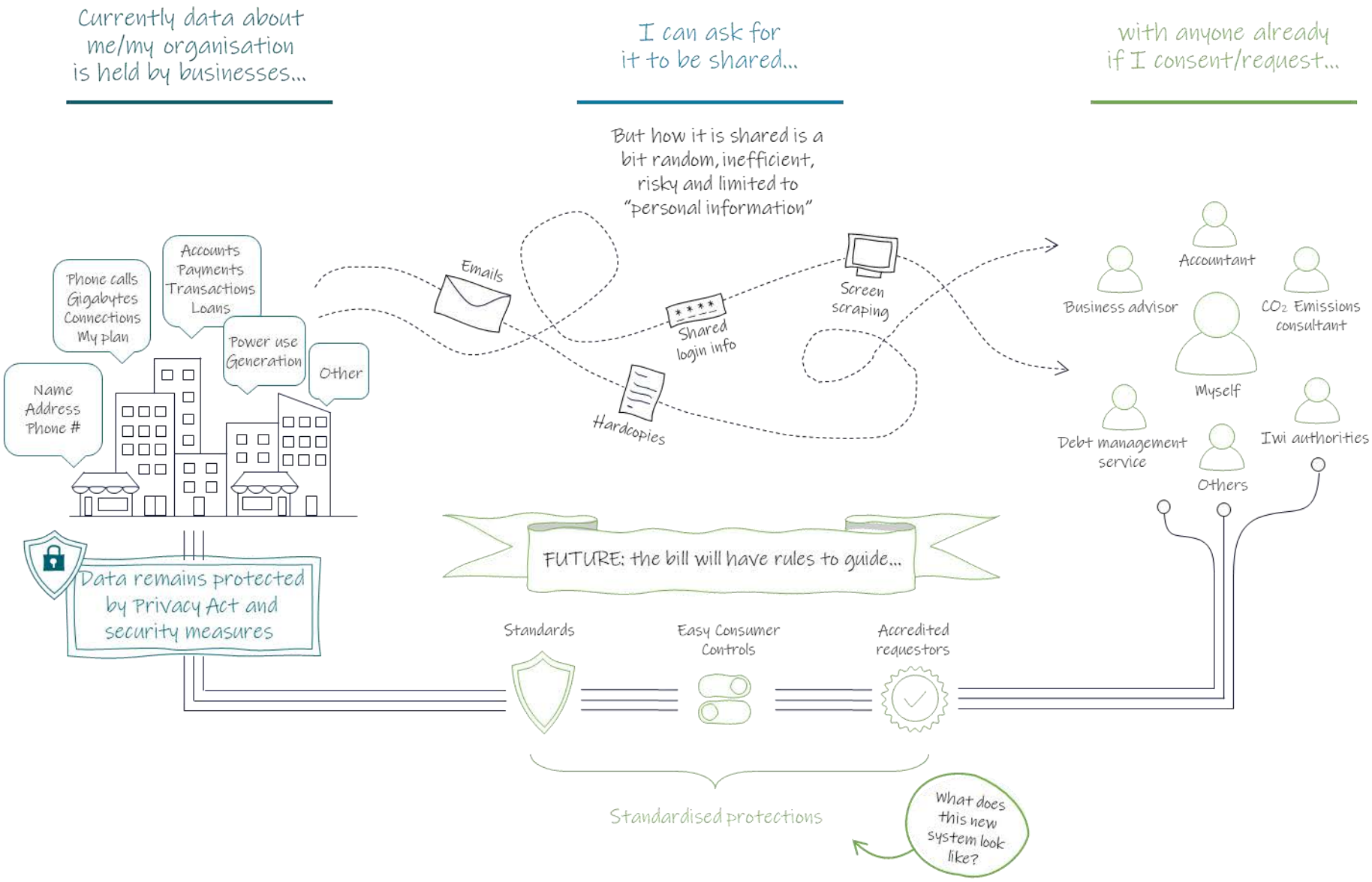
- access their own customer data
- transfer their customer data to other businesses of their choice – for example when switching providers, seeking advice or add-on services
- monitor or update their consent settings for who can access their data
- access product data in a format which can be automatically read and processed by a computer
- direct businesses to take actions like opening accounts or making payments
- access redress and be confident that the system participants are subject to monitoring and enforcement for breaches of the law.

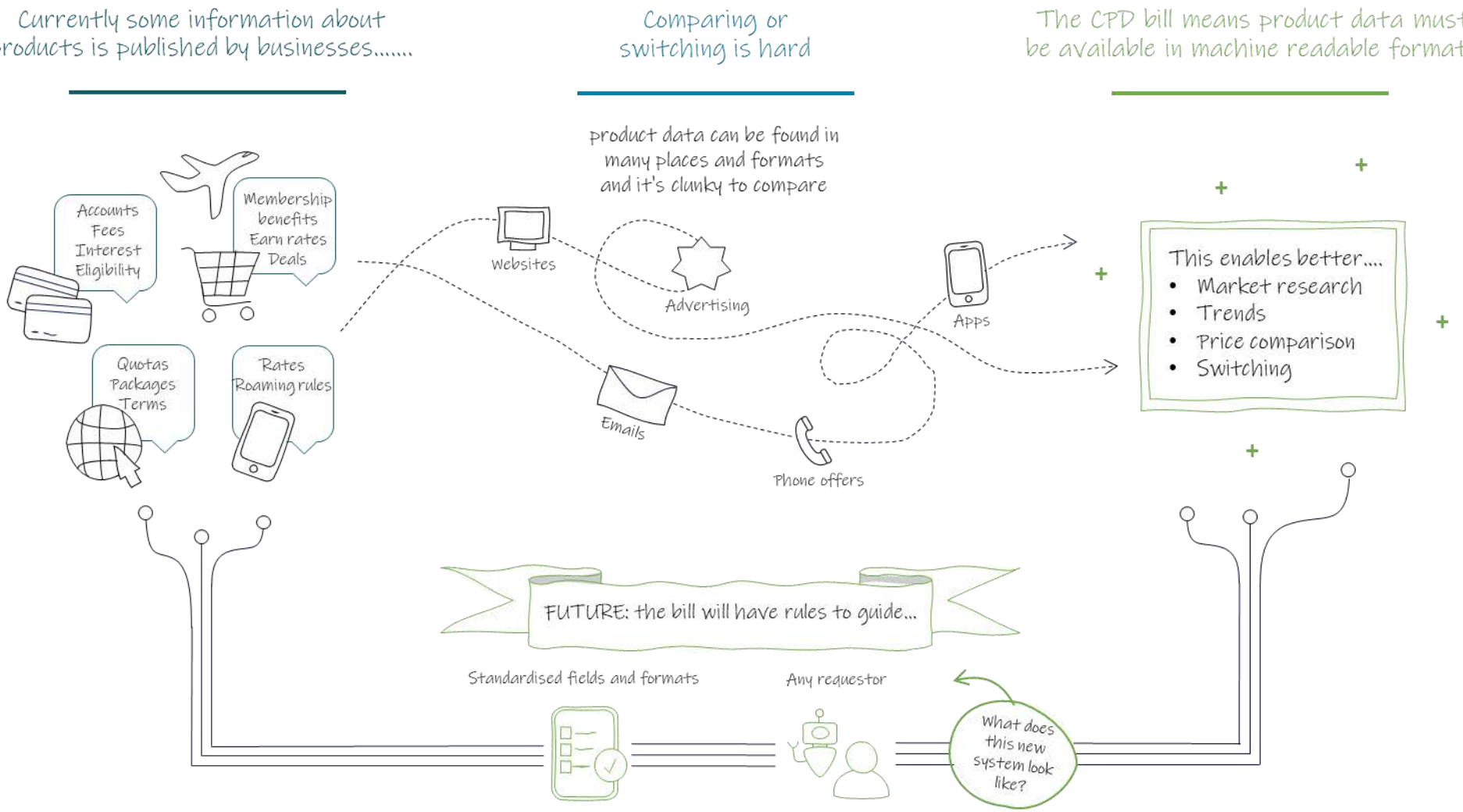
[3] ANZ, ASB, BNZ and Westpac have agreed to implement Payments NZ API Centre's open banking standards over the next 18 months, including the account information API standard. See more at ***https://www.apicentre.paymentsnz.co.nz/news/articles/open-banking-implementation-timeline-set-for-largest-banks/***.

[4] The Privacy Act protects personal information by requiring secure handling and storage of personal information, and protecting the collection, retention, use, accuracy and disclosure of our personal information. It ensures individuals can access and seek correction of their own personal information, as well as allows representatives to seek access and correction to the individual's personal information.

Visual summaries

14. Summaries of the current and proposed future exchange of customer and product data are set out on the following pages.


Currently data about me/my organisation is held by businesses...
I can ask for it to be shared...
with anyone already if I consent/request...
But how it is shared is a bit random, inefficient, risky and limited to "personal information"
Phone calls
Gigabytes
Connections
My plan
Accounts
Payments
Transactions
Loans
Power use
Generation
Other
Name
Address
Phone #
Emails
Shared login info
Hardcopies
Screen scraping
Accountant
Business advisor
CO2 Emissions consultant
Myself
Debt management service
Iwi authorities
Others
Data remains protected by Privacy Act and security measures
FUTURE: the bill will have rules to guide...
Standards
Easy Consumer Controls
Accredited requestors
Standardised protections
What does this new system look like?


Currently some information about products is published by businesses.....
Comparing or switching is hard
The CPD bill means product data must be available in machine readable formats
Accounts
Fees
Interest
Eligibility
Membership benefits
Earn rates
Deals
Quotas
Packages
Terms
Rates
Roaming rules
product data can be found in many places and formats and it's clunky to compare
Websites
Advertising
Apps
Emails
Phone offers
This enables better....
Market research
Trends
Price comparison
Switching
FUTURE: the bill will have rules to guide...
Standardised fields and formats
Any requestor
What does this new system look like?

Navigating this document

15. This discussion document is divided into two chapters. We are seeking feedback on how the overall system should work (Chapter 1) and on technical matters and system settings (Chapter 2). A range of detailed rules will be subject to further engagement and consultation in due course. At this stage, we want to know whether the draft law sets the right framework for the overall system.

Chapter 1: Overview and key issues

16. Chapter One provides a map of the proposed customer and product data framework. Submitters who would like to learn more about how the draft law will work more generally, including how it will fit with other laws and Te Tiriti of Waitangi/the Treaty of Waitangi (Te Tiriti/the Treaty), may wish to read this.

17. Submitters may wish to provide feedback on:

    - how the draft law respects and protects customers' authority over their data, enables standards to care for data during exchange, and the potential requirements for accreditation
    - how the design of the draft law can best enable by-Māori for-Māori uses of data, support business-specific needs, as well as ensure diverse customer needs and interests are met
    - whether and how ethical use protections could be incorporated in the draft law.

Chapter 2: Technical matters

18. Includes technical questions about the draft law. Submitters who are interested in having a say on technical components or the drafting of specific provisions may wish to read this section.

19. Chapter 2 also includes information on the proposed system settings of the draft law. Submitters who would like to have a say on the regulatory system design may wish to provide feedback on this section.

Chapter 1: Overview and key issues for the proposed customer and product data framework

20. This chapter provides a map of the proposed customer and product data framework and illustrates some key roles in the system. It also describes:

    - how the draft law will fit with other laws such as the Privacy Act, and with Te Tiriti/the Treaty
    - the proposed scope of the framework.

Map of the draft law

21. The draft law will become an Act of Parliament, containing key definitions protections and powers. It will eventually be accompanied by:

    - regulations containing detailed rules, including which data is designated into the system
    - standards, containing highly technical specifications.

22. In different parts of the discussion document we will be asking questions about the wording of the draft law, the content of the future regulations, and how technical standards should be set. Feedback on these will help get the 'ground rules' right in the draft law.

23. The draft law aims to improve the way that customer data is exchanged, but it will rely on existing laws and obligations relating to data and information, wherever possible.

24. The map on the next page shows the key elements, and the questions we have about each. This is followed by an illustration of the key roles in the system, and how they interact with each other.

Unlocking value for people and their organisations: standardising data exchange

DRAFT BILL:

Purpose & definitions - Part 1

Obligations on data holders - Part 2

Protections -Part 3
Consent, verifying identity, transparency, complaints

Regulatory powers and remedies - Part 4

Rules for
- Accreditation by MBIE
- Register, levy etc
- Regs & standards
- Designation - Part 5

Enforcement powers

Penalties for breaching

not included (will depend on main provisions)

Are these ground rules right?

REGULATIONS & STANDARDS:

Details of safeguards and rules

Rules for controls

Respect
The persons/orgs authority over their data = CONSENT

What should these look like?

Rules for technology

Care
For the data during exchange
STANDARD SECURITY & FORMATS

What should the process be?

Rules for access

Trust
Those who join in ACCREDITATION

How do we decide who?

Unlocking value for all

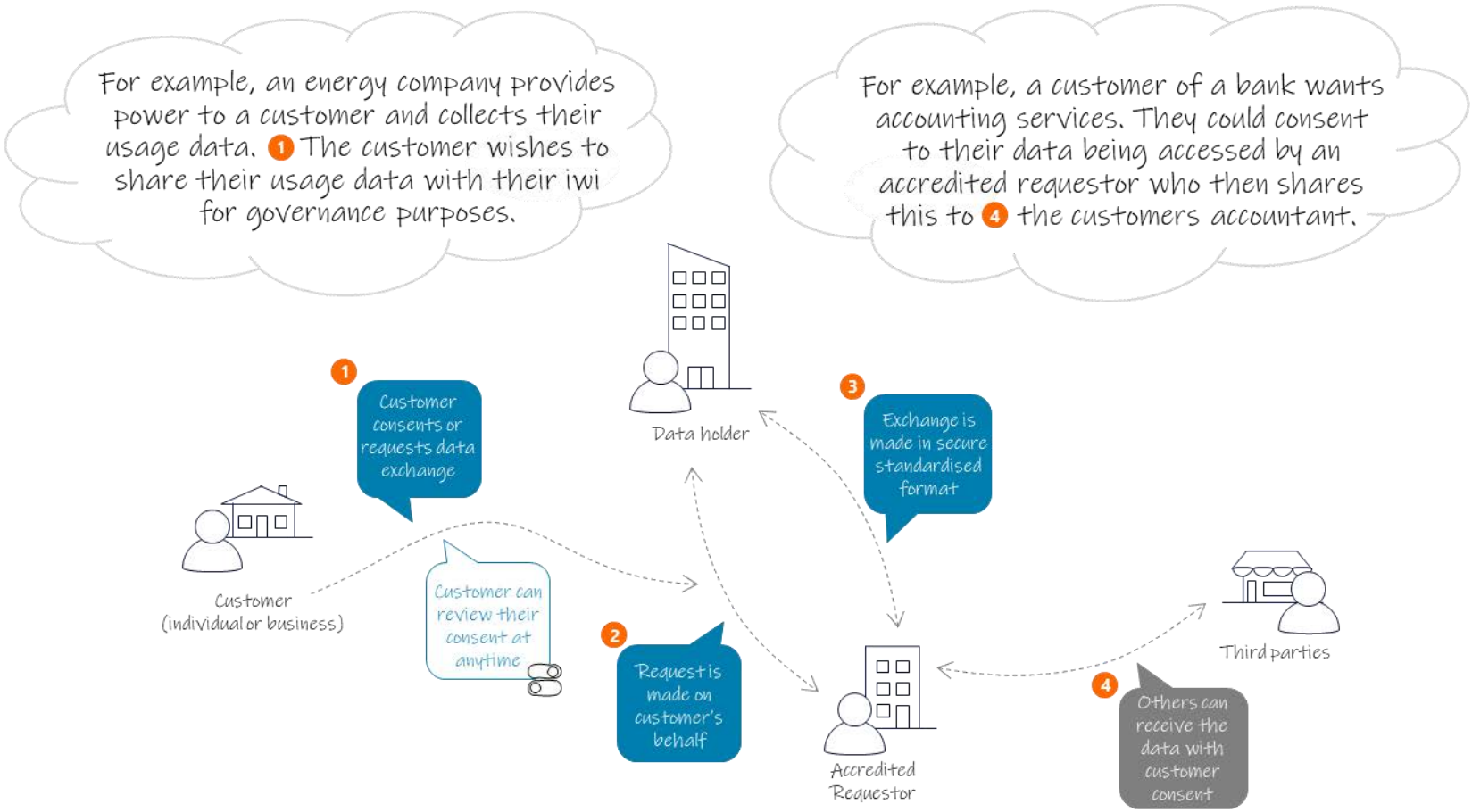
How might we guide ethical use?

DESIGNATION:

Deciding when, who and what is covered (Part 5)

Designated data must be exchanged on request & according to regulations & standards (Part 2)

Illustration of key roles



How will the draft law interact with protections under the Privacy Act?

25. The Privacy Act provides rights and obligations around 'personal information', which is information about an identifiable individual. It protects personal information by requiring secure handling and storage of personal information, and protecting the collection, retention, use, accuracy and disclosure of our personal information. It ensures individuals can access and seek correction of their own personal information, as well as allows representatives to seek access and correction to the individual's personal information.

26. The Privacy Act applies across the economy, including to any person, business or organisation. Therefore, the draft law relies on existing Privacy Act protections. These are not replicated in the draft law unless:

    - the draft law provides the same protection as a privacy principle but sets a more specific requirement for customer data, or

    - an equivalent Privacy Act protection is required in the draft law to ensure consistent treatment of all customer data (whether or not it is personal information). Consistent treatment is important to ensure simplicity, cost effectiveness, and to ensure sensitive commercial information also has protection.

27. The draft law covers all customer data, which includes data that relates to an identifiable customer (eg trusts, companies). The Privacy Act protects information about identifiable individuals.

28. The Privacy Act will continue to apply to data holders, accredited requestors, and outsourced providers, so all personal information remains subject to the requirements of the Privacy Act, except where the draft law says otherwise.

29. Customer data requests under the draft law are similar to Information Privacy Principle (**IPP**) 6 requests for personal information under the Privacy Act. IPP 6 entitles an individual to access their information, and provides that requests may be made by an individual's representative on their behalf. The intent of the draft law is to more specifically enable access to customer information in a standardised format which can be exchanged and processed by computers, in a safe and secure way.

30. The draft law provides that all customer data requests are IPP 6 requests under the Privacy Act to the extent that they relate to personal information. The process under the draft law is a little different and is intended to make it easier to access customer data. Individuals will still have a right to access their personal information under the Privacy Act.

31. In some areas, the draft law makes it clear that there will be more specific requirements for customer data requests set in standards and regulations, that accredited requestors and data holders will need to follow. This includes, for example, a shorter deadline for

providing data to data requestors compared to the 20 working days prescribed in the Privacy Act.

32. The Privacy Commissioner will be able to exercise all their existing functions and powers in relation to personal information under the draft law. This means the Privacy Commissioner will continue to have investigation, guidance, enforcement and redress powers over any obligations in the draft law that relate to Privacy Act safeguards. The draft law 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. See pages 53 to 58 for further details on how shared jurisdiction, and various powers, penalties and liabilities are proposed to work.

33. At this stage, we have only considered Privacy Act interactions for customer data requests. Further consideration of Privacy Act interactions for action initiation under the draft law is required, but we expect it would follow a similar approach to how customer data requests are treated.

34. Adding special requirements for the draft law which do not have an equivalent for personal information more generally would add significant cost and complexity for participants. This will reduce uptake and benefits from using the draft law to exchange data rather than other less efficient and secure mechanisms (like screen scraping) where the draft law will not apply. Further policy decisions that relate to privacy more broadly are more appropriately considered in any future review of the Privacy Act.

Differences from the Australian Consumer Data Right

35. The draft law has similar aims to the Australian CDR, but also has some key differences because we are relying on our Privacy Act. Unlike our Privacy Act which applies across the economy, the Australian Privacy Act 1988 generally applies only to Government agencies and organisations with an annual turnover of more than $3 million. The Australian CDR includes requirements on CDR participants to invest in additional functionality which:

    - enables them to delete customer data, on request of the customer. In New Zealand, the Privacy Act's IPP 7 empowers an individual to request the correction of personal information that is held by them. The Privacy Act does not have a general right to request deletion of personal information, however IPP 9 states that an organisation should not keep personal information for longer than it is required for the purpose it may lawfully be used

    - enables customers to remain anonymous or use a pseudonym (eg 'customer 123') to minimise the data collected and held about them. In New Zealand, IPP 1 governs the collection of personal information more broadly and already requires data minimisation

    - prohibits the use of CDR data for direct marketing. In New Zealand, IPP 3, IPP 4 and IPP 10 govern the collection and use of personal information. A prohibition on direct

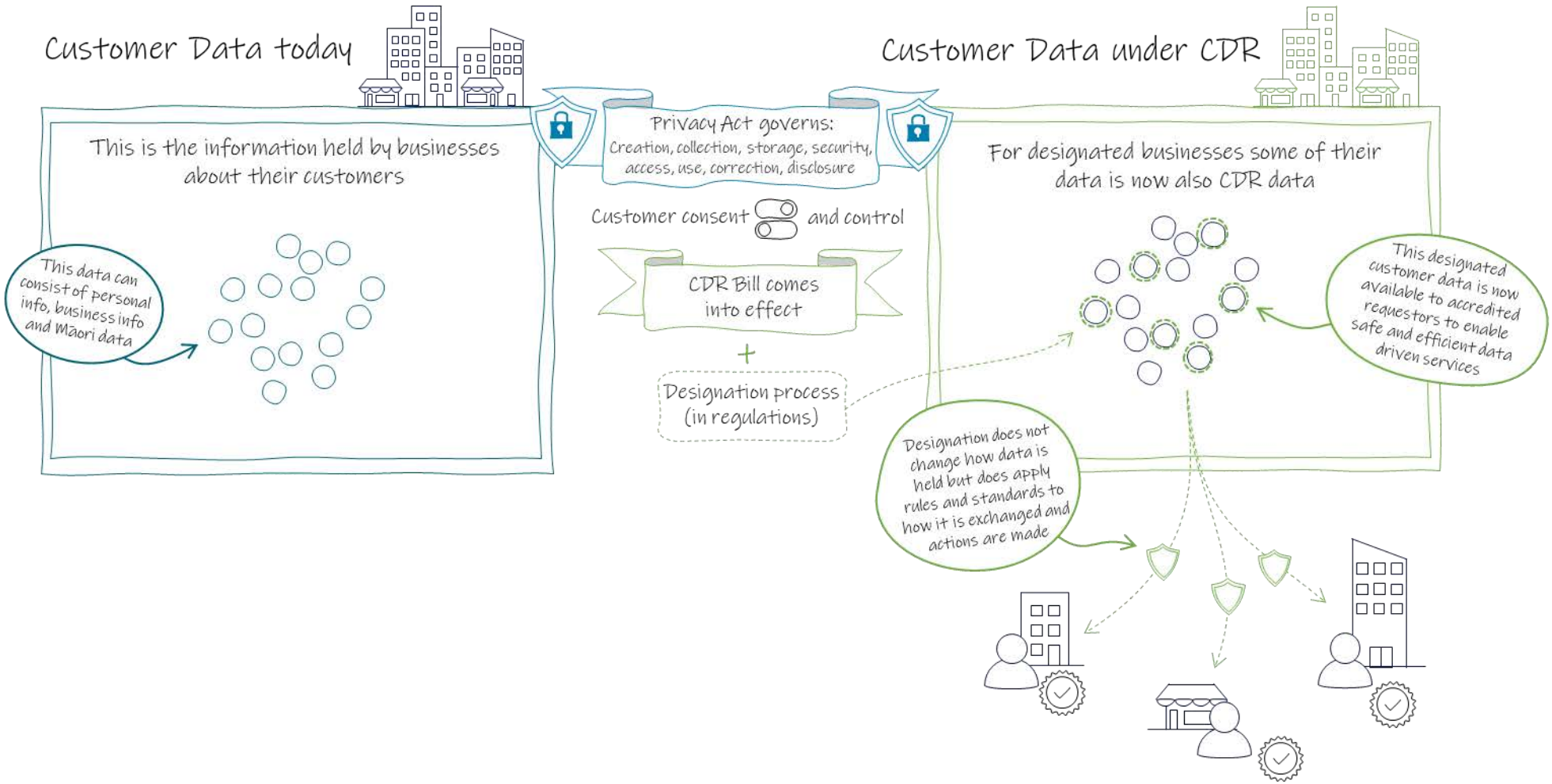
marketing is not proposed to be included in the draft law at this time because we wish to rely on the Privacy Act wherever possible.

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?

Diagram of customer data today and under the draft law

36. The diagram on the next page illustrates how the draft law's obligations overlay onto existing data held by businesses:

    - business security measures and Privacy Act obligations continue
    - designation will identify a subset of existing customer data, subject to the regime
    - customer consent and control remain central.


Customer Data today
This is the information held by businesses about their customers
This data can consist of personal info, business info and Māori data
Privacy Act governs:
Creation, collection, storage, security, access, use, correction, disclosure
Customer consent and control
CDR Bill comes into effect
+
Designation process (in regulations)
Customer Data under CDR
For designated businesses some of their data is now also CDR data
This designated customer data is now available to accredited requestors to enable safe and efficient data driven services
Designation does not change how data is held but does apply rules and standards to how it is exchanged and actions are made

Te Tiriti o Waitangi/The Treaty of Waitangi

37. The customer data that will be designated by the draft law will hold value and opportunity for all. Within designated customer data, some Māori data[5] will be a taonga (treasure).[6]

38. We consider that the draft law's requirements, and the overall purpose of the draft law, may be consistent with aspects of tikanga (Māori concepts, practices and values). This is because of the very high value placed by Māori on both:

    - safeguarding and protecting data, while also
    - ensuring it is used to advance collective and individual wellbeing.

39. We are interested in testing and exploring this.

40. The focus of the draft law is on standards relating to data exchange rather than data sets. However, we also think the draft law could benefit significantly from looking to and learning from the principles and concepts of Māori Data Governance. Again, this is because of the high value Māori place on care for and use of data.

41. As part of seeking feedback on the exposure draft, in questions 13, 15 and 28 we seek feedback on:

    - how a Te Tiriti/Treaty and te ao Māori lens could strengthen the processes and decisions required in the draft law
    - the detailed design of the draft law's requirements and implementation
    - the opportunities or risks that the implementation of the draft law could present for iwi, hapū and Māori individuals, businesses and organisations.

42. The draft law will apply to Māori data, even where it is not identifiable as such. Tikanga associated with data governance practices may be relevant to design of the draft law's regulations, standards and user interfaces.

43. There will be relationships between the articles of Te Tiriti/the Treaty, tikanga relating to data governance and use, and elements of the draft law (respect, care, trust and unlocking value). We are interested in feedback on these. There are strong linkages also with the

---

[5] Māori data is data that is produced by Māori, or that describes Māori and the environments they have relationships with. Hudson, Anderson, Dewes, Temara, Whaanga and Roa (2017) "He Matapihi ki te Mana Raraunga" - Conceptualising Big Data through a Māori lens. In Whaanga, Keegan & Apperley (Eds.), He Whare Hangarau Māori - Language, culture & technology (pp 64–73). Hamilton, New Zealand: Te Pua Wānanga ki te Ao / Faculty of Māori and Indigenous Studies, the University of Waikato, ***https://researchcommons.waikato.ac.nz/handle/10289/11814***.

[6] The data which becomes designated will likely have high value, will almost always have multiple uses, and we expect it will hold significant opportunity, thus meeting the criteria outlined by Hudson et al (2017), in footnote 5.

Māori Data Governance Model developed by Te Kāhui Raraunga[7] and we will be working to identify these now that this model has been published.

Other linkages and alignment

44. The draft law is aligned with elements of existing legislation (eg the Digital Identity Services Trust Framework Act 2023 (**DISTF Act**), and Accreditation and Standards Act 2015 where possible. We will also continue working to align with other work, including the Single Customer View requirements being developed under the Deposit Takers Bill, and work under the Retail Payment System Act 2022.

45. The draft law is informed by the Australian Consumer Data Right legislation – both the existing law and the proposed amendments currently before the Australian Parliament. To support interoperability of the two systems, the draft law:

    - provides that consistency with international standards is a consideration in the development of any binding standards relating to data exchange
    - limits the requirements relating to action initiation to accredited requestors and designated data holders
    - enables the setting of accreditation criteria similar to those in Australia, the United Kingdom.

Proposed scope

46. The draft law will:

    - apply to the entire economy, but will be turned on gradually through designation regulations (identifying particular data holders, product data and customer data)
    - apply to designated customer or product data held by those carrying on business in New Zealand irrespective of where data is collected or held, or where the customer or product concerned is located (see territorial application on page 44 for more detail)
    - apply to the Crown. Data held by government can be designated into the system.

47. Using the new system is opt-in for customers. The draft law requires that customers who opt-in can withdraw their consent at any time.

[7] Māori Data Governance Model (May 2023), Te Kāhui Raraunga, ***https://www.kahuiraraunga.io/tawhitinuku***.

Out of scope

48. The draft law does not seek to change broader legal settings regarding:

    - other methods of sharing data (eg screen scraping)
    - the use or on-sharing of personal information or other information
    - collection, storage, security of personal information or commercial information
    - data ownership or geographical location of where data is stored.

49. The intention is for these to be governed by existing, economy-wide requirements to minimise compliance costs and encourage uptake of secure data services regulated by the draft law.

50. The draft law does not require customer data to travel via government agencies when it is exchanged. These exchanges happen directly between a data holder and accredited requestor once the necessary safeguards are met.

51. The draft law does not create any additional powers for the government to collect, share or view people's customer data or business information.

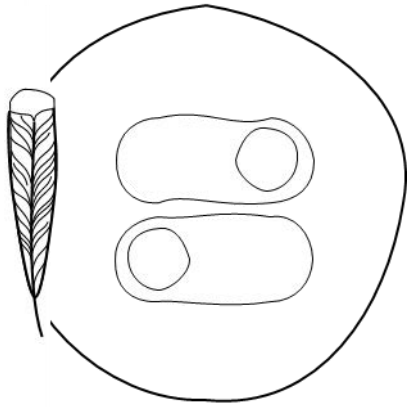
52. The draft law relates to existing data already held by product and service providers. It does not require the creation or collection of new customer data.

Key issues for feedback

53. The primary function of the draft law is to require designated data to be shared on request of the customer it is about, in standard formats, if the necessary checks and safeguards are met. This enhances the ability for customers to exercise authority and control over their data. It is why this type of legislation has been summarised as a 'consumer data right' here and overseas.

54. The draft law includes several safeguards, on which we are seeking feedback.

1. Consent settings: respecting and protecting customers' authority over their data



55. Strong consent protections are central to the draft law. They are the key to respecting the authority of all customers – including businesses or other entities – over the data held about them by businesses.

56. The draft law provides that designated customer data can only be shared if that customer has provided consent that is express and informed. It also provides that data holders and receivers must enable consent to easily be withdrawn at any time.

57. Regulations made under the draft law will provide more detail on these safeguards. These will be developed later following further public engagement and consultation.

58. In this document, we are seeking views on the design of the high-level consent safeguards in the draft law itself. We are also seeking feedback on some of the detail that future regulations could contain for requirements about consent, to make sure the two will work well together.

How should ongoing consent be managed?

59. When consent to access data is given, an important element is the length of time for which it lasts. Consent is called an 'authorisation' in the draft law, and is addressed in clauses 30 to 35.

60. Customers will be able to specify how long an authorisation is for, when they sign up for a product or service which is enabled by access to their customer data.

61. Managing customer awareness and consent over time is important too. Some customers will be forgetful, or have low motivation to review their settings and check they are still aligned with their needs and interests. The risk in these circumstances is that data continues to be accessible after a customer is no longer interested in or using the product or service they signed up for.

62. The draft law provides that regulations can specify a maximum length of time (after which all consents must expire), or else stay silent on the matter. We are seeking feedback on the best approach to managing ongoing consent, and what safeguards are proportional to risk. We think the key considerations to balance here are ease of use for customers, maximising participation, and implementation cost for businesses.

63. Australia's CDR has a 12-month expiry period.[8] This means that even if customer wants to give consent for a period longer than 12 months (for example, ongoing access for a budgeting platform), the customer's consent must still expire after 12 months.

64. The United Kingdom's Open Banking system originally had a consent expiry date of 90 days. This created a strong sense of security for customers. However, it also led to a large proportion of customers losing data-enabled services that they still wanted to use, because of fatigue and frustration, or because they didn't know they had to log back on, or because they forgot. In March 2022, the rules were changed to require only a yes/no confirmation of consent every 90 days.[9]

65. We note that regulations will also be able to specify events which require authorisation to end. We propose that they should specify that when a customer closes an account with a data holder, or when an accredited requestor's accreditation is suspended or cancelled, associated consents would end automatically.

2	Should there be a maximum duration for customer consent? What conditions should apply?
3	What settings for managing ongoing consent best align with data governance tikanga?
4	Do you agree with the proposed conditions for authorisation ending? If not, what would you change and why?

Future regulations about obtaining, withdrawing, or modifying of consent

66. The draft law requires that customers must give consent to data exchange – and be able to view and withdraw consent at any time. Regulations will lay out obligations for obtaining express and informed consent, and withdrawing consent. Where practical, regulated entities may also be required to have capability for modifying consent.

[8] Australia originally had 90 days but changed to 12 months in response to user submissions ***https://www.accc.gov.au/system/files/CDR-Rules-Outline-corrected-version-Jan-2019.pdf***, para. 7.25.
[9] See article 'UK changes from 90 days for consumers' ***https://www.fca.org.uk/publication/policy/ps21-19.pdf*** para. 1.30, page 7.

67. We are conscious that these safeguards should not create an inconvenient or burdensome customer experience which will discourage customers. This is because the process enabled by the draft law will be safer and more efficient than many alternatives currently in use, so good uptake will be important.

68. Further, we expect that customers may not always be able to interact with a data holding business online, or may prefer to interact in other ways. Therefore, the draft law should account for these needs and preferences.

69. We propose that the following obligations be required of data holders and accredited requestors in regulations:

- All parts of the consent process must be outlined in a clear and accessible way.
- When customers are consenting in the first instance, accredited requestors must inform customers that their consent can be withdrawn at any time and explain how to do so.
- In addition to the methods required by the draft law for the customer to view and end their consent (eg a dashboard) accredited requestors and data holders must also enable customers to withdraw their consent via a simple alternative method of communication (eg by phone or email).
- Ending consent must not be harder than agreeing to consent.
- If a customer wishes to withdraw their consent, the consequences (if any) of doing so must be outlined by the accredited requestor or data holder.
- If an accredited requestor receives a withdrawal of consent, they must notify the data holder (and vice versa). The customer must be notified once their request for withdrawal is actioned.

70. The regulations may also prescribe that certain modifications of consent must be available to customers (eg changing the expiry date of the consent).

71. We consider that this level of prescription in obligations provides clear and sufficient guidance without being overly detailed. This could enable the industry to maintain a degree of flexibility in how they meet the obligations. We also consider these obligations to be interoperable with Australia's CDR model.[10]

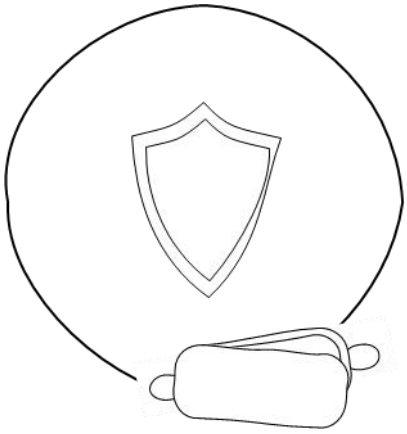
5	How well do the proposed requirements in the draft law and regulations align with data governance tikanga relating to control, consent and accountability?

[10] Subdivision 4.3.2A and B of Australia's Competition and Consumer Data (Consumer Data Right) Rules 2020 prescribe similar requirements ***https://www.legislation.gov.au/Details/F2021C00076***.

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?

72. As noted above, the relevant regulations will be developed in due course following further public engagement and consultation. They will also include specific functionality required for common situations. These include joint account holders or secondary users (eg staff acting on behalf of their employer).

2. Care during exchange: standards



73. Increased flows of data across the economy also increase the risks of breaches of privacy, or of unauthorised releases of commercially sensitive information. The creation of standardised safeguards, processes, and penalties around the electronic exchange of customer data are important to ensure all customers can have confidence in the level of protection provided for their information when it is exchanged.

74. Put simply, standards are a set of requirements for how something should be done. The purpose of standards under the draft law will be to set certain technology requirements and specifications for regulated entities, so that accredited requestors' computer systems can 'talk to' those of data holders securely and effectively.

75. Standards will include technical standards for the interfaces between API's. These cover security and access controls, the description and format of data fields, and the structure of requests and responses. To ensure accessibility, inclusion, and consistency, it may also be necessary to set standards for the functionality or design of customer consent dashboards, or the structure of a customer's consent process. The draft law is designed to enable these types of standards too.

76. The standards themselves will be instruments of secondary legislation under the draft law.

How will standards be set?

77. Clauses 87 to 89 of the draft law provide that MBIE's Chief Executive will set standards. This can be done as part of the designation process of a particular sector.

78. The intention is to build on the industry-led work already underway. For example, in the banking and payments sector, the Payments New Zealand API Centre has been developing technical standards for the exchange of payments and transaction information. These are already being implemented by the sector, at various speeds.

79. The draft law sets out considerations that must be taken into account prior to creating new standards or incorporating existing ones. These include whether the material is consistent with tikanga Māori in relation to data governance, and whether incorporating the material would create unnecessary obstacles to international trade and investment.

80. Further, the draft law requires that prior to making standards, MBIE must consult with the Privacy Commissioner, and people and groups that will be substantially affected by the issue of the proposed standard. This includes iwi, hapū and Māori organisations (see clause 88 of the draft law).

81. The proposed considerations and procedural requirements are based on those which currently apply either to the making of standards under the Standards and Accreditation Act 2015[11] or under the DISTF Act.[12] The intention is to ensure due process before a proposed standard is granted legally binding status. There may be occasions in which some considerations are in tension with others. In these cases, it will be appropriate for the various trade-offs to be expressly identified.

82. We note that we do not expect it to be necessary for standards to cover collection, use and storage of personal information. These matters are currently, and will continue to be, governed by the Privacy Act as outlined on pages 17 to 20.

83. The draft law provides that failing to adhere to certain requirements in relation to personal information will be treated as breaching Privacy Act requirements (see clauses 47 and 48).

7	Do you think the procedural requirements for making standards are appropriate? What else should be considered?
8	Do you think the draft law is clear enough about how its storage and security requirements interact with the Privacy Act?

84. Thinking ahead, it is also essential to ensure that standards about data in different sectors of the economy are as interoperable as possible.

85. We want to ensure the draft law is well-adapted for when data in second and subsequent sectors is designated under the draft law. We are interested in your views on which elements of the current API standards for banking are suitable for use in other sectors, and which would require significant modification.

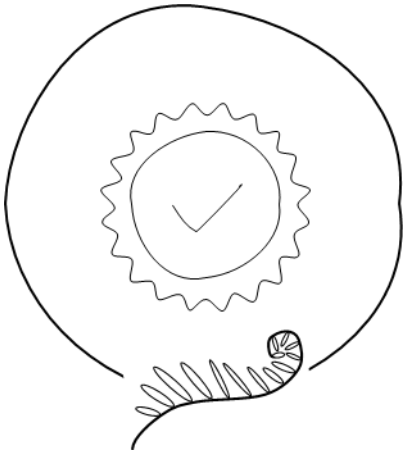
86. We think that the security standards that have been developed for banking could be appropriate for many other types of sensitive data or transactions. Using bank-level security standards for exchanges under the draft law would effectively protect all data as if it had a high level of sensitivity.

---

[11] See considerations for Board in section 13(4) ***https://www.legislation.govt.nz/act/public/2015/0091/latest/DLM6203017.html***.
[12] Section 21, DISTF Act provides for similar consultation requirements and exceptions ***https://www.legislation.govt.nz/act/public/2023/0013/latest/LMS459644.html***.

9	From the perspective of other data holding sectors: which elements of the Payments NZ API Centre Standards[13] are suitable for use in other sectors, and which would require significant modification?
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?

3. Trust: Accreditation of requestors



87. The draft law will create an accreditation regime for those who want to make binding requests for designated customer data or actions (clauses 64 to 73 of the draft law). It will also make it an offence for requestors to falsely hold themselves out as accredited when they are not.

88. An accreditation regime ensures only trusted people with trusted systems can make data or action requests using the draft law. It is critical to creating an environment in which customers and data holders can efficiently share data with service providers of their choice.

What privileges will accreditation provide?

89. Accreditation will grant a requestor the right to request data or actions from data holders, if other safeguards are also met. While any entity or person (accredited and non-accredited) can request data or actions on behalf of a consenting customer, the draft law *requires* data holders to comply with requests from accredited requestors. Non-accredited requestors can still make requests, but they will not have the benefits of the draft law, meaning data holders can choose whether or not they comply, and what format they send the data in.

How will accreditation be structured?

90. We intend to introduce different classes of accreditation according to risk level so accreditation processes and fees can be tailored to different kinds of use. This helps ensure costs and protections are proportionate to the use. With this in mind, we propose introducing two classes of accreditation in regulations, listed below.

[13] 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.

Class One: Action initiation

91. Requestors with this accreditation would be able to access, hold, view, change and use data. For example, they could initiate a payment or change information on a customer's online profile with the customer's consent. This class of accreditation would have more stringent requirements. The more stringent requirements would reflect the increased risk profile inherent in action initiation.

Class Two: Read-only access

92. Requestors with this accreditation would be able to access, view and hold data. For example, they could retrieve a transaction history or fee data. This class of accreditation would have less stringent requirements.

We have not provided a special class of accreditation for intermediaries

93. The Australian CDR regime has a special class of accreditation for intermediaries (entities which collect designated customer data on behalf of other entities).[14] This special class of accreditation was necessary because the Australian regime otherwise prevents accredited persons from sharing their data with others.[15]

94. Under our draft law, accredited requestors can share data with another entity if the customer consents to it. Considering this, we do not see a need to include a special class of accreditation for intermediaries. Instead, businesses that help other businesses request designated customer data or actions from a data holder would be expected to become an accredited requestor themselves.

Intermediaries and outsourced providers are different concepts

95. This discussion document and the draft law make reference to 'outsourced providers' (clauses 23 and 24). While there are overlaps between the concept of outsourced providers and the Australian concept of intermediaries, they refer to different things.

96. An outsourced provider is defined in the draft law as an entity that helps a data holder or accredited requestor perform a duty or power it holds. For a data holder, an outsourced provider might be an entity which helps it connect its data systems to enable regulated data services to be provided. For an accredited requestor, an outsourced provider might be an entity that requests the data from the data holder on the accredited requestor's behalf. In this latter situation, the outsourced provider would also need to be an accredited requestor themselves.

---

[14] See ***https://www.accc.gov.au/by-industry/banking-and-finance/the-consumer-data-right/consumer-data-right-cdr/accc-makes-accredited-intermediary-rules***.

[15] Subdivision 7.2.3 of the Competition and Consumer (Consumer Data Right) Rules 2020.

Reciprocal data sharing requirements are not proposed

97. In the Australian CDR Rules, accredited parties are treated as if they are data holders in some circumstances. This is called 'reciprocity' and means that accredited persons may be required to share specific CDR data as if they were designated data holders (including data they have generated themselves). These obligations are intended to bring more types of data into the CDR system more quickly, and to even the playing field between holders and others who provide data-enabled products and services. In recognition of the additional cost of reciprocal obligations, the Australian Rules provide for case-by-case applications to delay the onset of reciprocal obligations.[16]

98. We have proposed a different approach. To encourage the transition to regulated data services from other methods such as screen-scraping, our intention is to maximise uptake and the participation of accredited requestors. Accordingly, our draft law does not provide for reciprocal data holder obligations on accredited requestors. If customer data created by accredited requestors (or their clients) is considered suitable for regulated data services, a designation process can be used to bring this data into the regime.

What should the requirements for becoming accredited be?

99. Regulations will set the criteria which must be met before an applicant is accredited.

100. We propose that the initial criteria set out in regulations include a fit and proper person test and a demonstration of adequate information protection and security measures. We are also considering whether they should include proof of appropriate business insurance. Each of the proposed criteria is set out below.

Fit and proper person

101. We propose that the directors and senior managers of the applying entity – or anyone in an equivalent position – must be 'fit and proper persons'. The requirements for this criterion could be similar to other 'fit and proper' tests in existing legislation, such as the Credit Contracts and Consumer Finance Act 2003.[17] If the applicant can show they have passed an equivalent test under another Act, we propose there should be a fast-track option available.

Demonstrated information protection and security measures

102. We propose that the applicant must have demonstrated appropriate information protection and security measures.

---

[16] ***https://www.cdr.gov.au/sites/default/files/2022-12/CDR-Accreditation-fact-sheet-version-2-December-2022.pdf*** Pages 10 to 11.

[17] For more information, see ***https://comcom.govt.nz/business/credit-providers/fit-and-proper-person-certification***.

103. To meet this criterion the regulations could require the applicant pass a system security test, complete a self-report on information protection and security measures, or demonstrate their ability to connect to and safely use the IT systems the draft law will rely on. These general regulations could be supplemented by sector-specific requirements. For example, businesses in high-risk sectors may be required to demonstrate more robust levels of information protection and security.

Evidence of appropriate insurance

104. Business insurance increases the ability of customers and other persons to obtain redress or compensation against a company which may have caused harm or loss. With business insurance, wronged customers are more likely to be compensated in the case of a breach of their legal obligations.

105. We are considering introducing a requirement in the regulations that businesses hold "appropriate" insurance. The regulations would not define what appropriate insurance must be – instead, whether insurance is appropriate would be assessed on a case-by-case basis by the accrediting agency when it assesses the application. However, as has been done overseas, we propose publishing guidance which would set out what insurance would be considered appropriate. This guidance could be easily updated by the accrediting agency as insurance practices change. We believe this approach would provide sufficient clarity to affected businesses whilst also being flexible enough to accommodate differing industries and practices so that it does not create barriers to entry.

Supporting the participation of Māori

106. To ensure that the regime works well for all, it must earn the trust of a wide variety of potential users. As noted earlier, there are strong interests on the part of iwi, hapū and Māori organisations in the care and guardianship of data. For this reason, we would like to understand their particular perspectives on the proposed criteria to become an accredited requestor. We would like to know if these criteria are sufficient to support trust from Māori customers, and whether the proposed criteria would affect the willingness or ability of Māori organisations to apply for accreditation.

Other ways to support trust

Transparency requirements

107. In addition to accreditation criteria, the draft law provides for regulations to add further safeguards (clause 84). This could include a requirement that both accredited requestors and data holders publish information in their data policies stating whether they, for example:

    - use customer data for research or statistical purposes

- sell or rent customer data, or insights from the data, to other parties.

108. Both of these things are currently permitted under the Privacy Act if there is customer consent, or if individuals are not identifiable.[18] This kind of transparency requirement would mean that people can make informed decisions as to whether to become a client of any given data holder or accredited requestor. See also paragraphs 172 to 173 below for more detail on data policies, and paragraphs 138 to 146 regarding options for guiding ethical data use.

Cultural capability of accredited requestors

109. Under the draft law, the ultimate 'user' is the customer themselves, but the accredited requestor or the ultimate data receiver will use access to the data to provide the good or service requested by the customer. They may hold the data for different lengths of time, subject to the Privacy Act (for personal information) or commercial agreements (in the case of non-personal information).

110. Not all accredited requestors or service providers will have the knowledge or capability to ensure that data is stored and used in a manner which is culturally appropriate for Māori customers, or for others with specific approaches or interests in relation to their data.

111. We have not proposed that accredited requestors be required to meet cultural capability thresholds as a criterion for accreditation. This is because other safeguards in the draft law and Privacy Act mean that customers will:

- choose which services they wish to opt-in to
- have to give express, informed consent prior to any data exchange.

112. Therefore, those providers who can demonstrate culturally appropriate approaches will be offering a point of difference in the market. We are interested in feedback on this point.

11	Should there be a class of accreditation for intermediaries? If so, what conditions should apply?
12	Should accredited requestors have to hold insurance? If so, what kind of insurance should an accredited requestor have to hold?
13	What accreditation criteria are most important to support the participation of Māori in the regime?

[18] More specifically: IPP 10 provides that "an agency that holds personal information that was obtained in connection with one purpose may not use the information for any other purpose unless the agency believes, on reasonable grounds, that the information: (i) is to be used in a form in which the individual concerned is not identified; or (ii) is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned".

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

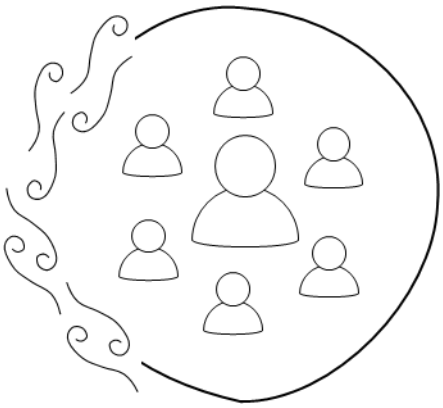
Note regarding interoperability

113. When developing the regulations, we will seek as much as possible to:

- align our accreditation criteria with similar criteria in international accreditation regimes
- introduce fast-tracks in the accreditation regime for businesses that will be required to complete a similar process for other domestic schemes, such as the DISTF Act. The rules for this are currently in development.

114. Interoperability will not however be an over-riding consideration. Cost-effectiveness, fit with our statute-book and constitution, equivalency of user experience with data exchange outside of the system, supporting accessibility and inclusion, and ensuring safeguards are proportional to risk will also be essential considerations.

4. Unlocking value for all



115. This section looks at future use cases to check that the settings in the draft law are suitable for all types of customers to benefit. Below we ask for feedback about opportunities for Māori, customers who are businesses, and about ways of ensuring accessibility and inclusion.

Māori, iwi and hapū

116. We seek your feedback on how the design of the draft law could best enable by-Māori for-Māori uses of data.

Māori approaches to data

117. All data has a whakapapa (genealogy).[19] Data about an individual is considered an extension of that person and can have different levels of tapu (sensitivity) depending on its nature and context.[20]

[19] Te Mana Raraunga, Principles of Data Sovereignty (2018) ***https://cdn.auckland.ac.nz/assets/psych/about/our-research/documents/TMR%2BM%C4%81ori%2BData%2BSovereignty%2BPrinciples%2BOct%2B2018.pdf***.
[20] See Hudson et al (2017), footnote 5, and Kukutai, Campbell-Kamariera, Mead, Mikaere, Moses, Whitehead, Cormack (2023).

118. There will be relationships between the articles of Te Tiriti/the Treaty, tikanga relating to data governance and use, and elements of the draft law. We are interested in feedback on these potential relationships.

Opportunities created by the draft law

119. In New Zealand, iwi, hapū and Māori organisations have significant responsibilities, but can face challenges in accessing timely, relevant and accurate data in order to carry out their functions and meet their aspirations.

120. By enabling data portability at the customer's consent, the draft law creates opportunities for access to data not only for the customer's direct benefit, but also potentially for collective benefit. Opportunities may include the following:

- Family trusts or businesses will be able to share account information easily with specialist advisers.
- Individuals could request that specific data about them be shared with collectives, such as hapū or iwi for governance purposes, or with initiatives such as Te Whata.[21]
- Accredited requestors or other data receivers could develop services enabling customer self-identification of Māori data (eg adding the hapū/iwi they belong to, before on-sharing with a party of their choice).
- Action initiation could assist with maintaining up to date contact details across tribal registers.
- Māori organisations could consider becoming accredited data requestors – to offer specialist data capability and functionality for iwi/Māori groups.

121. We want to ensure that the design of the draft law best:

- removes barriers to Māori accessing and using their own data
- enables use cases which align with iwi and Māori aspirations.

122. While not directly connected to the design of the draft law, we are also interested to hear from iwi/hapū/Māori organisations about their aspirations for capability to receive, use and protect customer data and product data.

[21] Te Whata is a data platform designed specifically by iwi, for iwi. See ***https://tewhata.io/*** for more information.

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.

Business customers

123. The draft law holds significant potential for businesses. Unlocking business' transaction and account records for access by accountants or other specialist advisers saves time and effort, and can generate new insights. The potential for efficiency and innovation will increase further as other sectors are designated, and banking data can, for example, be layered with energy use data or connected with non-bank finance products.

124. Small businesses in particular have been clear that they want to see an environment in which the cost and process of lending is reduced. The draft law will enable these efficiencies. A variety of use cases have emerged in the United Kingdom based on banking data and payment functionality. These include a range of business to business payments products, working capital lending products, and business operations products and services.

125. We are interested to understand any other use cases of particular interest to businesses, including small businesses, to ensure we don't inadvertently create barriers for them in our design.

126. We note that when the draft law is introduced and regulations design is underway, business input will be essential to ensuring that requirements for 'secondary user' functionality meet business operational and administrative needs.

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

Ensuring inclusion and accessibility

127. The intention is for accreditation to be open to all entities who meet the requirements, and for participation of customers to be driven primarily by the use cases on offer in the market. This is consistent with the purpose of the draft law as enabling infrastructure.

128. However, relying only on market-driven expansion could widen existing gaps in consumer access to some products or pricing. It may also mean the benefits of data-enabled products and services are focused on commercial customers and businesses, and not extended to collective and social purposes or the voluntary sector.

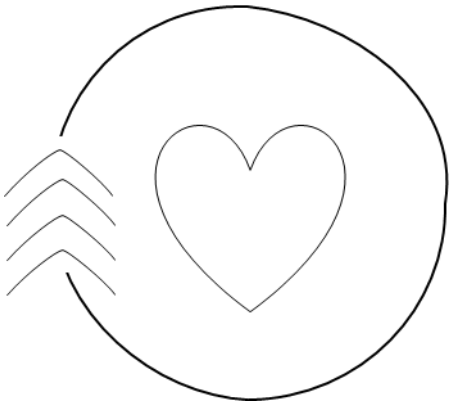
129. In other jurisdictions, 'data for good' initiatives have been proposed as a potential solution, to stimulate development of products and services specifically for broader social benefit, or else for customers who are not perceived as 'high value' or who might otherwise be underserved by the market. Any inclusion initiatives here would need to consider Te Mahere mō te Whakaurunga Matihiko – The Digital Inclusion Blueprint, Action Plan and its Outcomes Framework.[22] The blueprint defines four 'elements' key to inclusion: Motivation, Access, Skill, Trust. This is something which will be considered in due course.

130. At this stage, we are interested to understand the types of use cases which may be of interest to ensure we don't inadvertently create barriers for them in the design.

131. Further, we want to hear about ways that the implementation of systems and user interfaces under the draft law could actively support inclusion and accessibility. Guidance for data holders and accredited requestors will likely be of assistance here. We are considering whether a resource library could play a role. This could involve developing and/or sharing 'good practice' templates, user journeys or other 'patterns' which meet technical and accessibility standards as well as supporting participation from diverse customers. The availability of such templates or other guidance which could be adapted and re-used on a 'creative commons' basis could reduce compliance costs for designated sectors as well as make it easier for those who want to become accredited requestors to deliver services which are accessible and culturally inclusive. We seek your feedback on this idea.

17	What settings in the draft law or regulations should be included to support accessibility and inclusion?
18	In what ways could regulated entities and other data-driven product and service providers be supported to be accessible and inclusive?

5. Ethical use of data and action initiation



132. Accredited requestors will transmit or hold a lot of designated customer data, including potentially sensitive information. Where authorised by a customer, some will also be able to issue instructions to data holders on behalf of customers. This could include instructions to, for example, move money, update contact details, or open and close accounts.

133. A primary purpose of the draft law is to unlock data to generate value, including valuable insights, from data. Another is to encourage investment in more secure and efficient alternatives to data

[22] See ***https://www.digital.govt.nz/dmsdocument/113-digital-inclusion-blueprint-te-mahere-mo-te-whakaurunga-matihiko/html*** for more information

sharing methods currently in use. During previous consultations, several submitters highlighted the importance of also considering safeguards on the *ethical use* of customer data and action initiation. Ethical use of data sets is a key concept in Māori approaches to governance of data sets and would be in line with the purpose of the draft law regarding customer and social benefit.

What is 'ethical use'?

134. Ethics are beliefs about what is morally right and wrong. A variety of guidance and principles already exist with ethical data use in mind, such as the Stats NZ Ngā Tikanga Paihere data ethics principles,[23] the recently published Māori Data Governance Model[24] as well as the Ministry of Social Development's NZ Privacy, Human Rights and Ethics Framework[25] (PHRaE). None of these are binding on the broader economy.

135. Overseas, the Australian CDR amendment Bill currently before Parliament contains a duty that accredited persons act 'efficiently, honestly, and fairly' when initiating CDR actions.[26]

Existing legal protections on data use

136. The Privacy Act limits the use of personal information to the purpose for which it was collected, or where there is consent for a different use. However, there are exceptions, so personal information can be used for other purposes without an individuals' consent, including if:

    - it is used in a form that does not identify individuals, or
    - it is used for statistical or research purposes and won't be published in a form which would reasonably identify the individual(s).

137. In addition, the Privacy Act only covers personal information, so the protections for use do not extend to all designated customer data under the draft law. This means that insights from customer data can potentially be used for any purpose, including ones at odds with customer wellbeing or business interests.

---

[23] See ***https://www.data.govt.nz/toolkit/data-ethics/nga-tikanga-paihere/*** for more information.
[24] See ***https://www.kahuiraraunga.io/tawhitinuku*** for more information.
[25] Ministry of Social Development's Privacy, Human Rights and Ethics Framework (PHRaE) ***https://www.msd.govt.nz/documents/about-msd-and-our-work/work-programmes/initiatives/phrae/phrae-on-a-page.pdf***.
[26] See section 56BZA in the Treasury Laws Amendment (Measure for Consultation) Bill 2022: Consumer Data Right – Implementing Action Initiation, ***https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6950_first-reps/toc_pdf/22126b01.pdf***.

Considering safeguards for use of customer data

138. As noted at paragraph 107 to 108 above, the draft law enables transparency requirements to be set for data holders and data requestors, in relation to customer data, product data and action performance.

139. If it is considered necessary to include additional safeguards for ethical use of customer data, there are two proposed options for safeguards which we would like feedback on. We note these are preliminary options and that we are open to other approaches.

140. In line with feedback to date, the intention is that these additional requirements would apply to participants in regulated data services, rather than travel with the data (eg when it is on-shared in compliance with the Privacy Act).

Option one: Ethical requirements as a condition of accreditation

141. This could involve an additional requirement that requestors' systems and policies ensure data and action initiation are used ethically, responsibly and appropriately, and would be necessary for accreditation (as mentioned in paragraphs 99 to 112).

142. Requirements could be tailored for different sectors, as appropriate. For example, for accredited requestors of designated banking data this could potentially look like the fair conduct principle in the Financial Markets (Conduct of Institutions) Amendment Act 2022.[27] Other data designated in future may need a different standard (eg health data).

Option two: Requirement to get express consent from customers for de-identification of designated customer data

143. This could involve requiring accredited requesters and data holders to request and receive consent from customers before their data is de-identified[28] or used for research or statistical purposes. This option could relate specifically to 'read access' to data (rather than action initiation).

144. This requirement would give customers additional awareness and control over their customer data being used for purposes other than the direct good or service they obtain from the accredited requestor or other data receiver (ie they can choose to consent to de-identification or not).

145. When considering options for safeguards on use, a key consideration will be the purpose of the draft law. As well as unlocking data for the benefit of people and their organisations,

---

[27] Section 446C, Financial Markets (Conduct of Institutions) Amendment Act 2022.

[28] De-identification refers to a range of methods for reducing the amount of information in a data set such that individuals are not identifiable or are less easily identifiable. Some examples of de-identification methods and their effectiveness are provided here by Digital.govt.nz: ***https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/manage-a-privacy-programme/sharing-personal-information/making-personal-information-safe-for-reuse/***.

another purpose is to encourage investment in more secure and efficient alternatives to existing data sharing methods already in everyday use. If accreditation or other participation requirements on holders and requestors are too high or costly, the draft law will not be able to achieve either purpose.

146. If an appropriate balance cannot be struck in the draft law, it may be necessary to consider economy-wide safeguards in other legislation.

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

Chapter 2: The Customer and Product Data Bill - technical matters and system settings

147. We invite feedback on all aspects of the draft law. This Chapter:

- provides more information about some technical matters, and asks questions on specific details to ensure the draft law works well, and
- outlines regulatory settings including dispute resolution, powers and penalties, and the proposed regulators.

A. Structure of the draft law

Part of the draft law	What does it do?
Part 1 Preliminary provisions	Part 1 contains preliminary provisions. This includes clauses that cover the purpose and interpretation of the draft law, and the draft law's territorial application and application to the Crown.
Part 2 Regulated data services	Part 2 contains the main obligations for data holders and accredited requestors.
Part 3 Protections	Part 3 contains: • requirements about customers' consent and verification of their identity • provisions regarding notification, transparency of data policies, record keeping, complaints, and the relationship with other legislation such as the Privacy Act and the Official Information Act.
Part 4 Regulatory and enforcement matters	Part 4 contains regulatory and enforcement powers and penalties.
Part 5 Administrative matters	Part 5 enables and sets the process for: • the draft law being "turned on" for each sector to which it will apply • accredited requestors to apply for and receive accreditation • a public register of designated and accredited entities. • any cost recovery of government functions • standard making and exemptions • regulations.
Schedule	This will contain transitional, savings and related provisions (if required).

Part 1: Preliminary provisions

Purpose

148. Clause 3 provides the purpose statement of the draft law. It sets out the immediate and longer-term outcomes that the framework seeks to achieve.

21	What is your feedback on the purpose statement?

Definition

149. Our draft law, Australia's consumer data right, and the Payments NZ API Centre's standards each use different words to describe similar concepts. The table below shows how the words in the draft Bill relate to the words used in these other regimes. This table also aims to clarify where certain concepts do not have direct equivalents.

Terms			Concept
NZ draft law	**Australia CDR**	**API Centre Standards**	
Accredited requestor (clause 7)	Accredited data recipient (also called a consumer data right provider or provider) Accredited action initiator	Third party	A business which is accredited to request a data holder provide data or give effect to an action. While other businesses (who are not accredited) can request data or actions, data holders do not have to respond to the request. Data holders are only required to respond to a request when the request comes from an accredited requestor.
Data holder (clause 6)	Data holder Action service provider	Provider	A business which holds the data, or is capable of giving effect to the action, which an accredited requestor has requested. Only designated businesses holding designated data are considered data holders for the purposes of the draft law.
Outsourced provider (clause 21)	No equivalent	No equivalent	A business which helps a data holder or accredited requestor perform their duties or powers under the draft law. The definition is broad and captures a range of tasks and different kinds of help that a business might assist with. For example, an outsourced provider might: • help a data holder confirm the identity of a customer. • help an accredited requestor collect information from a data

Terms			Concept
NZ draft law	Australia CDR	API Centre Standards	
			holder (in which case the outsourced provider would also need to be an accredited requestor themselves). • help a data holder make their data available to accredited requestors.
No equivalent	**Intermediary**	No equivalent	A business which helps accredited requestors collect data from data holders. Intermediaries are an Australian regulatory concept and do not appear in the draft law. However, some kinds of actions an intermediary might do in Australia are caught under the definition of outsourced provider in New Zealand's draft law.
No equivalent	**Affiliate**	No equivalent	A class of accreditation which is used in Australia. Businesses can become an affiliate when they are 'sponsored' by an accredited requestor. Affiliates can request data from a data holder as if they were accredited themselves.
No equivalent	**CDR representative**	No equivalent	A business which is not accredited to request data or actions, but is allowed to handle consumer data. The Australian CDR regime sets rules around who may be a CDR representative and how a business can become one. In Australia, accredited requestors can only ask other businesses to handle data (store it, clean it, or help an accredited requestor use it) if the other business is a CDR representative. In New Zealand, accredited requestors can employ the services of outsourced providers to do these things, as long as they comply with the Privacy Act. The draft law includes the ability to make regulations relating to outsourced providers. No specific requirements are currently considered to be necessary, but the power has been included in case it is needed in future.

Data

150. The term ‘data’ is not defined. The draft law notes that data includes information, and personal information within the meaning of the Privacy Act.

151. The intention is for the term to include derived data, and data derived from derived data. The designation regulations will identify which customer and product data, and which data holders become subject to the draft law, following the process set out in clauses 59 to 63.

Directors and senior managers

152. The term director has the same meaning as in Section 6 of the Financial Markets Conduct Act 2013.

153. Similarly, senior manager, in relation to person (A), means a person who is not a director but occupies a position that allows that person to exercise significant influence over the management or administration of A (for example, a chief executive or chief financial officer).

154. The definitions of director and senior manager have two purposes in the draft law:

- They are relied on when providing for who may authorise data exchange on behalf of customers who are businesses.
- One of the proposed accreditation criteria is a ‘fit and proper person’ test for directors and senior managers of accredited requestors. The definitions are in line with the Credit Contracts and Consumer Finance Act and Financial Markets Conduct Act to enable the ability for a ‘fast track’ process for this criterion, where an entity’s directors and senior managers have already been considered a fit and proper person under those laws. See paragraph 101 of Chapter 1.

Territorial application

155. The draft law would apply in respect of designated customer data or designated product data held by those who carry on business in New Zealand.

156. It does not matter where the data is collected or held, or where the customer or product concerned is located.

157. A business can be treated as carrying on business in New Zealand without necessarily:

- being a commercial operation
- having a place of business in New Zealand
- receiving payment for goods or services
- intending to make a profit from its business in New Zealand.

158. This proposed scope of application is based on that of the Privacy Act. It is important to note that in practice, the application of the draft law's requirements will be limited to those who either apply for accreditation, or who are brought into the scheme via designation regulations.

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

Part 2: Regulated data services

159. Part 2 of the draft law includes the obligations that apply to data holders, and provides for specific rules to be set around joint account holders and secondary users. It also provides for obligations in relation to 'outsourced providers'.

Joint customers (clause 19) and secondary users (clause 22)

160. The draft law needs to cover a wide range of customers, including individuals, businesses and other entities.

161. Many customers hold accounts jointly with another person, such as their spouse. Other customers are businesses or trusts, and will have different needs to individuals in relation to giving and managing consents for the exchange of their data. For example, a customer which is a business may need different permissions for staff in accounts, and for its chief financial officer.

162. This is why the draft law provides that data holders and accredited requestors may be required to maintain systems or processes for dealing with secondary users and joint customers. The detailed requirements for this functionality will vary by sector, and will be provided for in regulations.

163. We acknowledge that many data holders already have systems or processes in place for dealing with secondary users and note that these will be considered during the designation process. This will help ensure that as many types of customers as possible can benefit from regulated consumer data services.

Electronic system

164. Clause 26 of the draft law proposes that regulated data services must be provided electronically and in the way prescribed by the regulations and standards. This is a core requirement of the draft law – ensuring that data is exchanged efficiently, securely, and with standard formats and safeguards.

165. The draft law provides for a broad range of matters which the rules and standards may cover, however not all of them will require a standard or a rule to be created in the first instance. Security of the exchange process, and standard formats will, however, be essential.

Reasons to refuse access to customer data or to carry out an action

166. The draft law proposes that if a customer or an accredited requestor makes a valid request for designated customer data, or to perform an action, then this must be provided or performed.

167. We would like feedback on how best to align this requirement with existing obligations and safeguards:

- Regarding automated access to customer data, existing practices and protections in the Privacy Act allow access to data to be refused in some cases, including but not limited to if the data holder has reasonable grounds to believe that the request is made under the threat of physical or mental harm (section 57(b) of the Privacy Act) or if the disclosure of the information would cause harm to an individual (in the categories set out in section 49 of the Privacy Act).
- Regarding the performance of an action, existing practices and common contract terms which allow the refusal to act on instructions where they have good reason to do so, such as where there is a risk of fraud.

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

Part 3: Protections

168. Part 3 of the draft law includes the key safeguards which should be part of customer data exchange in any sector. These include the requirement for customer consent, the ability for customers to easily view and withdraw consent, the requirement for authentication of customers' identity and for certain notifications. They also include the following, which are discussed in more detail below:

- record keeping
- customer data policy
- complaints.

Data holders and accredited requestors must keep certain records

169. The draft law provides that a data holder and accredited requestors must keep records of a range of matters.

170. The purpose of these record keeping requirements is to enable monitoring of data holder and accredited requestor compliance, to support enforcement. For example, in the event of a reported breach MBIE or the Privacy Commissioner could request these records as part of their investigation. If this record keeping requirement requires the development of new systems and storage we expect it would incur compliance costs, however, we also consider that record keeping would improve consumer protection and trust in the system.

171. We note that the provisions do not require the storage of the customer information itself. The draft law proposes that records must be kept by data holders and accredited requestors for five years.

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?

Data holders and accredited requestors must have customer data policy

172. The draft law requires data holders and accredited requestors to develop, publish, implement and maintain policies relating to customer, product and action requests.

173. These policies are intended to help customers choose whether to do business with a data holder or accredited requestor based on how customer data is managed. We think customers will want to know the following:

- For both data holders and accredited requestors:
    - how a customer can complain about compliance with obligations in the Bill
    - the complaints process
    - the name of any outsourced providers used, the nature of the services provided, and the type of data used or held by them; potentially also what checks are carried out before using an outsourced provider
    - whether any customer data or insights from customer data are rented or on-sold, and if so, for what purposes, and in what manner (including how it is de-identified prior to being shared further).
- For accredited requestors only, we propose the policy must also contain:
    - what class of designated customer data or designated action the accredited requestor is accredited for.
- For data holders only, we propose it must also contain:

- what designated customer and product data they hold, and what designated actions they must perform.

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

Complaints

174. Clause 43 sets out requirements relating to the complaints process that data holders and accredited requestors must have. The early resolution of complaints is beneficial to all parties.

175. We expect that many data holders will already have customer complaints processes in place and therefore this requirement will not impose significant additional costs (if any). However, some accredited requestors may need to establish customer complaints processes to comply with this requirement. This will incur a compliance cost.

176. When a sector is designated, we propose that accompanying regulations will require customer complaints to be referred to existing industry dispute resolution bodies when these have not been resolved in the internal complaints process.

Part 4: Regulatory and enforcement matters

177. Part 4 contains regulatory and enforcement powers and penalties. We note that much of this part is not included the draft law at present. These provisions will depend on the final form of the main obligations.

Regulatory powers

178. Currently, the Privacy Commissioner has broad responsibility under the Privacy Act to monitor and enforce compliance with the Privacy Act, including own-motion investigations, providing redress for breaches of an individual's privacy and receiving reports of notifiable privacy breaches. The Privacy Commissioner will continue to have the role of compliance and enforcement of privacy matters to the extent that breaches of this new legislation are also breaches of the Privacy Act, including in setting expectations through guidance and (if necessary) Commissioner-issued Codes of Practice (akin to regulations).

179. However, a specific enforcement agency with appropriate regulatory powers for compliance and enforcement is necessary to uphold the obligations in the draft law (beyond those which would be covered in the Privacy Act) and to ensure the integrity of the new system.

MBIE's chief executive may require person to supply information, produce documents, or give evidence

180. Clause 49 introduces information gathering powers to ensure that MBIE is able to effectively monitor and enforce the draft law's obligations on data holders and requestors.

181. These requirements are similar to the information gathering powers in the Australian CDR regime.[29]

27	Are there any additional information gathering powers that MBIE will require to investigate and prosecute a breach?

Part 5: Administrative matters

182. Part 5 of the draft law contains provisions which enable and set the process for, among other things, designation, regulations and standards, government fees and levies, reporting requirements, and the operation of a register of data holders and accredited requestors. These are discussed in more detail below.

Designation process

183. A person or a class of persons (in effect a sector) may be designated as data holders through regulations made by the Governor-General on recommendation of the Minister.

184. Clause 60 of the draft law provides that the Minister must have regard to certain matters before recommending that designation regulations be made. This includes the interests of customers, including Māori customers, and the impacts and benefits for data holders.

185. We consider that these specific considerations are necessary in addition to standard Regulatory Impact Assessment considerations because of the significant investment required by data holders to comply with the draft law.

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?

Note on context for designation process

186. Proposed designations will come after dedicated rounds of engagement on:

[29] Section 56BI(2) of the Australian Competition and Consumer Act 2010 and rule 9.6 of the Competition and Consumer (Consumer Data Right) Rules 2020 give power to the Australian Competition and Consumer Commission or Information Commissioner to give written notice to produce copies of records or information for such records.

- the proposed data, and data holders
- the text of the proposed designation regulations, and the implementation plan for a sector – including the sequencing of mandatory functionality within that sector.

187. The first sector which will be designated is banking. The criteria that the Government took into account when deciding to prioritise banking for designation were:

- opportunities or benefits that a designation could realise and problems it could solve or mitigate in the sector
- ease and speed of implementation
- whether data sharing in the sector is likely without regulatory intervention.

188. These criteria will continue to be relevant when considering which sectors to bring into the system next.

Giving effect to Te Tiriti o Waitangi/the Treaty of Waitangi in decision making

189. Te Tiriti/The Treaty creates a basis for civil government extending over all New Zealanders, on the basis of protections and acknowledgements of Māori rights and interests within that shared citizenry.

190. To give effect to Te Tiriti/the Treaty when making decisions about regulations and standards,[30] the draft law proposes an approach similar to that in the sections 21 and 47(2)(a) of the DISTF Act. This alignment will assist with consistency, and reducing complexity and cost for government, iwi, hapū and other participants in the system.

191. To align with the DISTF Act the draft law provides:

- procedural requirements before regulation and standard making. It requires consultation with iwi, hapū and Māori organisations, as well as with tikanga experts who have knowledge of te ao Māori approaches to data governance (see clauses 61 and 88 of the draft law)
- specific considerations during the making of technical standards or their incorporation by reference. MBIE (through its chief executive) must have regard to whether the material is consistent with tikanga Māori in relation to data governance (see clause 89 of the draft law).

[30] As noted in Chapter 1, the nature of requirements in the regulations, and the use cases which are enabled by the CDR are both relevant to Te Tiriti/Treaty obligations. Thoughtful design of user experience and interfaces are also relevant as they can help to ensure the system is accessible and unlocks value for all.

192. The draft law also proposes that the Minister must have regard to (among other considerations) the following matters before designating data (see clause 60 of the draft law):

- the interests of customers, including Māori customers
- the sensitivity of the data. This could include whether it is tapu.

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?

Government fees and levies

193. The draft law will enable the imposition of levies, as well as some cost recovery through accreditation fees.

194. No policy decisions have been made regarding the appropriate extent or timing of cost recovery. We are aware that significant investment will likely be required from data holders and potentially also accredited requestors in order to participate. This cost to participate will be a key consideration when developing any cost recovery approach. Engagement and consultation on these matters will take place in due course.

Register of data holders and accredited requestors

195. The draft law enables MBIE to maintain a publicly accessible register of data holders and accredited requestors. This is important for transparency and accountability.

196. The draft law also provides for MBIE to maintain a closed register accessible only to data holders and accredited requestors. This register will have machine-readable interfaces for automated access and use, eg to check whether a data holder is currently able to respond to data requests, or whether a requestor is accredited.

197. We would like to know what further information would be of particular assistance to data holders and accredited requestors to include on the closed register.

30	What should the closed register for data holders and accredited requestors contain to be of most use to participants?
31	Which additional information in the closed register should be machine-readable?

Reporting requirements

198. The draft law proposes a fixed date for annual reporting for accredited requestors, to ensure a consistent basis for measuring performance of the regulated data system overall.

199. A reporting date of 31 October for the period ending on 30 June each year has been proposed, to be away from financial year and tax reporting deadlines.

200. The measures which must be reported annually will be defined in due course. We imagine they will include the number of customers requesting access to their data or requesting action initiation, and transaction volumes.

201. There may also be an opportunity for data holders to provide real-time reporting to the enforcement agency. This could cover the performance of data holder APIs in a frequent, automated manner, to ensure system health and promote accountability. This would be similar to the requirement on data holders in the Australian CDR.[31] Clause 26(2)(h) in the draft law enables this kind of requirement to be introduced. We seek your feedback on this idea.

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?
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?

Specifying customer refunds or redress in regulations – nature of cap

202. The draft law enables requirements to be set in regulations allowing for customer refunds or redress in some circumstances. Such requirements will provide clear accountability and processes in cases of error or delay in action initiation (eg a payment error causes the customer to be charged a late fee). Similar regulations are in place in the United Kingdom.[32]

203. For this kind of requirement to be suitable for regulations (rather than the Act itself) it may be necessary to include a cap on the amount which can be required to be repaid. This amount could be reviewed and adjusted by the Minister of Commerce and Consumer Affairs, in line with the Consumer Price Index, as with the approach taken in the Financial Reporting Act 2013[33] or else it could be indexed or tethered to the Consumer Price Index.

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

[31] Under the Australian CDR data holders report information to the Australian Competition and Consumer Commission regarding performance and availability as set out in the Consumer Data Standards. See the dashboard here: ***https://www.cdr.gov.au/performance***.
[32] See clauses 91-94 of the UK's Payment Services Regulation 2017.
[33] Under sections 48 and 49 of the Financial Reporting Act 2013 the Minister must regularly review amounts for the purposes of determining whether or not to recommend that an adjustment be made to take into account any increase in the CPI during the period to which the review relates.

B. System settings

Regulators

204. MBIE will be responsible for standard setting, accrediting requestors, operating the register, and promoting the use and uptake of regulated data services. MBIE will also be responsible for compliance and enforcement functions under the draft law.

205. Where breaches relate to personal information, the Privacy Commissioner and Human Rights Review Tribunal will also have a compliance and enforcement remit under the Privacy Act.

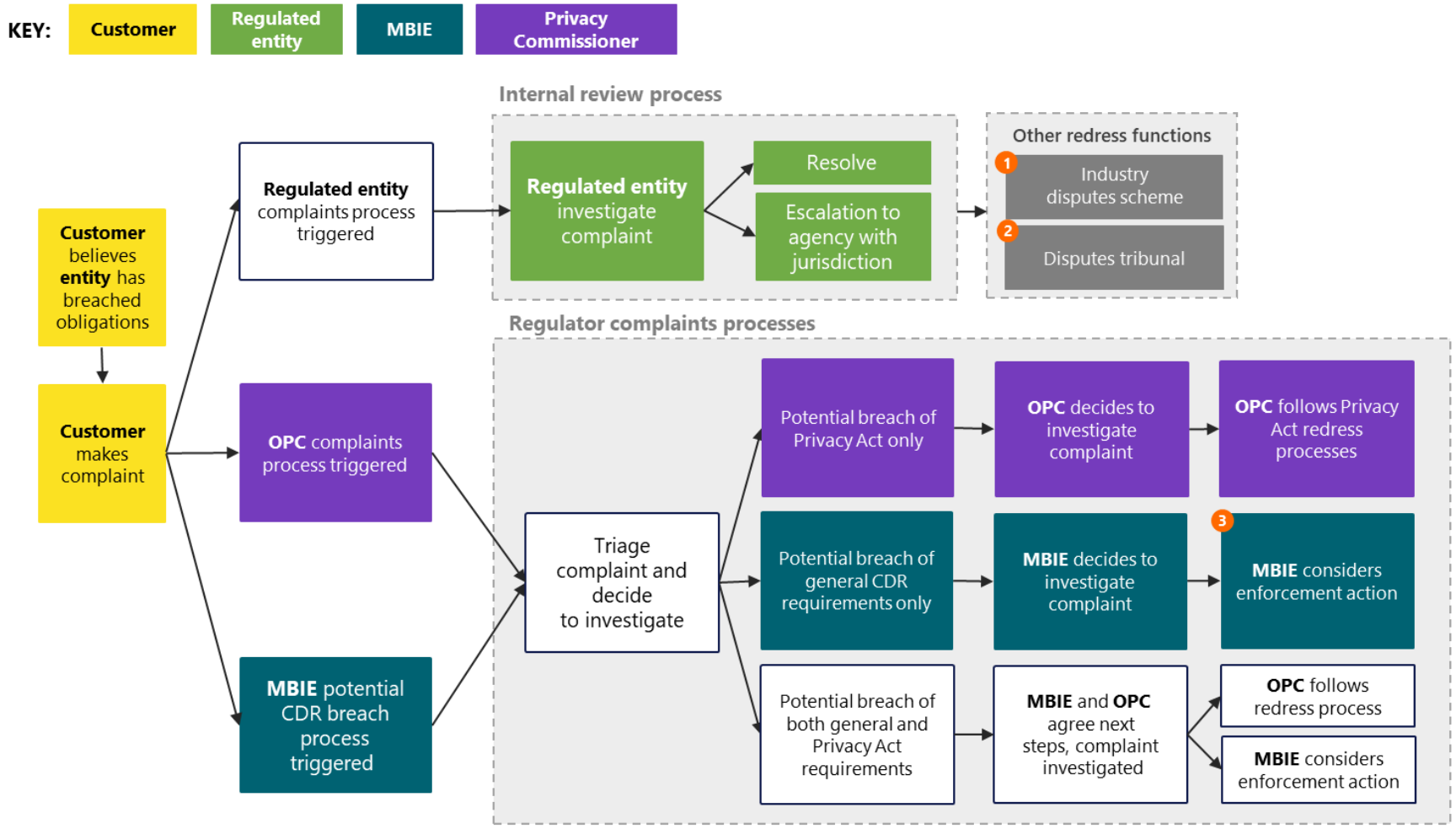
206. A Memorandum of Understanding between MBIE and the Office of the Privacy Commissioner will clarify the roles and processes of the two regulators where both privacy and non-privacy considerations are involved.

Complaints and dispute resolution

207. While there are protections in place for customers under the draft law, issues between customers, data holders and accredited requestors will still arise at times. It is therefore important to have a way to resolve these issues quickly and effectively.

208. Complaints can be made to accredited requestors and data holders, or else to the regulators. The following diagram shows an overview of the complaints system. This is then discussed in more detail below.

Overview of the complaints system



1. E.g. Banking Ombudsman, Utilities Disputes.
2. The Disputes Tribunal can act as a back-stop where it might be inappropriate to require membership for an industry dispute resolution scheme. The Disputes Tribunal has a general jurisdiction to cover claims up to $30,000.
3. New powers, processes and remedies under the draft law in addition to existing remedies.

Privacy-related complaints to regulators

209. We expect that many of the complaints that customers will have about regulated entities will be privacy related. These will follow the current process for privacy complaints.

210. Where a complaint relates to personal information or breaches of the Privacy Act IPPs[34] it will be dealt with by the Privacy Commissioner using their existing powers, systems and processes. The Privacy Commissioner will encourage parties to settle complaints using conciliations, even where they do not investigate. Where the Privacy Commissioner is unable to resolve the issue, they will close the complaint and provide a certificate that can be used to take the case to the Human Rights Review Tribunal.

Other complaints to regulators

211. Where a complaint to regulators relates to a situation where the Privacy Act does not apply (eg the customer is a company, and personal information is not involved), this will be dealt with by MBIE as the enforcement agency.

212. There will be cases in which the Privacy Commissioner's and MBIE's jurisdictions overlap (eg a participant has not complied with a security standard and this has resulted in the unauthorised disclosure of personal information). A Memorandum of Understanding will clarify the roles and processes of the two regulators where both privacy and non-privacy considerations are involved. To support the functioning of this relationship, the Privacy Commissioner and MBIE must be able to share information to assess the case and refer complaints to one another where appropriate. Following consultation, the necessary information sharing provisions will be developed for inclusion in the draft law.

Customer complaints to data holders or accredited requestors

213. The draft law requires that data holders and accredited requestors have an internal process to resolve customer complaints (see clause 43 of the draft law).

214. Customers whose complaints are not resolved during the internal process should have the option of taking their complaint to an independent external dispute resolution scheme. These schemes provide a low-cost way to resolve disputes when compared to taking court action. Unless special provision is made in our draft law, many unresolved complaints would only be able to be pursued through the courts.

215. Non-privacy complaints about breaches of the draft law's obligations will be dealt with by existing industry dispute resolution schemes within the designated sector. For example, in the banking sector a non-privacy complaint about a bank's regulated data services would

[34] Breaches may include but are not limited to the collection of information without a lawful purpose (IPP 1), failure to take reasonable steps to make an individual aware of key information about collection (IPP 3), or inadequate measures around the storage or security of information (IPP 5) ***https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23342.html***.

be considered by the Banking Ombudsman, if it was not able to be resolved using the bank's internal complaint process.

216. This approach is preferred over establishing a dedicated new dispute resolution scheme for regulated data services. It will avoid complexity and be easier for customers to navigate.

217. However, some accredited requestors may not have existing obligations to be members of an industry dispute resolution scheme. To ensure all customers have access to independent dispute resolution services, we consider that a similar approach to the Australian CDR[35] could be given effect through regulations, during the designation process. Both data holders and accredited requestors would be required to be a member of the relevant industry dispute resolution scheme.

218. This approach would make it easier for customers to navigate and ensure consistent and fair options for redress. However, it would impose additional costs on accredited requestors and data holders to be members of dispute resolution schemes and may, depending on the number of complaints, require upskilling and resourcing for the relevant industry dispute resolution schemes.

219. In cases where it is inappropriate to require data holders and accredited requestors to be members of an industry dispute resolution scheme, we consider that the Disputes Tribunal[36] could be a built-in back stop in the draft law. This reflects that complaints about non-privacy matters under the draft law will often also be actionable under other legislation, such as the Consumer Guarantees Act and the Fair Trading Act, or under contract, where the Disputes Tribunal has existing jurisdiction.

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?

Powers, penalties and liability

220. MBIE has a compliance and enforcement function. Where breaches relate to personal information, the Privacy Commissioner and Human Rights Review Tribunal also have a compliance and enforcement remit under the Privacy Act.

[35] Under rule 6.2. of the Australian Competition and Consumer (Consumer Data Right) Rules 2020 data holders and accredited persons are required to be members of recognised external dispute resolution scheme in relation to CDR consumer complaints.

[36] See ***https://www.disputestribunal.govt.nz/about-2/*** for more information about the Disputes Tribunal.

221. The draft law will include a range of enforcement options, including infringement offences, compensation orders, pecuniary penalties and criminal offences. These are outlined in the table below and will be drafted after the main obligations and protections are finalised.

Regulator	Liability tier	Penalty	Breach
MBIE	Tier 1	Infringement notice of up to **$20,000**. Infringement offence of up to **$50,000**.	Failure to maintain transaction records. Breach of notification or disclosure requirements (eg notification about how customers make a complaint, notification that transfer of data is complete).
	Tier 2	For a body corporate, a pecuniary penalty of up to **$600,000**. For an individual, a pecuniary penalty of up to **$200,000**. Compensation orders awarded through civil action.	Failure to maintain transaction records. Breach of notification or disclosure requirements (eg notification about how customers make a complaint, notification that transfer of data is complete).
	Tier 3	For a body corporate, a pecuniary penalty of up to **$2,500,000**. For an individual, a pecuniary penalty of up to **$500,000.** Compensation orders awarded through civil action.	Data holder fails to provide a CDR service to customers and accredited persons. A person misleads or deceives another person into believing either that a person is a CDR customer for CDR data, or a person is making a valid request for the disclosure of CDR data.
	Tier 4	For a body corporate, punishable on conviction by a fine of no more than **$5,000,000** or either: • if it can be readily ascertained that the contravention occurred in the course of producing a commercial gain, **three times the value of any commercial gain** resulting from the	A person knowingly/intentionally/recklessly misleads or deceives another person into believing either that a person is a CDR customer for CDR data, or a person making a valid request for the disclosure of CDR data. A person fraudulently holds out that they are an accredited person (or particular type of accredited person).

Regulator	Liability tier	Penalty	Breach
		contravention, or • if the commercial gain cannot readily be ascertained, **10% of the turnover** of the person and its interconnected bodies corporate in each accounting period in which the contravention occurred. For an individual, punishable on conviction by **imprisonment** of not more than **5 years**, a fine of up to **$1,000,000**, or both.	

222. For contraventions of civil penalty provisions, we propose an approach to liability similar to that used in Australia. In Australia, a person who suffers loss or damage by conduct which contravenes a civil penalty provision may recover the amount of loss or damage by action against that person (or any other person involved in the contravention).[37]

223. The draft law does not include a provision equivalent to section 56GC of the Australian Competition and Consumer Act. This provides protection from civil and criminal liability where an entity complied with the Act, in good faith. We do not consider this provision to be necessary as compliance with an Act should not, as a matter of law, create liability.

[37] See section 82 of the Australian Competition and Consumer Act.

Acronyms and Glossary

Accreditation	Proof that a service or provider meets the trust criteria under the draft law and future regulations.
Accredited requestor	An entity which is accredited under the draft law to request data from a data holder, or request actions by the data holder. While other entities (who are not accredited) can request data or actions, data holders do not have to respond to these. Data holders are only required to respond to a request when the request comes from an accredited requestor and otherwise complies with the safeguards.
Action request	A request from a customer (or an accredited requestor on behalf of a customer), that a data holder perform an action. This could be making payments, or updating information. Sometimes referred to as 'write access'.
API	Application Programming Interface
Breach	Not acting in accordance with the draft law, or regulations or standards under it.
CDR	Consumer Data Right
Consent	Customer authorisation for an entity to access data or perform an action on their behalf. A customer may revoke or withdraw consent at any time.
Consumer data right	A legal framework that requires businesses that hold data (data holders) to share prescribed data that they hold about customers (customer data) with trusted third parties (accredited requestors) with the consent of the customer.
Customer	A person – whether individual or entity – that acquires goods or services from a data holder.
Customer data	Data relating to a particular customer, eg account histories, transaction data, product usage. For the purposes of the draft law, customer data is only part of the regime where that type of data has been designated and/or the data holder has been designated.
Data holder	An entity that holds data (or is capable of giving effect to an action) to which the consumer data right applies. Only designated entities holding designated data are considered data holders under the draft law.
Designation	The process of choosing a sector and set of product data and customer data to be brought into the regulated data system established by the draft law.
DISTF Act	Digital Identity Services Trust Framework Act 2023
Draft law	The Customer and Product Data Bill
Fintech	Financial technology

IPP	Information Privacy Principle. The Privacy Act sets thirteen privacy principles to govern how businesses and organisations should collect, handle and use personal information.
MBIE	Ministry of Business, Innovation and Employment
Regulated entities	Data holders and accredited requestors.

How to have your say

Submissions process and timeline

The Ministry of Business, Innovation and Employment (MBIE) seeks written submissions on the issues raised in this document by 5pm on **Monday, 24 July 2023**.

The purpose of this consultation is to seek your feedback on whether the proposed drafting achieves the policy intent and is workable in practice. There may be some instances where the draft provisions may not adequately account for the variety of situations which occur in practice. Where that is the case, we encourage feedback on suggested alternatives.

Your submission may respond to any or all of these issues. Where possible, please include evidence to support your views, for example references to independent research, facts and figures, or relevant examples.

Please use the submission template provided at: ***https://www.mbie.govt.nz/have-your-say/seeking-feedback-on-the-customer-and-product-data-bill-consumer-data-right/***. This will help us to collate submissions and ensure that your views are fully considered. Please also include your name and (if applicable) the name of your organisation in your submission.

Please include your contact details in the cover letter or email accompanying your submission.

You can make your submission by:

- sending your submission as a Microsoft Word document to ***consumerdataright@mbie.govt.nz***.
- mailing your submission to:

  Consumer Policy Team
  Building, Resources and Markets
  Ministry of Business, Innovation & Employment
  PO Box 1473
  Wellington 6140
  New Zealand

Please direct any questions that you have in relation to the submissions process to ***consumerdataright@mbie.govt.nz***.

Use of information

The information provided in submissions will be used to inform MBIE's policy development process and will inform advice to Ministers on the CDR. We may contact submitters directly if we require clarification of any matters in submissions.

Release of information

MBIE intends to upload PDF copies of submissions received to MBIE's website at www.mbie.govt.nz. MBIE will consider you to have consented to uploading by making a submission, unless you clearly specify otherwise in your submission.

Personal contact details will be removed before publication.

Submissions can be published anonymously upon request.

If your submission contains any information that is confidential or you otherwise wish us not to publish, please:

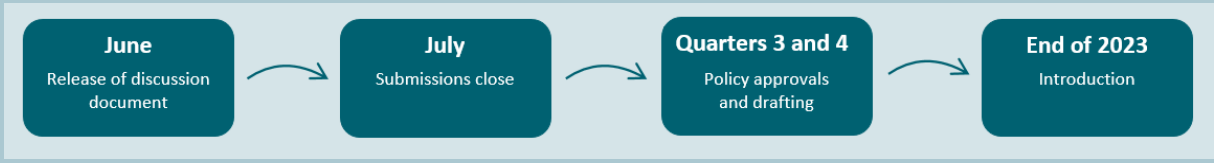
- indicate this on the front of the submission, with any confidential information clearly marked within the text
- provide a separate version excluding the relevant information for publication on our website.

Submissions remain subject to request under the Official Information Act 1982. Please set out clearly in the cover letter or e-mail accompanying your submission if you have any objection to the release of any information in the submission, and in particular, which parts you consider should be withheld, together with the reasons for withholding the information. MBIE will take such objections into account and will consult with submitters when responding to requests under the Official Information Act 1982.

Next steps

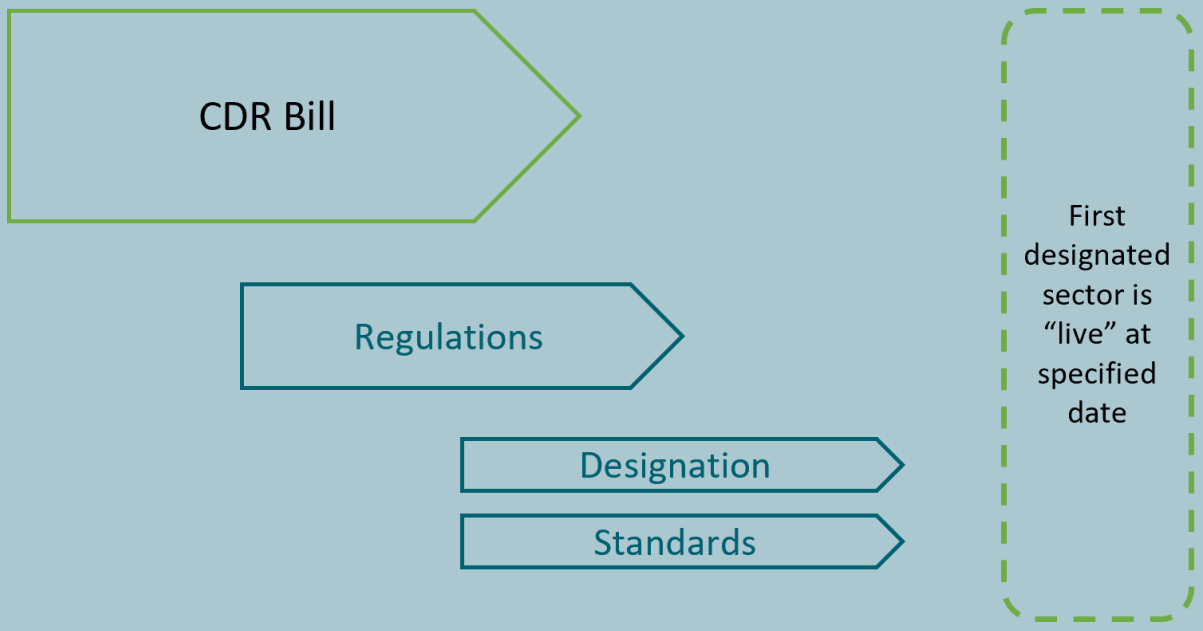
Following the close of submissions officials will review the feedback and use it to make recommendations to the Minister of Commerce and Consumer Affairs of any changes required to the exposure draft Customer and Product Data Bill.

The Government aims to introduce legislation to the House of Representatives to establish a CDR framework by the end of 2023. The anticipated timelines for this work are set out below:



Once introduced to Parliament, the normal Parliamentary process for the passage of legislation will begin. This will include a select committee process which will provide a further opportunity for public submissions on the Bill.

Engagement on regulations and designation can begin in parallel however these can only be finalised and made once the Bill has passed.



All previously published material relating to this work can be found at: ***http://www.mbie.govt.nz/CDR***.