Departmental Disclosure Statement

Customer and Product Data Bill

The departmental disclosure statement for a government Bill seeks to bring together in one place a range of information to support and enhance the Parliamentary and public scrutiny of that Bill.

It identifies:

- the general policy intent of the Bill and other background policy material;
- some of the key quality assurance products and processes used to develop and test the content of the Bill;
- the presence of certain significant powers or features in the Bill that might be of particular Parliamentary or public interest and warrant an explanation.

This disclosure statement was prepared by the Ministry of Business, Innovation, and Employment.

The Ministry of Business, Innovation, and Employment that, to the best of its knowledge and understanding, the information provided is complete and accurate at the date of finalisation below.

13 May 2024.

Contents

Contents....2
Part One: General Policy Statement....3
Part Two: Background Material and Policy Information....5
Part Three: Testing of Legislative Content....8
Part Four: Significant Legislative Features....11
Appendix One: Further Information Relating to Part Three....13

Part One: General Policy Statement

The purpose of the Bill is to establish an economy-wide framework to enable greater access to, and sharing of, customer and product data between businesses. This is commonly referred to as a "consumer data right". The intention is to give customers (including both individuals and entities) in designated sectors greater control over how their customer data is accessed and used, promote innovation and facilitate competition, and facilitate secure, standardised, and efficient data services. The Bill will –

- give customers greater control over their data. This will make it easier for them to shop around and switch providers for services such as banking, electricity, and telecommunications, and allow them to have greater trust that their data is secure and only shared for their benefit, and with their knowledge and authorisation; and
- enable innovation as it will facilitate the introduction of new products and services that are only viable when customer data and product data is shared; and
- facilitate competition by creating new opportunities for new entrants to break into established markets, and remove barriers that are preventing customers from being able to access and share their data, including a lack of incentives for data holders to transfer data to third parties; and
- enable efficient data services, through accreditation of data recipients that removes the need for separate due diligence and high costs in negotiating bilateral agreements; and
- provide a standardised and secure way for customers to access and use their customer data, to access product data, and for actions to be performed on their behalf, which removes the need for bespoke interfaces or workarounds.

The Bill aims to achieve this by requiring businesses that hold designated customer data (data holders) to provide that data to the customer and, with the customer's authorisation, to accredited third parties. The Bill will require data holders to perform actions in response to electronic requests from customers and accredited third parties (with customer authorisation), such as opening accounts, making payments, or changing customer plans. The Bill will also require product data, which is data about a data holder's goods and services, to be made available electronically on request.

To protect the privacy of individuals and confidentiality of customer information, the Bill provides privacy safeguards. The privacy safeguards in the Bill will complement existing protections in the Privacy Act 2020, which will continue to apply except where the Bill says otherwise. This will allow customers to derive value from their data without compromising their privacy or data security. The Bill sets out a framework for the accreditation of third parties. Only accredited third parties with the authorisation of customers will be able to request customer data from data holders or request actions on a customer's behalf. The chief executive of the Ministry of Business, Innovation, and Employment (the chief executive) will be responsible for the accreditation of third parties. Accreditation is intended to check and certify that accredited third parties are trustworthy, competent, and secure. Once accredited, third parties will be able to request and receive data from data holders electronically, securely, and in a standard machine-readable format.

The Bill provides for a full range of compliance and enforcement powers, from powers aimed at supporting willing compliance to powers aimed at detecting and penalising non-compliance. The Bill provides that the chief executive enforces the Bill, alongside the Privacy Commissioner who will continue to have investigation, guidance, enforcement, and redress powers over obligations in the Privacy Act 2020.

The Bill will be applied to 1 sector at a time via a designation process. Applying the same legislative framework to different sectors will improve certainty and predictability for businesses operating in multiple markets. The interoperability among different sectors enabled by a consistent framework is intended to support further innovation.

The Minister of Commerce and Consumer Affairs is responsible for recommending the designation of individual markets, industries, and sectors to which the Bill will apply. The designation will specify the type of data and functionality that is required to be made available to accredited requestors, customers, or both, and will be accompanied by rules and standards that govern the transfer of that data. To achieve this, the Bill delegates a significant amount of detail

to secondary legislation, which enables flexibility to adjust to different sectors of the economy. The first sector to be designated will be the banking sector.

The Bill has been designed in response to submissions on the Ministry of Business, Innovation, and Employment's 2020 discussion document on establishing a consumer data right in New Zealand, which identified issues with current data portability settings. Australia, the United Kingdom, and Europe have introduced open banking or consumer data right regimes. Australia takes a similar sector-based approach and has applied their consumer data right to the banking and energy sectors.

It is intended that the Bill should not prevent industry-led options from being progressed in parallel to regulatory intervention and where possible, should seek to leverage that work, for example by making use of existing industry standards, technologies, and expertise.

Part Two: Background Material and Policy Information

Published reviews or evaluations

2.1. Are there any publicly available inquiry, review or evaluation reports that have informed, or are relevant to, the policy to be given effect by this Bill?	YES
Discussion document: Options for establishing a consumer data right in New Zealand, Ministry of Business, Innovation and Employment, 5 August 2020 https://www.mbie.govt.nz/dmsdocument/11625-discussion-document-options-for-establishing-a-consumer-data-right-in-new-zealand *New Zealand firms:* Reaching for the frontier, Productivity Commission, April 2021 https://www.productivity.govt.nz/assets/Documents/Final-report-Frontier-firms.pdf *Discussion document:* Unlocking value from our customer data, Ministry of Business, Innovation and Employment, 22 June 2023 https://www.mbie.govt.nz/dmsdocument/26877-unlocking-value-from-our-customer-data-bill-discussion-document-pdf	

Relevant international treaties

2.2. Does this Bill seek to give effect to New Zealand action in relation to an international treaty?	NO

Regulatory impact analysis

2.3. Were any regulatory impact statements provided to inform the policy decisions that led to this Bill?	YES
Regulatory Impact Statement: Establishing a Consumer Data Right, Ministry of Business, Innovation and Employment, Published 9 July 2021. A copy of the RIS is available at: https://www.mbie.govt.nz/dmsdocument/15545-regulatory-impact-statement-establishing-a-consumer-data-right-proactiverelease-pdf Supplementary Regulatory Impact Statement: Further decisions on establishing a consumer data right, Ministry of Business, Innovation and Employment, 19 December 2022. A copy of the RIS is available at: https://www.mbie.govt.nz/dmsdocument/25845-supplementary-regulatory-impact-statement-further-decisions-on-establishing-a-consumer-data-right-proactiverelease-pdf	

2.3.1. If so, did the RIA Team in the Treasury provide an independent opinion on the quality of any of these regulatory impact statements?	YES
A quality assurance panel with members from the Treasury's Regulatory Impact Analysis Team and the Ministry of Business, Innovation and Employment (MBIE) reviewed the first Regulatory Impact Statement (RIS) "Establishing a consumer data right" finalised by MBIE on 23 June 2021. The review panel's opinion is set out in the Cabinet paper that this RIS accompanied: https://www.mbie.govt.nz/dmsdocument/15536-establishing-a-consumer-data-right-proactiverelease-pdf. The second RIS "Supplementary Regulatory Impact Statement: Further decisions on establishing a consumer data right" did not meet the threshold for receiving an independent opinion on the quality of the RIS from the RIA Team based in the Treasury.	

2.3.2. Are there aspects of the policy to be given effect by this Bill that were not addressed by, or that now vary materially from, the policy options analysed in these regulatory impact statements?	**NO**

Extent of impact analysis available

2.4. Has further impact analysis become available for any aspects of the policy to be given effect by this Bill?	**NO**

2.5. For the policy to be given effect by this Bill, is there analysis available on:	
(a) the size of the potential costs and benefits?	**YES**
(b) the potential for any group of persons to suffer a substantial unavoidable loss of income or wealth?	**NO**
The RIS identifies a range of benefits for customers and businesses from enabling greater data portability.[1] For consumers these include improvements to the range and quality of goods and services, greater choice and convenience, easier switching between providers and plans, and more control over their data. For businesses, these include opportunities to introduce new products and improve productivity. It is difficult to estimate the overall monetary value of benefits to customers or businesses as this is contingent upon a number of factors, including the market or sectors that are designated, the scope of any designations, the rate of innovations that rely on the transfer of data, and overall participation. However, research in New Zealand and the United Kingdom suggests that improving switching alone could allow individual customers to save significant sums each year by moving to alternative bank accounts, and electricity or mobile plan providers that better suit their needs.[2] Businesses within a designated sector would be required to put in place systems and processes that enable data to be shared in a machine-readable format. The extent of these costs will vary depending on the size of the market, the types of data subject to the consumer data right, and whether businesses are already complying with other portability regimes. Those wishing to access to access data will incur costs associated with obtaining accreditation. The cost of accreditation may be greater for smaller providers or new entrants, who are less likely than larger providers to have already made adequate investment in infrastructure to handle and protect data. Government will incur indicative costs of approximately $10 million to $19 million per year, however, the amount will depend on how its rulemaking, enforcement, accreditation and registry functions are implemented.	

2.6. For the policy to be given effect by this Bill, are the potential costs or benefits likely to be impacted by:	
(a) the level of effective compliance or non-compliance with applicable obligations or standards?	**YES**

[1] https://www.mbie.govt.nz/dmsdocument/15545-regulatory-impact-statement-establishing-a-consumer-data-right-proactiverelease-pdf
[2] https://www.mbie.govt.nz/dmsdocument/6932-electricity-price-review-final-report; https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf

(b) the nature and level of regulator effort put into encouraging or securing compliance?	YES
Benefits will only be realised to the extent that data holders comply with core obligations under the Bill to implement electronic systems to give effect to requests for data and actions. However, the Bill provides MBIE with a full range of compliance, monitoring and enforcement powers, and given this and the nature of the regulated population (primarily larger firms that hold significant amounts of customer data) we do not anticipate that there will be a high rate of non-compliance.	

Part Three: Testing of Legislative Content

Consistency with New Zealand's international obligations

3.1. What steps have been taken to determine whether the policy to be given effect by this Bill is consistent with New Zealand's international obligations?
MFAT has been consulted on the content of the Bill.

Consistency with the government's Treaty of Waitangi obligations

3.2. What steps have been taken to determine whether the policy to be given effect by this Bill is consistent with the principles of the Treaty of Waitangi?
MBIE officials have considered findings by the Waitangi Tribunal in relation to Māori data[3], consulted with Māori, including both individuals and iwi, Māori data experts, Māori data service providers, and sought and considered advice from the Treaty Provisions Oversight Group. The Bill ensures that the views of iwi/Māori are considered when setting the rules in secondary legislation for how and what data is accessed and what protections there should be around how this data is accessed. This will help ensure the Bill supports uses of data by hapū and iwi are, and there are appropriate protections around use of data, which is consistent with treating Māori data as taonga.

Consistency with the New Zealand Bill of Rights Act 1990

3.3. Has advice been provided to the Attorney-General on whether any provisions of this Bill appear to limit any of the rights and freedoms affirmed in the New Zealand Bill of Rights Act 1990?	**YES**
Advice provided to the Attorney-General by the Ministry of Justice, or a section 7 report of the Attorney-General, is generally expected to be available on the Ministry of Justice's website upon introduction of a Bill. Such advice, or reports, will be accessible on the Ministry's website at https://www.justice.govt.nz/justice-sector-policy/constitutional-issues-and-human-rights/the-bill-of-rights-act/advice/.	

Offences, penalties and court jurisdictions

3.4. Does this Bill create, amend, or remove:	
(a) offences or penalties (including infringement offences or penalties and civil pecuniary penalty regimes)?	**YES**
(b) the jurisdiction of a court or tribunal (including rights to judicial review or rights of appeal)?	**YES**
The Bill's offences and penalties regime and jurisdiction of a court or tribunal is included in Appendix One.	

[3] In the Waitangi Tribunal's report on the Comprehensive and Progressive Agreement for Trans-Pacific Partnership the Waitangi Tribunal concluded that Māori data may be a component of mātauranga Māori, and may in combination with related data be, or have the potential to be, taonga.

3.4.1. Was the Ministry of Justice consulted about these provisions?	YES
The Ministry of Justice was consulted on the jurisdiction of a court or tribunal clauses in the Bill and was comfortable with the approach taken. The Ministry was consulted on clauses in the Bill relating to the offences and penalties regime and defences. Feedback from the Ministry on the penalties and offences regime and defences (and our responses to their feedback) is included in Appendix One.	

Privacy issues

3.5. Does this Bill create, amend or remove any provisions relating to the collection, storage, access to, correction of, use or disclosure of personal information?	YES
Much of the Bill relates to access to customer data, including personal information, by customers and authorised third parties. These include obligations in clauses 14–16, 27, 38–44, and regulations and standards made in accordance with clauses 28, 31 and 33. The Bill also contains provisions setting out how information privacy principles under the Privacy Act 2020 apply to requests and storage and security in clauses 52 and 53. Clause 52 specifies that requests for customer data are not IPP 6 requests and, accordingly, nothing in part 1 of Part 4 of the Privacy Act 2020 applies. Notwithstanding, for the purposes of Parts 5 and 6 of the Privacy Act, an action of the data holder must be treated as being an interference with the Privacy of an individual if the data holder contravenes the provisions relating to requests for customer data. Clause 53 provides that certain contraventions relating to storage and security (clause 38(3) or 44(2) must be treated as breaching information privacy principle 5 set out in section 22 of the Privacy Act 2020 for the purposes of Parts 5 and 6 of that Act. In line with the purpose of the Bill, these provisions seek to enhance the access that customers otherwise have to their personal information, by facilitating secure, standardised, and efficient data services.	

3.5.1. Was the Privacy Commissioner consulted about these provisions?	YES
The Privacy Commissioner has been consulted about these provisions. See Appendix Three for the Privacy Commissioner's feedback on these provisions.	

External consultation

3.6. Has there been any external consultation on the policy to be given effect by this Bill, or on a draft of this Bill?	YES
There have been two rounds of public consultation: on the policy underlying the Bill and on a draft of the Bill. These have informed the policy design in the Bill. On 29 July 2020 Cabinet agreed to release a discussion document seeking feedback on options for establishing a consumer data right in New Zealand [DEV-20-MIN-0155]. Overall, submitters agreed that New Zealand needs a consumer data right to realise the economic and consumer welfare benefits by removing the barriers that are preventing widespread data portability. There was broad support among submitters for the Bill's sectoral-designation model, similar to that in Australia. There were differing views from submitters on issues such as the extent of any privacy protections that the Bill should provide in addition to the Privacy Act 2020 On 19 June 2023 Cabinet agreed to release of the draft Customer and Product Data Bill and accompanying discussion document [CAB-23-MIN-0425]. Submitters were able to provide feedback through a variety of different means, including through formal written submissions, online webinars and workshops, and a consumer-focused survey. We received 940 responses to the consumer-focused survey. We also had more than 330 participants attend our online webinars, our online workshop in collaboration with industry, and three hui with iwi and hapū representatives, and Māori data experts and practitioners. Submitters broadly supported the approach and objectives of the draft Bill. However, they provided feedback on a range of specific issues, including issues relevant to the draft Bill, issues for future regulations and standards, and operational and implementation considerations.	

Other testing of proposals

3.7. Have the policy details to be given effect by this Bill been otherwise tested or assessed in any way to ensure the Bill's provisions are workable and complete?	YES
MBIE has engaged with international counterparts, including the Australian Treasury and the Australian Competition and Consumer Commission about their legislative regimes and the Bill.	

Part Four: Significant Legislative Features

Compulsory acquisition of private property

4.1. Does this Bill contain any provisions that could result in the compulsory acquisition of private property?	NO

Charges in the nature of a tax

4.2. Does this Bill create or amend a power to impose a fee, levy or charge in the nature of a tax?	YES

Clauses 127 and 128 provide for prescribed fees and charges in connection with the performance or exercise of any function, power, or duty of the chief executive under the Bill.

Clause 129 allows for levies to be prescribed for data holders and accredited requestors to cover:

a) a portion of the costs of the chief executive of MBIE when performing or exercising their functions, powers, and duties under the Bill
b) a portion of the costs of the Privacy Commissioner in performing or exercising their functions, powers, and duties under the Privacy Act 2020 in connection with a contravention referred to in section 52(3) or 53(1)
c) to cover the costs of collecting the levy money.

This may be preferred to recovering those costs from general taxation where the benefits of the Bill are received by a limited group (e.g. data holders, accredited requestors and customers in a particular designated sectors).

As well as restricting levies to regulator costs incurred under the Bill, safeguards include a requirement on the Minister to consult on any proposed levies (clause 131), an ability for regulations to provide for refunds of any over-recovery of actual costs (clause 129(6)(d)).

Retrospective effect

4.3. Does this Bill affect rights, freedoms, or impose obligations, retrospectively?	NO

Strict liability or reversal of the usual burden of proof for offences

4.4. Does this Bill:	
(a) create or amend a strict or absolute liability offence?	YES
(b) reverse or modify the usual burden of proof for an offence or a civil pecuniary penalty proceeding?	NO

The Bill contains strict liability offences in clauses 30 (failing to comply with notice to test electronic system), and 58 (failing to comply with notice to supply information or produce documents). These offences are of a regulatory nature and are subject to a defence of reasonable excuse. Where a defendant points to evidence capable of amounting to a reasonable excuse, the burden is on the prosecution to prove the lack of any such excuse.

Civil or criminal immunity

4.5. Does this Bill create or amend a civil or criminal immunity for any person?	**NO**

Significant decision-making powers

4.6. Does this Bill create or amend a decision-making power to make a determination about a person's rights, obligations, or interests protected or recognised by law, and that could have a significant impact on those rights, obligations, or interests?	**NO**

Powers to make delegated legislation

4.7. Does this Bill create or amend a power to make delegated legislation that could amend an Act, define the meaning of a term in an Act, or grant an exemption from an Act or delegated legislation?	**YES**
Regulations can exempt persons from compliance with any requirement in the Act (clause 135). This is considered necessary to accommodate any unique circumstances in particular sectors of the economy, or particular participants, that may make compliance with specific provisions of the Bill unduly onerous or burdensome. Before recommending an exemption, the Minister must have regard to the purpose of the Act, and be satisfied that the extent of the exemption is not broader than is reasonably necessary to address the matters that gave rise to the exemption. There is also a requirement to publish a statement of reasons.	

4.8. Does this Bill create or amend any other powers to make delegated legislation?	**YES**
The Bill includes powers for the Minister to make regulations (clauses 97–100, 126-131), and for the chief executive of the administering Ministry to make technical standards (clauses 132-134). The Bill provides an enabling framework for a consumer data right, but individual sectors of the economy will be brought into the regime one at a time by regulations. This is necessary to ensure that the costs associated with the Bill are only incurred where there will be sufficient benefits. Different detailed requirements will need to be implemented in each sector, appropriate to the nature of the businesses, customer data and goods and services provided. In addition, the Bill's core duties rely on implementation of an electronic system, and the functionality that will be required to be provided by that system is technical in nature and subject to frequent updates. A number of safeguards for regulations are provided by clauses 98, 99, 126(2) and 131. These comprise considerations that the Minister must have regard to before recommending regulations, and consultation requirements. Safeguards are provided for standards made by the chief executive. Clause 134 requires consultation. Clause 133 requires the chief executive to comply with any requirements, limits and restrictions prescribed by the regulations.	

Any other unusual provisions or features

4.9. Does this Bill contain any provisions (other than those noted above) that are unusual or call for special comment?	**NO**

Appendix One: Further Information Relating to Part Three

Offences or penalties – question 3.4(a)

The Bill creates infringement offences for contravening:

a) a "specified data requirement" (clause 35)
b) requirements to keep records about data services (clauses 45 and 46)
c) requirement to have customer data, product data, and action performance policies (clause 58)
d) Annual reporting requirement (clause 114)

Infringement offences create liability for a fee of $20,000, or a fine imposed by the court of $50,000.

The Bill creates liability for a civil pecuniary penalty of up to:

a) $200,000 for an individual and up to $600,000 for a body corporate, for the contravention of a section listed in clause 75:
b) $500,000 for an individual and up to $2,500,000 for a body corporate, for the contravention of a section listed in clause 74.

Clause 43 creates an offence for a person to knowingly make a request they are not permitted to make. On conviction, the offence brings liability to imprisonment for a term of up to 5 years and/or a fine of up to $1 million for an individual, or $5 million for a body corporate.

Clause 30 creates an offence for a data holder to refuse or fail, without reasonable excuse, to comply with a notice to test their electronic system or give a test report knowing it to be materially false or misleading. On conviction, an individual offender is liable to a fine of up to $100,000 and in any other case (such as a body corporate) $300,000.

Clause 58 creates an offence for refusing or failing, without reasonable excuse, to comply with a notice to supply or give documents or to supply information, or produce a document, knowing it to be materially false or misleading. On conviction, an individual offender is liable to a fine of up to $100,000 and in any other case (such as a body corporate) $300,000.

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

The jurisdiction of a court or tribunal – question 3.4(b)

The Bill includes clauses relating to the jurisdiction of a court or tribunal. Clause 93 provides that the High Court may hear and determine applications for orders, or for a court to exercise any other power under, under any provision of subpart 6, Part 4 and appeals arising from any proceeding in the District Court under this subpart. Clause 111 allows that a person may appeal to the High Court against a decision of the chief executive. Clause 94 allows the district court to hear and determine applications for orders, or for the court to exercise any other power under the provisions for compensatory orders and injunctions. Clause 95 allows the Disputes Tribunal to order compensation if the amount claimed does not exceed $30,000.

Offences, penalties, and court jurisdiction – was the Ministry of Justice Consulted about these provisions – question 3.4.1

The Ministry of Justice noted that:

a) the infringement fees and penalties were set quite high
b) offences in clauses 30 and 58 include two different types of conduct with different kinds of moral culpability: *refuses or fails* but both carry the same penalty

c) clause 43 could capture a range of contraventions and wondered whether a more graduated approach relative to the level of harm was not taken
d) the Bill provides that the defence in clause 91(b) does not apply to clause 27 or clause 28 (to the extent that it requires a data holder to comply with CPD reliability and availability requirement, and queried whether we had considered applying it to these clauses
e) including 92(2)(c) as part of the defence for contraventions due to technical fault is relevant, however raised concern about the potential for double jeopardy.

Low-level fines can effectively become a cost of doing business and therefore have relatively minor deterrent effect in a commercial context. The proposed penalty level for infringement fees is aimed at ensuring there is sufficient commercial deterrent against contravening conduct.

The offences in clauses 30 and 58 relate to frustration of the exercise of a regulator's power. It is intended to be a strict liability offence if they fail (via negligence or wilful refusal) to comply. There are equivalent offences in other Acts such as in s183(1)(a) Grocery Industry Competition 2023, s250(2) Civil Aviation Act 2023, s100(1) Deposit Takers Act 2023, s61 of the FMA Act 2011 which also refer to "refuses or fails" (and don't have different maximum tariffs for fails vs refuses).

Clause 43 can capture a range of contraventions and levels of harm. The Court will likely exercise discretion in applying the penalties according to (inter alia) the severity of harm. A graduated approach has not been adopted, however, because given the breadth of designated sectors, information, and actions the regime can cover it is not practicable to demarcate graduations of contraventions.

Clause 91(b) does not apply to clauses 27 or 28 (to the extent that it requires data holders to comply with CPD reliability and availability requirements) because data holders operating electronic systems, as required in clause 27, is essential to the consumer data right functioning. Developing these electronic systems will require significant investment from data holders and therefore there is stronger incentive for non-compliance. We are concerned that the defences may allow data holders to escape deadlines for implementation of the required electronic systems by asserting that they were missed due to difficulties with third party IT providers, IT skill shortages, etc. We therefore consider that disapplying this aspect of the defence is necessary to ensure that the deadline can be effectively enforced, and that the consumer data right regime is successful.

The Bill does not allow for double jeopardy. Clause 89 of the Bill provides that only one pecuniary penalty order may be made for the same conduct. This aligns with paragraph 26.7 of the 2021 Legislation Guidelines issued by the Legislation Design and Advisory Committee.

Was the Privacy Commissioner Consulted on these provisions – question 3.5.1

The Privacy Commissioner has stated that:

a) a timeliness requirement will be necessary to ensure there are clear parameters set for the Privacy Commissioner to find an interference with Privacy, and therefore suggested inserting a timeliness requirement in either clause 14 or 52
b) the way that clause 51 is currently drafted means that if an individual has an issue with the way their personal information has been dealt with, they could either go through the dispute resolution scheme or go to the Commissioner. The Commissioner notes that this would align with the status quo, and that they are happy with this approach. The Commissioner queried whether this was intentional.
c) clause 44(3)(b) requires that data holders need to verify the identity of the requestor, but notes that 'verify' is not defined in the Bill.

Data standards will require data holders' systems to respond to API requests for data within milliseconds. If the system does not respond essentially immediately, then it will not be possible to provide the data at all as required, because the recipient will no longer be connected to the data holder's system, and therefore clause 14 or 15 will be breached. Therefore, we do not consider a timeliness requirement is necessary.

The drafting of clause 51 intentionally allows for either use of the dispute resolution scheme or the Privacy Commissioner (to the extent the complaint relates to personal information).

Verify has its ordinary meaning 'make sure or demonstrate that (something) is true, accurate, or justified'. However, in practice, the specific steps required to verify will be prescribed by standards under clause 44(3).