Customer and Product Data Bill

Government Bill

Explanatory note

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 its 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.

Departmental disclosure statement

The Ministry of Business, Innovation, and Employment is required to prepare a disclosure statement to assist with the scrutiny of this Bill. The disclosure statement provides access to information about the policy development of the Bill and identifies any significant or unusual legislative features of the Bill.

A copy of the statement can be found at http://legislation.govt.nz/disclosure.aspx?type=bill&subtype=government&year=2024&no=44

Regulatory impact statements

The Ministry of Business, Innovation, and Employment produced regulatory impact statements on 23 June 2021 and 4 May 2022 to help inform the main policy decisions taken by the Government relating to the contents of this Bill.

Copies of these regulatory impact statements can be found at—

- https://www.mbie.govt.nz/dmsdocument/15545-regulatory-impact-statement-establishing-a-consumer-data-right-proactiverelease-pdf
- https://www.mbie.govt.nz/dmsdocument/25845-supplementary-regulatory-impact-statement-further-decisions-on-establishing-a-consumer-data-right-proactiverelease-pdf
- https://treasury.govt.nz/publications/informationreleases/ris

Clause by clause analysis

Clause 1 is the Title clause.

Clause 2 provides for the Bill to come into force on the day after Royal assent.

Part 1
Preliminary provisions

Purpose

Clause 3 sets out the overall purpose of the Bill, which is to establish a framework to—

- realise the value of certain data; and
- promote competition and innovation; and
- facilitate secure, standardised, and efficient data services in certain sectors.

The Bill achieves this purpose by improving the ability of customers to access and use data held about them by participants in those sectors, improving access to data about products, and standardising safeguards, controls, standards, and functionality in connection with data services.

Overview

Clause 4 sets out an overview of the Bill.

Interpretation

Clauses 5 to 10 define various key terms used in the Bill, including—

- data holder. This is a person of a class specified in regulations made under the Bill that holds customer data or product data of a kind that is designated in those regulations (**designation regulations**):
- accredited requestor. This is a person that is accredited under *subpart 3 of Part 5*:
- customer. This is a person who acquires, or is seeking to acquire, goods or services from a data holder. Customer data is data that is about an identifiable customer that is held by a data holder:
- regulated data service. This is the service of providing data, or performing an action, under *Part 2*:
- standards. Standards are made under *clause 132*.

Territorial application of Act

Clause 11 provides that the Bill applies to—

- New Zealand agencies; and
- overseas agencies in relation to conduct in the course of carrying on business in New Zealand.

Clause 11 is based on section 4 of the Privacy Act 2020.

Transitional, savings, and related provisions

Clause 12 relates to the transitional, savings, and related provisions set out in *Schedule 1*.

Act binds the Crown

Clause 13 provides for the Bill to bind the Crown. *See also clause 115*, which relates to Crown organisations being customers, data holders, or accredited requestors.

Part 2
Regulated data services

Subpart 1—Main obligations

Customer data

Clauses 14 and 15 require a data holder to provide data about a customer on the request of the customer or an accredited requestor. However, the following requirements must be met:

- the data must be designated by the regulations:
- the request must be valid under *clause 26* and made using an electronic system under *clause 27*:
- if the request is made by an accredited requestor, the data holder must check that the service is within the scope of an authorisation given by or on behalf of the customer (*see clause 38*, which requires the authorisation to be confirmed). In addition, the accredited requestor must be acting within the class of its accreditation and the data holder must verify the identity of the customer or secondary user who authorised the accredited requestor.

Clause 16 allows the data holder to refuse a request for data if, for example, disclosure would be likely to pose a serious threat to health or safety or the data holder reasonably believes that disclosure would have a materially adverse effect on the security, integrity, or stability of the data holder's information and communication technology systems. A data holder may also refuse a request in the circumstances prescribed in the regulations.

A data holder must refuse the request if it has reasonable grounds to believe that the request is made under the threat of physical or mental harm.

Clause 17 confirms that *clauses 14 and 15* do not prevent an individual from accessing their personal information on request under the Privacy Act 2020.

Designated actions

Clauses 18 and 19 require a data holder to perform an action relating to a customer on the request of the customer or an accredited requestor. However, the following requirements must be met:

- the action must be designated by the regulations:
- the action must be of a kind that the data holder would ordinarily perform in the course of its business:
- the request must be valid under *clause 26* and made using an electronic system under *clause 27*:
- if the request is made by an accredited requestor, the data holder must check that the service is within the scope of an authorisation given by or on behalf of the customer (*see clause 38*, which requires the authorisation to be confirmed).

In addition, the accredited requestor must be acting within the class of its accreditation and the data holder must verify the identity of the customer or secondary user who authorised the accredited requestor.

Clause 20 allows the data holder to refuse a request to perform an action if, for example, the data holder reasonably believes that performing the action would create a significant likelihood of serious financial harm to any person or have a materially adverse effect on the security, integrity, or stability of the data holder's information and communication technology systems. A data holder may also refuse a request in the circumstances prescribed in the regulations.

A data holder must refuse the request if it has reasonable grounds to believe that the request is made under the threat of physical or mental harm.

Joint customers

Clause 21 requires data holders and accredited requestors to deal with joint customers in accordance with requirements prescribed in the regulations. Joint customers may include, for example, joint holders of a bank account. The regulations may provide for when a request or an authorisation under the Bill may be made or given by joint customers individually or acting together.

Product data

Clause 22 requires a data holder to provide data about a product on the request of any person. However, the following requirements must be met:

- the data must be designated by the regulations:
- the request must be valid under *clause 26* and made using an electronic system under *clause 27*.

Clause 23 allows the data holder to refuse a request for data if, for example, the data holder reasonably believes that disclosure would have a materially adverse effect on the security, integrity, or stability of the data holder's information and communication technology systems. A data holder may also refuse a request in the circumstances prescribed in the regulations.

Subpart 2—Additional obligations

Secondary users

Clause 24 requires data holders and accredited requestors to deal with secondary users in accordance with requirements prescribed in the regulations. A secondary user is a person of a class specified in designation regulations (and, if required by the regulations, has been approved as a secondary user). For example, a director may be a secondary user for a customer that is a company. The regulations may provide for when a request or an authorisation under the Bill may be made or given by a secondary user on behalf of the customer.

Regulations may specify that a request or an authorisation under the Bill may be made or given by a customer only if it is made or given by a secondary user on their

behalf. *Clause 25* provides that a request made or an authorisation given in another manner is ineffective.

Valid requests

Clause 26 provides that a request is valid if the person making the request complies with the requirements provided for in the standards and the regulations.

Electronic system

Clauses 27 and 28 require a data holder to operate an electronic system for providing regulated data services with reasonable reliability. The system must comply with technical or performance requirements set out in the regulations and standards (for example, requirements relating to security, monitoring, and reporting).

Clause 29 allows the chief executive to issue a notice to a data holder requiring it to test its electronic system for the purpose of verifying that the system complies with technical or performance requirements.

A person commits an offence under *clause 30* if the person refuses or fails, without reasonable excuse, to comply with the notice or the person gives a report knowing it to be materially false or misleading. A person that commits the offence is liable to a fine not exceeding $100,000 in the case of an individual or $300,000 in any other case.

Requirements for requests, providing services, making information available, and dealing with data

Clauses 31 to 34 require a data holder or an accredited requestor to comply with a range of requirements specified in the regulations and standards, for example, requirements about—

- charges for regulated data services:
- making information available to customers and other persons:
- the manner in which data is provided and received (for example, a requirement to use an application programming interface (API)):
- how an accredited requestor must deal with the data.

Clause 35 provides for a contravention of certain disclosure requirements to be an infringement offence. Those requirements will be specified by the regulations or standards for the purposes of this clause. Generally speaking, the infringement offences will be for relatively straightforward and low-level contraventions. *See subpart 5 of Part 4*.

A person that contravenes other, more significant disclosure requirements may be liable to a pecuniary penalty and other civil liability consequences under *subpart 6 of Part 4*.

Part 3
Protections

Authorisation

Clauses 36 to 41 provide for matters relating to a customer (or secondary user) giving an authorisation to another person. In summary,—

- an authorisation is given if the customer (or secondary user) is reasonably informed about the matter, it is given expressly in the manner prescribed by the regulations and the standards, and it has not ended:
- before providing a regulated data service on the request of an accredited requestor, the data holder must check that the service is within the scope of the authorisation given by the customer (or secondary user):
- a data holder must have systems in place to enable an authorisation to be changed:
- an accredited requestor must comply with the duties in respect of authorisation that are prescribed by the regulations or standards. For example, duties relating to ensuring that the customer (or secondary user) is reasonably informed and how an authorisation may be obtained:
- a person must not require a customer to authorise a regulated data service as a condition for providing some other goods or service unless the data service is reasonably necessary to enable the person to provide the other goods or service.

Restriction on who may request regulated data service

Clause 42 provides that only customers, secondary users, and accredited requestors may request, or purport to request, regulated data services.

Clause 43 creates an offence for a person to knowingly make a request that they are not permitted to make. A person that commits the offence is liable,—

- in the case of an individual, to imprisonment for a term not exceeding 5 years or to a fine not exceeding $1 million (or both):
- in any other case, to a fine not exceeding $5 million.

Clause 44 requires a data holder to verify the identity of a person who makes a request for a regulated data service.

Record keeping

Clauses 45 and 46 require data holders and accredited requestors to maintain certain records.

Customer data, product data, and action performance policies

Clause 47 requires a data holder or an accredited requestor to maintain policies relating to customer data, product data, and action performance.

Clause 48 provides for a contravention of certain policy requirements to be an infringement offence. Those requirements will be specified by the regulations or standards for the purposes of this clause.

A person who contravenes other, more significant policy requirements may be liable to a pecuniary penalty and other civil liability consequences under *subpart 6 of Part 4*.

Complaints

Clauses 49 to 51—

- require a data holder or an accredited requestor to have a complaints process relating to its conduct in connection with regulated data services; and
- require a data holder or an accredited requestor to be a member of a dispute resolution scheme if a scheme has been prescribed by the regulations; and
- allow dispute resolution scheme rules to be modified to cover complaints about regulated data services.

Privacy Act 2020

Clause 52 provides that a request for data under the Bill (that involves personal information) is not a request under information privacy principle 6 (access to personal information) set out in section 22 of the Privacy Act 2020. This means that requirements under subpart 1 of Part 4 of that Act do not apply to the request. However, certain contraventions under this Bill are treated as an interference with the privacy of an individual for the purposes of Parts 5 and 6 of the Privacy Act 2020 (which relate to complaints, investigations, proceedings, notifiable privacy breaches, and compliance notices).

Clause 53 relates to various data storage and security requirements imposed under this Bill. Contraventions of those requirements under this Bill must be treated as breaching information privacy principle 5 (storage and security of personal information) set out in section 22 of the Privacy Act 2020. This means that the contraventions may involve an interference with the privacy of an individual for the purposes of Parts 5 and 6 of the Privacy Act 2020.

Part 4
Regulatory and enforcement matters

Subpart 1—Regulatory powers

This subpart allows the chief executive to issue a notice requiring a person to supply information or produce a document for inspection. The power can be used if the chief executive considers it necessary or desirable for the purposes of performing or exercising their functions, powers, or duties under the Bill.

A person required to supply information or produce documents has the same privileges as witnesses have in a proceeding before a court.

A person commits an offence if the person refuses or fails, without reasonable excuse, to comply with a notice or the person supplies information, or produces a document, knowing it to be materially false or misleading. A person that commits the offence is liable to a fine not exceeding $100,000 in the case of an individual or $300,000 in any other case.

Subpart 2—Duties to take remedial action

This subpart requires a data holder or an accredited requestor to take the steps prescribed by the regulations if—

- it contravenes a duty under this Bill; and
- a customer or some other data holder or accredited requestor suffers or is likely to suffer loss or damage.

The subpart does not limit—

- any other remedies a person may obtain; or
- the powers of the chief executive or a court in respect of the contravention.

Subpart 3—Prohibition against taking certain actions against customer

This subpart prevents a data holder or an accredited requestor from taking certain actions against a customer if a duty under this Bill has been contravened. A data holder or an accredited requestor may be prohibited from taking the action regardless of whether it is the data holder or accredited requestor in contravention.

The prohibition applies only in the circumstances prescribed in the regulations. The actions include imposing a financial penalty, enforcing a security interest, and enforcing a debt.

Subpart 4—Prohibition against holding out

This subpart prohibits a person from falsely holding out that the person, or another person,—

- is an accredited requestor; or
- is able to make certain requests, or provide certain goods or services, in connection with a regulated data service.

Subpart 5—Infringement offences

This subpart provides for the chief executive to issue an infringement notice to a person if the chief executive believes on reasonable grounds that the person is committing, or has committed, an infringement offence.

Various relatively minor contraventions of the Bill are identified as infringement offences, including certain disclosure requirements (*clause 35*), record-keeping requirements (*clauses 45 and 46*), certain requirements relating to policies (*clause 48*), and certain annual reporting requirements (*clause 114*).

The penalty for infringement offences under the Bill is—

- an infringement fee of $20,000; or
- a fine imposed by a court not exceeding $50,000.

Subpart 6—Civil liability

This subpart provides for civil remedies for contraventions of a wide range of duties under this Bill. The provisions for which there is civil liability are set out in *clauses 74(1) and 75(1)* (**civil liability provisions**).

Pecuniary penalty order

Clauses 73 to 76 provide for the High Court to impose a pecuniary penalty against a person who has contravened a civil liability provision, attempted a contravention, or been involved in a contravention. There are 2 tiers of penalties.

Tier 1 has maximum penalties of $500,000 for an individual or $2,500,000 in any other case. Tier 1 covers, for example, a data holder failing to operate an electronic system for providing regulated data services.

Tier 2 has maximum penalties of $200,000 for an individual or $600,000 in any other case. Tier 2 covers, for example,—

- a data holder failing to perform a regulated data service under *clauses 14 to 19 and 22*; and
- a data holder failing to maintain an electronic system that complies with prescribed technical or performance requirements; and
- a data holder or an accredited requestor failing to comply with prescribed requirements for requests, providing services, making available information, and dealing with data; and
- a data holder or an accredited requestor failing to comply with requirements about having a customer complaints process and being a member of a dispute resolution scheme; and
- a person breaching the holding out prohibition in *clause 64*.

In determining an appropriate pecuniary penalty, the court must have regard to all relevant matters. For example, the nature and extent of the relevant conduct and of the loss or damage caused by that conduct.

Declaration of contravention

Clauses 77 to 79 provide for the High Court to make a declaration of contravention in the course of a pecuniary penalty proceeding or if a person applies for a declaration. An applicant for compensation may rely on that declaration (they are not required to prove the contravention again in order to obtain compensation).

Compensatory orders

Clauses 80 and 81 provide for the court (or the Disputes Tribunal) to order compensation for a contravention of a civil liability provision.

Injunctions

Clauses 82 to 85 provide for the court to grant injunctions that—

- restrain a person from contravening a civil liability provision; or
- require a person to do something in order to ensure that the person complies with a civil liability provision.

Rules of procedure

Clause 86 provides for the rules of civil procedure and evidence to apply (including proof to the balance of probabilities standard).

Clause 87 requires a proceeding under this subpart to be commenced within 3 years after the relevant conduct was discovered or ought reasonably to have been discovered.

Relationship between proceedings and orders

Clauses 88 to 90 provide that a person may not be liable to—

- more than 1 pecuniary penalty order for the same conduct; or
- both a pecuniary penalty and a criminal penalty for the same conduct.

Defences

Clause 91 provides general defences for a person (**A**) in contravention of a civil liability provision if—

- the contravention was due to reasonable reliance on information supplied by another person; or
- the contravention was due to the act or default of another person, or to an accident, and A took reasonable precautions and exercised due diligence to avoid the contravention.

Clause 92 provides a defence for a data holder that is in contravention of certain provisions if the contravention is due to a technical fault in its electronic system and it took reasonable precautions and exercised due diligence to avoid the contravention.

Jurisdiction

Clauses 93 and 94 provide for the jurisdiction of the High Court and the District Court.

Clause 95 provides for the Disputes Tribunal to hear and determine applications for compensation under *clauses 80 and 81* if the amount claimed does not exceed $30,000.

Part 5
Administrative matters

Subpart 1—Chief executive's functions

This subpart provides for the chief executive's functions under this Bill. This includes acting as the regulator of regulated data services, including by—

- accrediting persons as accredited requestors; and
- issuing standards; and
- keeping the register of participants in the customer and product data system (the **register**); and
- monitoring compliance with and enforcing this Bill.

Subpart 2—Designation regulations

This subpart provides for designation regulations. The regulations designate the following:

- persons as data holders:
- data as designated customer data or designated product data in respect of which requests may be made:
- actions in respect of which requests may be made:
- classes of accreditation:
- classes of secondary users.

Before the designation regulations are made, the Minister of Commerce and Consumer Affairs must—

- have regard to certain matters, including the interests of customers, the likely costs and benefits for data holders, and likely benefits and risks in relation to the security, privacy, confidentiality, or other sensitivity of customer data and product data; and
- consult the Privacy Commissioner, persons who will be substantially affected, and 1 or more people who have expert knowledge of te ao Māori approaches to data.

Subpart 3—Accreditation of requestors

This subpart provides for the chief executive to accredit a person as an accredited requestor. The chief executive may accredit the person if they are satisfied that—

- an application is made in accordance with the regulations; and
- they know the applicant's identity; and
- the applicant, and its directors and senior managers, meet the criteria or other requirements prescribed by the regulations (if any); and

- if *clause 50* will apply, the applicant is, or will be, a member of a dispute resolution scheme.

The subpart provides for—

- applications to be made before designation regulations are fully in force; and
- the modification of accreditation (for example, to add or remove classes of accreditation); and
- the duration and renewal of accreditation; and
- the suspension or cancellation of accreditation if the requirements for accreditation are no longer met or the chief executive is satisfied that the accredited requestor has materially contravened a term or condition of the accreditation or any other requirement imposed under this Bill.

Subpart 4—Appeals

This subpart allows a person to appeal to the High Court against various decisions of the chief executive relating to accreditation, for example, a decision to decline an application for accreditation.

Subpart 5—Annual reporting by data holders and accredited requestors

This subpart requires a data holder or an accredited requestor to give an annual report to the chief executive. The report will include, for example, a summary of the complaints made about its conduct in connection with regulated data services.

Subpart 6—Crown organisations

This subpart provides that a Crown organisation may be a customer, a data holder, or an accredited requestor in its own right. The term Crown organisation includes Crown entities, government departments, and a range of other government-related organisations.

Subpart 7—Register

This subpart establishes the register of participants in the customer and product data system. The register will—

- enable a person to confirm whether any person is a data holder or an accredited requestor and to obtain information about those persons; and
- enable data holders and accredited requestors to access information about each other; and
- assist any person in the performance or exercise of the person's functions, powers, or duties under this Bill or any other legislation.

In summary,—

- persons that will become data holders when designation regulations come into force must provide certain information to the chief executive before those regulations come into force:

- any other data holder must provide certain information to the chief executive after the data holder becomes aware that it has become a data holder:
- the information that will be publicly available includes—
    - a data holder's or an accredited requestor's name and New Zealand Business Number; and
    - the designation regulations that are relevant to a data holder or an accredited requestor; and
    - how customers may complain about a data holder's or an accredited requestor's conduct; and
    - how customers may contact data holders or accredited requestors:
- other information that is not publicly available through the register may be available to data holders and accredited requestors.

Subpart 8—Information sharing

This subpart allows the chief executive to share information that they hold under this Bill with certain other people and agencies (for example, the Privacy Commissioner, the Commerce Commission, or the Ministry of Justice). The chief executive may impose conditions on providing information under the subpart (for example, to maintain the confidentiality of anything provided).

Subpart 9—Regulations, standards, and exemptions

Regulations

Clause 126 provides for regulations to be made for the purposes of the Bill, including—

- providing for anything that the Bill contemplates will or may be provided for by regulations; and
- prescribing, for the purposes of any provision of the Bill that requires a thing to be done in a prescribed manner, the manner in which the thing must be done; and
- prescribing matters relating to the register.

Different requirements may be prescribed by the regulations for different designated sectors, customer data, product data, or actions. The various matters that may be prescribed include—

- circumstances in which a request under *subpart 1 of Part 2* (a **request**) does not need to be complied with:
- requirements for how data holders and accredited requestors must deal with joint customers and secondary users:
- requirements relating to whether a request is valid:

- technical or performance requirements for the electronic system that a data holder must operate:
- requirements for data holders and accredited requestors to make information available to, for example, customers, the chief executive, or the public generally:
- requirements for how an authorisation may be given and how a data holder must check that a service is within the scope of an authorisation:
- duties an accredited requestor must comply with when obtaining an authorisation (for example, ensuring that the customer is reasonably informed):
- requirements for how regulated data services must be provided:
- requirements for identifying customers, accredited requestors, and secondary users:
- requirements relating to records:
- requirements for customer data, product data, and action performance policies:
- allowing the rules of dispute resolution schemes to be changed to provide for complaints about regulated data services:
- whether a breach of a storage and security requirement imposed under this Bill must be treated as breaching information privacy principle 5 under section 22 of the Privacy Act 2020:
- duties for a data holder or an accredited requestor to take steps to avoid, mitigate, or remedy loss or damage caused by its contravention:
- when a data holder or an accredited requestor may be prohibited from taking certain actions against a customer:
- criteria and requirements that must be met in order to be accredited as an accredited requestor.

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

Clauses 129 and 130 provide for levy regulations. The regulations may require data holders and accredited requestors to pay a prescribed levy to recover—

- a portion of the costs of the chief executive in performing or exercising their functions, powers, and duties under the Bill; and
- 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 certain contraventions of the Bill; and
- collection costs.

The Minister of Commerce and Consumer Affairs determines the size of the portion to be met by levies.

Clause 131 requires the Minister to consult certain persons and groups before recommending that regulations be made under the subpart.

Standards

Clause 132 authorises the chief executive to make standards for the purposes of the Bill. The standards may provide for anything that the Bill says must or may be provided for by the standards. This includes—

- circumstances in which a request under *subpart 1 of Part 2* (a **request**) does not need to be complied with:
- requirements relating to whether a request is valid:
- technical or performance requirements for the electronic system that a data holder must operate:
- requirements for data holders and accredited requestors to make information available to, for example, customers, the chief executive, or the public generally:
- requirements for data (including its format and quality and the manner in which data is provided and received):
- duties an accredited requestor must comply with when obtaining an authorisation (for example, ensuring that the customer is reasonably informed) and when dealing with data:
- requirements for identifying customers, accredited requestors, and secondary users:
- requirements for how regulated data services must be provided:
- requirements for customer data, product data, and action performance policies.

Clause 133 requires the chief executive to comply with requirements prescribed by the regulations relating to how standards are made and to be satisfied that the standards are consistent with any limits or restrictions prescribed by the regulations.

Clause 134 requires the chief executive to consult on proposed standards.

Exemptions

Clauses 135 and 136 provide for regulations to exempt (on terms and conditions, if any) classes of persons from any requirement under the Bill.

Before recommending exemption regulations, the Minister must have regard to the purpose of this Bill 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 regulations.

The Minister's reasons for making the recommendation (including why an exemption is appropriate) must be published together with the regulations.

Subpart 10—Miscellaneous

Clause 137 provides for the Bill to apply despite any provision to the contrary in any agreement.

Clause 138 protects the chief executive's warnings, reports, or other comments made under the Bill with qualified privilege under the Defamation Act 1992.

Clauses 139 and 140 provide for notices served for the purposes of *clause 29 or 54*.

Subpart 11—Consequential amendments

This subpart consequentially amends the Disputes Tribunal Act 1988, the Privacy Act 2020, and the Summary Proceedings Act 1957. In particular,—

- the Disputes Tribunal is given jurisdiction under *clause 95*:
- given the relationship of this Bill to the Privacy Act 2020 (*see clauses 52 and 53*), sections 75 and 208 of that Act are amended to allow the Privacy Commissioner to refer a complaint to, and to consult with, the chief executive.

Hon Andrew Bayly

Customer and Product Data Bill

Government Bill

Contents

		Page
1	Title	8
2	Commencement	8
	Part 1 **Preliminary provisions**	
	Purpose	
3	Purpose	8
	Overview	
4	Overview	8
	Interpretation	
5	Interpretation	9
6	Data holder	11
7	Accredited requestor	11
8	Customer, customer data, and designated customer data	12
9	Product, product data, and designated product data	12
10	Regulated data service	12
	Territorial application of Act	
11	Territorial application of Act	12
	Transitional, savings, and related provisions	
12	Transitional, savings, and related provisions	13
	Act binds the Crown	
13	Act binds the Crown	13

Part 2
Regulated data services

Subpart 1—Main obligations

Customer data

14 Data holder must provide customer data to customer 13
15 Data holder must provide customer data to accredited requestor if customer's authorisation is confirmed 14
16 Data holder may or must refuse request for data in certain circumstances 14
17 **Sections 14 and 15** do not prevent request to access personal information being made in some other manner 15

Designated actions

18 Data holder must perform certain actions on customer's request 15
19 Data holder must perform certain actions on accredited requestor's request if customer's authorisation is confirmed 15
20 Data holder may or must refuse to perform actions in certain circumstances 16

Joint customers

21 How data holders and accredited requestors must deal with joint customers 17

Product data

22 Data holder must provide product data to any person 18
23 Data holder may refuse request for data in certain circumstances 18

Subpart 2—Additional obligations

Secondary users

24 How data holders and accredited requestors must deal with secondary users 19
25 Regulations may require requests to be made or authorisations to be given only by secondary users 19

Valid requests

26 When request is valid 20

Electronic system

27 Data holder must operate electronic system for providing regulated data services 20
28 Electronic system must comply with prescribed technical or performance requirements 20
29 Chief executive may require data holder to test electronic system 21
30 Offence for failing to comply with notice to test electronic system 21

Requirements for requests, providing services, making information available, and dealing with data

31 Data holders must comply with requirements for requests, providing services, and making information available 21
32 Requirements for data holders in regulations or standards 22
33 Accredited requestors must comply with requirements for dealing with data and making information available 23
34 Requirements for accredited requestors in regulations or standards 23
35 Contravention of specified disclosure requirement is infringement offence 24

Part 3
Protections

Authorisation

36 Giving authorisation 24
37 Ending authorisation 24
38 Authorisation must be confirmed 25
39 Customer or secondary user must be able to control authorisation 25
40 Accredited requestor must comply with prescribed duties in respect of authorisation 26
41 Authorisation must not be required as condition of providing product 26

Restriction on who may request regulated data service

42 Only customer, secondary user, or accredited requestor may request regulated data service 26
43 Offence for contravention of request restriction 27
44 Verification of identity of person who makes request 27

Record keeping

45 Data holder must keep records about regulated data service 27
46 Accredited requestor must keep records about regulated data service 28

Customer data, product data, and action performance policies

47 Data holders and accredited requestors must have customer data, product data, and action performance policies 29
48 Contravention of policy requirement is infringement offence 29

Complaints

49 Data holders and accredited requestors must have customer complaints process 29
50 Data holder or accredited requestor must be member of dispute resolution scheme (if scheme has been prescribed) 30
51 Rules of scheme may be changed to provide for complaints about regulated data services 30

Privacy Act 2020

52 Access request not IPP 6 request but contravention is interference with privacy 30
53 Certain contraventions relating to storage and security treated as breaching information privacy principle 5 31

Part 4
Regulatory and enforcement matters

Subpart 1—Regulatory powers

54 Chief executive may require person to supply information or produce documents 31
55 Person has privileges of witness in court 32
56 Effect of proceedings 32
57 Effect of final decision that exercise of powers under **section 54** unlawful 33
58 Offence for failing to comply with notice to supply information or produce documents 34

Subpart 2—Duties to take remedial action

59 Data holder or accredited requestor must take prescribed steps to avoid, mitigate, or remedy loss or damage caused by contravention 34
60 Person who has suffered loss or damage may recover amount as debt due 35
61 Other remedies or powers not limited 35

Subpart 3—Prohibition against taking certain actions against customer

62 When subpart applies 35
63 Prohibition against taking certain actions against customer 35

Subpart 4—Prohibition against holding out

64 Prohibition against holding out 36

Subpart 5—Infringement offences

65 Infringement offences 36
66 When infringement notice may be issued 37
67 Revocation of infringement notice before payment made 37
68 What infringement notice must contain 37
69 How infringement notice may be served 37
70 Payment of infringement fees 38
71 Reminder notices 38

Subpart 6—Civil liability

72 Civil liability remedies available under this subpart 38

Pecuniary penalty order

73 When High Court may make pecuniary penalty order 39

74	Maximum penalty (Tier 1)	39
75	Maximum penalty (Tier 2)	40
76	Considerations for court in determining pecuniary penalty	41
	Declaration of contravention	
77	Declaration of contravention	41
78	Purpose and effect of declaration of contravention	41
79	What declaration of contravention must state	42
	Compensatory orders	
80	When court or Disputes Tribunal may make compensatory orders	42
81	Terms of compensatory orders	42
	Injunctions	
82	Court may grant injunctions	43
83	When court may grant restraining injunctions	43
84	When court may grant performance injunctions	43
85	Chief executive's undertaking as to damages not required	44
	Rules of procedure	
86	Rules of civil procedure and civil standard of proof apply	44
87	Limit on proceedings	44
	Relationship between proceedings and orders	
88	More than 1 civil liability remedy may be given for same conduct	45
89	Only 1 pecuniary penalty order may be made for same conduct	45
90	No pecuniary penalty and criminal penalty for same conduct	45
	Defences	
91	General defences for person in contravention	45
92	Defence for contraventions due to technical fault	46
	Jurisdiction	
93	Jurisdiction of High Court	46
94	Jurisdiction of District Court	46
95	Jurisdiction of Disputes Tribunal	47
	Part 5	
	Administrative matters	
	Subpart 1—Chief executive's functions	
96	Chief executive's functions	47
	Subpart 2—Designation regulations	
97	Designation regulations	48
98	Minister must have regard to certain matters	48
99	Minister must consult on proposed designation	48
100	Contents of designation regulations	49

Subpart 3—Accreditation of requestors

101 Application for accreditation 51
102 How application is made 51
103 Application may be made before designation regulations fully in force 51
104 Chief executive must verify applicant's identity 51
105 Decision by chief executive 51
106 Notice of decision 52
107 Application to modify accreditation 52
108 Duration of accreditation 53
109 Renewal of accreditation 53
110 When chief executive may suspend or cancel accreditation 53

Subpart 4—Appeals

111 Appeals against accreditation decisions 54

Subpart 5—Annual reporting by data holders and accredited requestors

112 Annual reporting by data holders 54
113 Annual reporting by accredited requestors 54
114 Contravention of specified annual report requirement is infringement offence 55

Subpart 6—Crown organisations

115 Crown organisations may be customer, data holder, or accredited requestor 55

Subpart 7—Register

116 Register of participants in customer and product data system 56
117 Purposes of register 56
118 Operation of register 56
119 Persons that will become data holders when designation comes into force must provide information to chief executive 56
120 Other data holders must provide information to chief executive 57
121 Contents of register that is publicly available 57
122 Contents of register that is available to data holders and accredited requestors (other than information publicly available under **section 121**) 58

Subpart 8—Information sharing

123 Sharing of information with certain law enforcement or regulatory agencies 58
124 Conditions that may be imposed on providing information under this subpart 59
125 Restriction on publication, disclosure, or use 59

Subpart 9—Regulations, standards, and exemptions

Regulations

126 General regulations 59
127 Regulations relating to fees and charges 61
128 Miscellaneous provisions relating to fees and charges 61
129 Levies payable by data holders and accredited requestors 61
130 Miscellaneous provisions relating to levies 63
131 Minister must consult on proposed regulations 63

Standards

132 Standards 63
133 Chief executive must comply with prescribed requirements and be satisfied that standards are consistent with any prescribed limits or restrictions 64
134 Chief executive's consultation on proposed standards 64

Exemptions

135 Exemptions 65
136 Effect of breach of term or condition of exemption 65

Subpart 10—Miscellaneous

137 No contracting out 65
138 Chief executive's warnings, reports, guidelines, or comments protected by qualified privilege 65
139 Notices 66
140 Service of notices 66

Subpart 11—Consequential amendments

Amendment to Disputes Tribunal Act 1988

141 Principal Act 67
142 Schedule 1 amended 67

Amendments to Privacy Act 2020

143 Principal Act 67
144 Section 75 amended (Referral of complaint to another person) 67
145 Section 208 amended (Consultation) 67

Amendment to Summary Proceedings Act 1957

146 Principal Act 67
147 Section 2 amended (Interpretation) 67

Schedule 1 68
Transitional, savings, and related provisions

The Parliament of New Zealand enacts as follows:

1 Title

This Act is the Customer and Product Data Act **2024**.

2 Commencement

This Act comes into force on the day after Royal assent.

Part 1
Preliminary provisions

Purpose

3 Purpose

(1) The purpose of this Act is to establish a framework to—

(a) realise the value of certain data for the benefit of individuals, organisations, and society; and

(b) promote competition and innovation for the long-term benefit of customers; and

(c) facilitate secure, standardised, and efficient data services in certain sectors of the New Zealand economy.

(2) The purpose is to be achieved by—

(a) improving the ability of customers, and third parties they authorise, to access and use the data held about them by participants in those sectors; and

(b) improving access to data about products in those sectors; and

(c) requiring certain safeguards, controls, standards, and functionality in connection with those data services.

Overview

4 Overview

(1) This Act regulates data services provided by persons that are designated as data holders under **subpart 2 of Part 5**.

(2) Services relating to customer data are regulated as follows:

If ...	A person (a data holder) is specified, or belongs to a class specified, in designation regulations; and it holds customer data of the kind specified in the regulations; and either— • a customer requests the data or requests that the data holder perform an action; or

	• an accredited requestor authorised by the customer requests the data or requests that the data holder perform an action.
Then ...	The data holder must comply with the request (**sections 14, 15, 18, and 19**).
However ...	Certain protections apply, including duties to— • confirm that the customer has authorised the request (**section 38**); and • check the identity of the person who makes the request (**section 44**); and • have a complaints process (**section 49**). In addition,— • the data holder may or must refuse the request in certain circumstances (**sections 16 and 20**); and • only a person granted accreditation under **subpart 3 of Part 5** may act as an accredited requestor; and • an accredited requestor may only act within the class of its accreditation.

(3) Services relating to product data are regulated as follows:

If ...	A person (a data holder) is specified, or belongs to a class specified, in designation regulations; and it holds product data of the kind specified in the regulations; and a person requests the data.
Then ...	The data holder must comply with the request (**section 22**).
However ...	The data holder may refuse the request in certain circumstances (**section 23**).

(4) Additional details are set out in secondary legislation, including as follows:

Designation regulations	which designate the data holders and classes of data that are regulated under this Act (**subpart 2 of Part 5**).
Other regulations	which specify general requirements relating to regulated data services (**section 126**).
Standards	which specify technical requirements relating to regulated data services (**section 132**).

(5) Data holders and accredited requestors may be granted exemptions under **section 135**.

(6) This section is only a guide to the general scheme and effect of this Act.

Interpretation

5 Interpretation

(1) In this Act, unless the context otherwise requires,—

accredited requestor has the meaning set out in **section 7**

authorisation and **authorise** have the meanings set out in **section 36**

chief executive means the chief executive of the Ministry

civil liability provision has the meaning set out in **section 72(2)**

confirmation has the meaning set out in **section 38(2)**

court means, in relation to any matter, the court before which the matter is to be determined (*see* **sections 93 and 94**)

customer has the meaning set out in **section 8(1)**

customer data has the meaning set out in **section 8(2)**

data includes information

data holder has the meaning set out in **section 6**

derived data has the meaning set out in **section 33(3)**

designated action, in relation to a data holder and a provision of this Act, means an action that is specified, or belongs to a class specified, in the data holder's designation regulations for the purposes of that provision

designated customer data has the meaning set out in **section 8(3)**

designated product data has the meaning set out in **section 9**

designation regulations—

(a) means designation regulations made under **section 97**; and

(b) in relation to a person that is a data holder, means any designation regulations that have the effect of designating that person

director has the same meaning as in section 6 of the Financial Markets Conduct Act 2013

document has the same meaning as in section 4 of the Evidence Act 2006

goods has the same meaning as in section 2(1) of the Fair Trading Act 1986

infringement fee, in relation to an infringement offence, means the infringement fee for the offence

infringement offence means an offence identified in this Act as being an infringement offence

involved in a contravention has the meaning set out in **subsection (2)**

IPP means an information privacy principle set out in section 22 of the Privacy Act 2020

IPP 6 means information privacy principle 6 (access to personal information) set out in section 22 of the Privacy Act 2020

Minister means the Minister of the Crown who, under the authority of a warrant or with the authority of the Prime Minister, is responsible for the administration of this Act

Ministry means the department that, with the authority of the Prime Minister, is responsible for the administration of this Act

New Zealand Business Number means the number allocated to an entity under the New Zealand Business Number Act 2016

personal information has the same meaning as in section 7 of the Privacy Act 2020

product has the meaning set out in **section 9(1)**

product data has the meaning set out in **section 9(2)**

register means the register established under **subpart 7 of Part 5**

regulated data service has the meaning set out in **section 10**

regulations means regulations made under this Act

secondary user has the meaning set out in **section 24(4)**

senior manager, in relation to a 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 a chief financial officer)

serious threat has the meaning set out in **section 16(3)**

services has the same meaning as in section 2(1) of the Fair Trading Act 1986

standard means a standard made under **section 132**

valid request has the meaning set out in **section 26**.

(2) In this Act, a person is **involved in a contravention** if the person—

(a) has aided, abetted, counselled, or procured the contravention; or

(b) has induced, whether by threats or promises or otherwise, the contravention; or

(c) has been in any way, directly or indirectly, knowingly concerned in, or party to, the contravention; or

(d) has conspired with others to effect the contravention.

6 Data holder

A person is a **data holder** if—

(a) the person is specified, or belongs to a class specified, in designation regulations; and

(b) either—

(i) the person holds designated customer data or designated product data (or both); or

(ii) another person holds that data on behalf of the person described in **paragraph (a)**.

7 Accredited requestor

A person is an **accredited requestor** if the person is accredited under **subpart 3 of Part 5**.

8 Customer, customer data, and designated customer data

(1) **Customer** means a person that acquires, or is seeking to acquire, goods or services from a data holder.

(2) **Customer data** means data that is about an identifiable customer that is held by or on behalf of a data holder (including, for example, personal information).

(3) **Designated customer data**, in relation to a data holder and a provision of this Act, means customer data—

(a) that is specified, or belongs to a class specified, in the data holder's designation regulations for the purposes of that provision; and

(b) that is held by (or on behalf of) the data holder on or after the day specified in, or determined in accordance with, the designation regulations.

9 Product, product data, and designated product data

(1) **Product**, in relation to a data holder, means goods or services offered by the data holder.

(2) **Product data**, in relation to a data holder,—

(a) means data that is about, or relates to, 1 or more of the data holder's products; but

(b) does not include customer data.

(3) **Designated product data**, in relation to a data holder and a provision of this Act, means product data—

(a) that is specified, or belongs to a class specified, in the data holder's designation regulations for the purposes of that provision; and

(b) that is held by (or on behalf of) the data holder on or after the day specified in, or determined in accordance with, the designation regulations.

10 Regulated data service

Regulated data service means either or both of the following:

(a) providing data under **Part 2**:

(b) performing an action under **Part 2**.

Territorial application of Act

11 Territorial application of Act

(1) This Act applies to—

(a) a New Zealand agency (**A**), in relation to any conduct by A (whether or not while A is, or was, present in New Zealand) in respect of designated customer data or designated product data held by or on behalf of A:

(b) an overseas agency (**B**), in relation to any conduct by B in the course of carrying on business in New Zealand in respect of designated customer data or designated product data held by or on behalf of B.

(2) For the purposes of **subsection (1)**, it does not matter—

(a) where the data is, or was, collected by or on behalf of the agency; or

(b) where the data is held by or on behalf of the agency; or

(c) where the customer or product concerned is, or was, located.

(3) For the purposes of **subsection (1)(b)**, an agency may be treated as carrying on business in New Zealand without necessarily—

(a) being a commercial operation; or

(b) having a place of business in New Zealand; or

(c) receiving any monetary payment for the supply of goods or services; or

(d) intending to make a profit from its business in New Zealand.

(4) In this section, **New Zealand agency** and **overseas agency** have the same meanings as in subpart 2 of Part 1 of the Privacy Act 2020.

Compare: 2020 No 31 s 4

Transitional, savings, and related provisions

12 Transitional, savings, and related provisions

The transitional, savings, and related provisions (if any) set out in **Schedule 1** have effect according to their terms.

Act binds the Crown

13 Act binds the Crown

This Act binds the Crown.

Part 2
Regulated data services

Subpart 1—Main obligations

Customer data

14 Data holder must provide customer data to customer

(1) This section applies if—

(a) a customer requests that a data holder provides data to the customer; and

(b) the data is designated customer data that is about that customer; and

(c) the request—

(i) is a valid request; and

(ii) is made using the system described in **section 27**.

(2) The data holder must provide the data to the customer using that system.

15 Data holder must provide customer data to accredited requestor if customer's authorisation is confirmed

(1) This section applies if—

(a) an accredited requestor (**A**) requests that a data holder provides data to A in respect of a customer; and

(b) the data holder has carried out confirmation in relation to the request under **section 38**; and

(c) the data is designated customer data that is about that customer; and

(d) the request—

(i) is a valid request; and

(ii) is made using the system described in **section 27**; and

(e) A is acting within the class of its accreditation; and

(f) the data holder has verified the identity of the person who made the request under **section 44(2)**.

(2) The data holder must provide the data to A using that system.

16 Data holder may or must refuse request for data in certain circumstances

(1) Despite **sections 14 and 15**, a data holder may refuse to provide any data requested under either of those sections—

(a) if the disclosure of the data would be likely to pose a serious threat to the life, health, or safety of any individual, or to public health or public safety (*see* **subsection (3)**); or

(b) if the data holder reasonably believes that disclosure of the data would create a significant likelihood of serious harassment of an individual; or

(c) if the data holder reasonably believes that disclosure of the data would be likely to have a materially adverse effect on the security, integrity, or stability of either or both of the following:

(i) the data holder's information and communication technology systems:

(ii) the register; or

(d) in the case of **section 14**, if the customer owes a debt to the data holder in relation to charges imposed in connection with the request; or

(e) in the case of **section 15**, if the accredited requestor owes a debt to the data holder in relation to charges imposed in connection with the request or any other regulated data services; or

(f) in the circumstances prescribed in the regulations or standards.

(2) Despite **sections 14 and 15**, a data holder must refuse to provide any data requested under either of those sections if the data holder has reasonable grounds to believe that the request is made under the threat of physical or mental harm.

(3) In this Act, **serious threat** means a threat that a data holder reasonably believes to be a serious threat having regard to all of the following:

(a) the likelihood of the threat being realised; and

(b) the severity of the consequences if the threat is realised; and

(c) the time at which the threat may be realised.

17 Sections 14 and 15 do not prevent request to access personal information being made in some other manner

Sections 14 and 15 do not prevent an individual from exercising their rights under IPP 6 by making a request in some other manner.

Guidance note

IPP 6 is set out in section 22 of the Privacy Act 2020. It confers an entitlement on an individual to access their personal information on request.

Designated actions

18 Data holder must perform certain actions on customer's request

(1) This section applies if—

(a) a customer requests that a data holder perform an action relating to the customer; and

(b) the requested action is a designated action; and

(c) the data holder would ordinarily perform the action to which the request relates in the course of the data holder's business (*see* **subsection (3)**); and

(d) the request—

(i) is a valid request; and

(ii) is made using the system described in **section 27**.

(2) The data holder must perform the action.

(3) When considering whether a data holder would ordinarily perform an action in the course of its business, regard must be had to the matters (if any) prescribed in the regulations and the standards.

19 Data holder must perform certain actions on accredited requestor's request if customer's authorisation is confirmed

(1) This section applies if—

(a) an accredited requestor (**A**) requests that a data holder perform an action in respect of a customer; and

(b) the data holder has carried out confirmation in relation to the request under **section 38**; and

(c) the requested action is a designated action; and

(d) the data holder would ordinarily perform actions to which the request relates in the course of the data holder's business (*see* **subsection (3)**); and

(e) the request—

(i) is a valid request; and

(ii) is made using the system described in **section 27**; and

(f) A is acting within the class of its accreditation; and

(g) the data holder has verified the identity of the person who made the request under **section 44(2)**.

(2) The data holder must perform the action.

(3) When considering whether a data holder would ordinarily perform an action in the course of its business, regard must be had to the matters (if any) prescribed in the regulations and the standards.

20 Data holder may or must refuse to perform actions in certain circumstances

(1) Despite **sections 18 and 19**, a data holder may refuse to perform any action requested under either of those sections—

(a) if performing the action would be likely to pose a serious threat to the life, health, or safety of any individual, or to public health or public safety (*see* **section 16(3)**); or

(b) if the data holder reasonably believes that performing the action would create a significant likelihood of serious financial harm to any person; or

(c) if the data holder reasonably believes that it is likely that the request was made (wholly or in part) as a consequence of deception (*see* **subsection (3)**); or

(d) if the data holder reasonably believes that performing the action would be likely to have a materially adverse effect on the security, integrity, or stability of either or both of the following:

(i) the data holder's information and communication technology systems:

(ii) the register; or

(e) in the case of **section 18**, if the customer owes a debt to the data holder in relation to charges imposed in connection with the request; or

(f) in the case of **section 19**, if the accredited requestor owes a debt to the data holder in relation to charges imposed in connection with the request or any other regulated data services; or

(g) in the circumstances prescribed in the regulations or standards.

(2) Despite **sections 18 and 19**, a data holder must refuse to perform any action requested under either of those sections if the data holder has reasonable grounds to believe that the request is made under the threat of physical or mental harm.

(3) In **subsection (1)(c)**, **deception** has the same meaning as in section 240(2) of the Crimes Act 1961.

Joint customers

21 How data holders and accredited requestors must deal with joint customers

(1) This section applies to a regulated data service provided in connection with 2 or more joint customers.

(2) A data holder and an accredited requestor must deal with the joint customers in the manner prescribed by the regulations, including in connection with the following:

(a) when or how the joint customers may or must make a request or give an authorisation under this subpart:

(b) how the data holder or accredited requestor may or must deal with a request or authorisation from 1 or more of the joint customers:

(c) when a request made, or an authorisation given, by 1 or more of the joint customers must be treated as effective (or ineffective) for the purposes of this Act.

(3) Regulations made for the purposes of this section may (without limitation) provide for any of the following:

(a) allowing or requiring a data holder or an accredited requestor to deal with a request or an authorisation in any of the following ways (on the terms and conditions (if any) specified in the regulations):

(i) that a request or an authorisation may be made or given by any 1 or more of the joint customers (without the other joint customers):

(ii) that a request or an authorisation may be made or given only by 2 or more of the joint customers acting together:

(iii) that a request or an authorisation may be made or given only if it is made or given by all of the joint customers acting together:

(iv) that a request or an authorisation may not be made or given by or on behalf of the joint customers:

(b) allowing 1 or more joint customers to view or change permissions for how those joint customers may or must make a request or give an authorisation.

(4) **Sections 14 to 20** are subject to this section.

(5) In this section, 1 or more customers are **joint customers** if—

(a) they jointly hold a financial product issued by the data holder; or

(b) they have rights or obligations under the same agreement with the data holder.

(6) In **subsection (5)**, **financial product** has the same meaning as in section 7 of the Financial Markets Conduct Act 2013.

Example

Two people, A and B, have a joint bank account. The regulations may require a data holder to—

- allow A and B to authorise A or B acting alone to make a request or give an authorisation in certain circumstances; or
- require both A and B acting together to make a request or give an authorisation in other circumstances.

Product data

22 Data holder must provide product data to any person

(1) This section applies if—

(a) a person requests that a data holder provides data to the person; and

(b) the data is designated product data; and

(c) the request—

(i) is a valid request; and

(ii) is made using the system described in **section 27**.

(2) The data holder must provide the data to the person using that system.

23 Data holder may refuse request for data in certain circumstances

Despite **section 22**, a data holder may refuse to provide any data requested under that section—

(a) if the data holder reasonably believes that disclosure of the data would be likely to have a materially adverse effect on the security, integrity, or stability of either or both of the following:

(i) the data holder's information and communication technology systems:

(ii) the register; or

(b) in the circumstances prescribed in the regulations or standards.

Subpart 2—Additional obligations

Secondary users

24 How data holders and accredited requestors must deal with secondary users

(1) A data holder and an accredited requestor must deal with a secondary user in the manner prescribed by the regulations, including in connection with the following:

(a) when or how a secondary user may or must make a request or give an authorisation under **subpart 1** on behalf of a customer; and

(b) how the data holder or an accredited requestor may or must deal with a request or an authorisation from a secondary user; and

(c) when a request made or an authorisation given by a secondary user must be treated as effective (or ineffective) for the purposes of this Act.

(2) Regulations made for the purposes of **subsection (1)** may (without limitation) provide for any of the following:

(a) whether, when, or how a person may or must be approved, or treated as being approved, to do either or both of the following:

(i) make a request under **subpart 1** on behalf of a customer:

(ii) give an authorisation under **subpart 1** on behalf of a customer:

(b) when or how the approval referred to in **paragraph (a)** may be viewed, changed, or revoked.

(3) **Sections 14 to 20** are subject to this section.

(4) A person (**A**) is a **secondary user** in relation to a customer (**B**) if—

(a) A is specified, or belongs to a class specified, in designation regulations as a secondary user in relation to a class of customers; and

(b) B belongs to that class of customers; and

(c) where required by the regulations, A has been approved, or is treated as being approved, as a secondary user in the manner required by the regulations (and that approval has not been revoked or otherwise ceased to be in effect).

(5) If regulations provide for approval of a person as a secondary user, the regulations may also provide for the manner in which the approval may or must be given, viewed, changed, or revoked.

25 Regulations may require requests to be made or authorisations to be given only by secondary users

(1) This section applies if the regulations provide that a particular kind of customer may make a request or authorise an accredited requestor to make a request

under **subpart 1** only if that is done on their behalf by 1 or more secondary users.

(2) A request or an authorisation in respect of the customer is of no effect under **subpart 1** if it is made or given otherwise than in accordance with those regulations.

Example

The regulations may provide that, if a customer is a company, the company must authorise at least 1 secondary user to act on its behalf under **subpart 1**.

A request or an authorisation in respect of a company may only be made through a secondary user.

Valid requests

26 When request is valid

A request is a **valid request** if the person making the request—

(a) specifies the data or action being requested; and

(b) complies with the requirements provided for in the standards about making requests (if any); and

(c) otherwise makes the request in the manner prescribed in the regulations (if any).

Electronic system

27 Data holder must operate electronic system for providing regulated data services

A data holder must operate an electronic system that has the capacity to do all of the following with reasonable reliability:

(a) enable the data holder to receive requests for regulated data services; and

(b) enable the data holder to provide regulated data services in response to those requests or to otherwise respond to those requests (including where the service must not or may not be provided).

28 Electronic system must comply with prescribed technical or performance requirements

(1) A data holder must ensure that the electronic system referred in **section 27** complies with the technical or performance requirements specified in the regulations and the standards.

(2) Regulations or standards made for the purposes of this section may (without limitation) relate to any of the following:

(a) security and identity verification measures:

(b) reliability and timeliness of responses to requests for regulated data services:

(c) availability:

(d) useability:

(e) accessibility:

(f) monitoring use and functionality:

(g) reporting on any of the matters referred to in **paragraphs (a) to (f)** (including to the chief executive).

29 Chief executive may require data holder to test electronic system

(1) The chief executive may, by written notice, require a data holder to—

(a) ensure that its electronic system is tested for the purpose of verifying that the system complies with some or all of the technical or performance requirements referred to in **section 28**; and

(b) give a report to the chief executive on the testing.

(2) The data holder must comply with **subsection (1)(a) and (b)** within the time and in the manner specified in the notice.

(3) *See* **sections 139 and 140**, which provide for notice requirements.

30 Offence for failing to comply with notice to test electronic system

(1) A person commits an offence if the person—

(a) refuses or fails, without reasonable excuse, to comply with a notice under **section 29**; or

(b) in purported compliance with a notice under **section 29**, gives a report to the chief executive knowing it to be false or misleading in a material particular.

(2) A person that commits an offence against **subsection (1)** is liable on conviction to a fine not exceeding—

(a) $100,000 in the case of an individual:

(b) $300,000 in any other case.

Requirements for requests, providing services, making information available, and dealing with data

31 Data holders must comply with requirements for requests, providing services, and making information available

(1) A data holder must comply with the requirements specified in the regulations and the standards in connection with the following:

(a) receiving requests for regulated data services (including in relation to performing an action):

(b) providing those services or otherwise responding to those requests:

(c) notifying or otherwise making available information to any of the persons referred to in **subsection (3)**.

(2) The requirements must be complied with in the manner prescribed in the regulations or standards.

(3) For the purposes of **subsection (1)(c)**, a data holder may be required to notify or otherwise make available information to any of the following:

(a) a customer:

(b) a secondary user:

(c) another person that is a data holder:

(d) an accredited requestor:

(e) the chief executive:

(f) any member of the public or any class of the public.

32 Requirements for data holders in regulations or standards

(1) Regulations or standards made for the purposes of **section 31** may (without limitation) relate to any of the following:

Charges in connection with regulated data services

(a) requirements about charging amounts payable in connection with regulated data services, including—

(i) when an amount may, must, or must not be charged; and

(ii) prohibitions or restrictions relating to charging those amounts (for example, a cap on how much may be charged):

Notifying or otherwise making available information

(b) the information that must be notified or otherwise made available to any person referred to in **section 31(3)**, the times at which, or the events on the occurrence of which, information must be notified or made available, and the manner of notifying or making available the information (including prescribing the manner in which the information is to be presented, calculated, or prepared):

Data

(c) the format and description of data:

(d) the manner in which requests for regulated data services are received and responded to (for example, a requirement to use an application programming interface (API)):

(e) data quality:

Confirmation

(f) the manner in which authorisations are confirmed under **section 38(2)**.

(2) In this section, **data** means designated customer data or designated product data (or both), as the case may be.

Guidance note

See **subpart 9 of Part 5** for provisions relating to the making of regulations and standards.

33 Accredited requestors must comply with requirements for dealing with data and making information available

(1) An accredited requestor must comply with the requirements specified in the regulations and the standards in connection with the following:

(a) the use, modification, or disclosure of—

(i) designated customer data; or

(ii) derived data:

(b) notifying or otherwise making available information to any of the persons referred to in **subsection (2)**.

(2) For the purposes of **subsection (1)(b)**, an accredited requestor may be required to notify or otherwise make available information to any of the following:

(a) a customer:

(b) a secondary user:

(c) a data holder:

(d) another accredited requestor:

(e) the chief executive:

(f) any member of the public or any class of the public.

(3) In this Act, **derived data** means data that is wholly or partly derived from—

(a) designated customer data; or

(b) other derived data.

34 Requirements for accredited requestors in regulations or standards

Regulations or standards made for the purposes of **section 33** may (without limitation) relate to any of the following:

Dealing with data

(a) requirements, or restrictions, relating to how designated customer data and derived data is used, modified, or disclosed (for example, requirements to de-identify data so that it no longer relates to an identifiable person):

Notifying or otherwise making available information

(b) the information that must be notified or otherwise made available to any person referred to in **section 33(2)**, the times at which, or the events on the occurrence of which, information must be notified or made available, and the manner of notifying or making available the information (including prescribing the manner in which the information is to be presented, calculated, or prepared).

Guidance note

See **subpart 9 of Part 5** for provisions relating to the making of regulations.

35 Contravention of specified disclosure requirement is infringement offence

(1) A person that contravenes a specified disclosure requirement commits an infringement offence and is liable to—

(a) an infringement fee of $20,000; or

(b) a fine imposed by a court not exceeding $50,000.

(2) In this section and **section 73**, **specified disclosure requirement** means a requirement imposed under **section 31(1)(c), 32(1)(b), 33(1)(b), or 34(b)** that is specified by the regulations or standards for the purposes of this section.

Part 3
Protections

Authorisation

36 Giving authorisation

(1) A customer (or a secondary user on their behalf) has given an **authorisation** to another person (**A**) if—

(a) the customer (or secondary user) gave the authorisation expressly, including by specifying any limits on the scope of the authorisation; and

(b) at the time of giving the authorisation, the customer (or secondary user) was reasonably informed about the matter to which the authorisation relates; and

(c) the authorisation was otherwise given in the manner (if any) prescribed by the regulations and the standards; and

(d) the authorisation has not ended.

(2) To **authorise** an action means to give an authorisation for that action.

37 Ending authorisation

An authorisation ends on the earliest of the following:

(a) the expiry of the maximum period for an authorisation specified by the regulations (if any):

(b) the occurrence of an event specified by the regulations (if any) (for example, when the customer closes an account with a data holder):

(c) the time (if any) specified by the customer (or a secondary user on their behalf).

38 Authorisation must be confirmed

(1) This section applies if a data holder receives a request from an accredited requestor to provide a regulated data service relating to a customer.

(2) The data holder must check that the service is within the scope of the authorisation given by the customer (or by a secondary user on their behalf) (**confirmation**).

(3) The data holder must not provide the regulated data service until confirmation has been completed.

(4) A confirmation is valid for any service within the scope of that authorisation until the time when the scope of the authorisation is modified or the authorisation ends (whichever is earlier).

(5) If the scope of the authorisation is modified or the authorisation ends, **subsection (2)** applies again.

Example

A customer authorises their electricity provider (a data holder) to provide details of their electricity usage to a company that makes recommendations about the best electricity deals in the market.

Before sharing any of the customer's data for the first time, the electricity provider must confirm the customer's authorisation.

However, it is not necessary to carry out confirmation for any subsequent actions performed within the scope of that authorisation. The electricity provider will only have to reconfirm the customer's authorisation if the scope of the authorisation is modified or the authorisation ends.

(6) A person that carries out a confirmation must carry out the confirmation in the manner (if any) prescribed by the regulations and the standards.

39 Customer or secondary user must be able to control authorisation

(1) If a data holder has confirmed an authorisation under **section 38** given by a customer (or by a secondary user on their behalf), the data holder—

(a) must have systems in place to enable the customer or secondary user (as the case may be) to view or end the authorisation; and

(b) must ensure that those systems meet the requirements (if any) provided for by the regulations and the standards.

(2) If a customer (or a secondary user on their behalf) has given an accredited requestor an authorisation, the accredited requestor—

(a) must have systems in place to enable the customer or secondary user (as the case may be) to view or end the authorisation; and

(b) must ensure that those systems meet the requirements (if any) provided for by the regulations and the standards.

(3) The data holder or accredited requestor must ensure that the systems are able to give immediate effect to a withdrawal of an authorisation.

40 Accredited requestor must comply with prescribed duties in respect of authorisation

(1) If an accredited requestor (**A**) seeks to obtain, or may accept, an authorisation from a customer (or a secondary user on their behalf),—

(a) A must take the prescribed steps (if any) to enable the customer or secondary user (as the case may be) to be reasonably informed about the matter to which the authorisation relates; and

(b) A must use only prescribed methods (if any) to obtain the authorisation (for example, a tool that requires the customer to perform an affirmative action in order to give the authorisation); and

(c) A must not obtain, or accept, an authorisation from a customer (or secondary user) in the prescribed circumstances; and

(d) A must comply with any other requirements in connection with obtaining, or accepting, the authorisation.

(2) In this section, **prescribed** means prescribed by the regulations or the standards.

41 Authorisation must not be required as condition of providing product

(1) This section applies if a person provides to a customer goods or services other than regulated data services (**products**).

(2) The person must not, as a condition of providing a product, require the customer to authorise a regulated data service unless that service is reasonably necessary to enable the person to provide the product.

Restriction on who may request regulated data service

42 Only customer, secondary user, or accredited requestor may request regulated data service

A person must not request, or purport to request, a regulated data service that relates to a customer unless the person is—

(a) the customer; or

(b) a secondary user who is acting on behalf of the customer in accordance with **section 24**; or

(c) an accredited requestor that is—

(i) authorised by the customer to request the service; and

(ii) acting within the class of its accreditation.

43 Offence for contravention of request restriction

(1) A person commits an offence if the person—

(a) requests, or purports to request, a regulated data service that relates to a customer in contravention of **section 42**; and

(b) knows that they are not permitted to make the request.

(2) A person that commits an offence against this section is liable on conviction,—

(a) in the case of an individual, to imprisonment for a term not exceeding 5 years or to a fine not exceeding $1 million (or both):

(b) in any other case, to a fine not exceeding $5 million.

44 Verification of identity of person who makes request

(1) This section applies if a data holder receives a request to provide a regulated data service relating to a customer.

(2) The data holder—

(a) must verify the identity of the person who made the request; and

(b) must not provide the regulated data service until it has complied with **paragraph (a)**.

(3) The data holder must verify the identity of a person in the manner (if any) prescribed by the regulations and the standards.

Record keeping

45 Data holder must keep records about regulated data service

(1) A data holder must keep records of the following matters in respect of any regulated data service that the data holder provides:

(a) the request made for the service:

(b) whether the data holder has given effect, or has attempted to give effect, to the request:

(c) the authorisation given by or on behalf of the customer (if any), including—

(i) any limitations on the scope of the authorisation; and

(ii) any modifications to the authorisation; and

(iii) any previous authorisation given by or on behalf of the customer:

(d) whether the authorisation (if any) has been confirmed under **section 38** and whether the identity of a person has been verified under **section 44**:

(e) the information specified by the regulations (if any).

(2) **Subsection (1)(c) to (e)** does not apply to product data requests.

(3) The records must be kept—

(a) for 5 years; and

(b) otherwise in the manner prescribed by the regulations (if any).

(4) If a person ceases to be a data holder, this section continues to apply with all necessary modifications as if the person were still a data holder.

(5) A person that contravenes this section commits an infringement offence and is liable to—

(a) an infringement fee of $20,000; or

(b) a fine imposed by a court not exceeding $50,000.

46 Accredited requestor must keep records about regulated data service

(1) An accredited requestor must keep records of the following matters in respect of any regulated data service relating to a customer that the accredited requestor requests:

(a) the authorisation given by or on behalf of the customer, including—

(i) any limitations on the scope of the authorisation; and

(ii) any modifications to the authorisation; and

(iii) any previous authorisation given by or on behalf of the customer:

(b) if, after receiving data under **section 15**,—

(i) the accredited requestor provided the data or derived data to another person (other than the customer or a secondary user), that person and the basis upon which the accredited requestor considers it is permitted to provide the data or derived data to that person:

(ii) the accredited requestor de-identified the data so that it no longer relates to an identifiable person, how the data was de-identified:

(c) the information specified by the regulations (if any).

(2) The records must be kept—

(a) for 5 years; and

(b) otherwise in the manner prescribed by the regulations (if any).

(3) If a person ceases to be an accredited requestor, this section continues to apply with all necessary modifications as if it were still an accredited requestor.

(4) An accredited requestor that contravenes this section commits an infringement offence and is liable to—

(a) an infringement fee of $20,000; or

(b) a fine imposed by a court not exceeding $50,000.

Customer data, product data, and action performance policies

47 Data holders and accredited requestors must have customer data, product data, and action performance policies

(1) A data holder or an accredited requestor (**A**) must develop, publish, implement, and maintain 1 or more policies relating to customer data, product data, and the performance of actions under this Act.

(2) A must comply with this section in the manner (if any) prescribed by the regulations and the standards.

48 Contravention of policy requirement is infringement offence

(1) A person that contravenes a specified policy requirement commits an infringement offence and is liable to—

(a) an infringement fee of $20,000; or

(b) a fine imposed by a court not exceeding $50,000.

(2) In this section and **section 73**, **specified policy requirement** means a requirement imposed under **section 47** that is specified by the regulations or standards for the purposes of this section.

Complaints

49 Data holders and accredited requestors must have customer complaints process

(1) A data holder or an accredited requestor (**A**) must have a process that—

(a) allows customers to make complaints about A's conduct in connection with regulated data services that A provides or requests; and

(b) provides for how those complaints must be investigated and otherwise dealt with.

(2) A must ensure that,—

(a) as far as practicable, the process enables complaints to be investigated and otherwise dealt with fairly, efficiently, and effectively; and

(b) the process meets the requirements provided for by the regulations (if any).

50 Data holder or accredited requestor must be member of dispute resolution scheme (if scheme has been prescribed)

(1) This section applies to a data holder or an accredited requestor if, for the purposes of this section, 1 or more dispute resolution schemes have been prescribed by the regulations for a class of persons that includes the data holder or accredited requestor.

(2) The data holder or accredited requestor must be a member of at least 1 of those schemes.

(3) The regulations may prescribe a dispute resolution scheme only if the scheme has been established, approved, or otherwise authorised for any purpose under any other legislation.

Examples of schemes that may be prescribed

A dispute resolution scheme approved under the Financial Service Providers (Registration and Dispute Resolution) Act 2008.

A dispute resolution scheme within the meaning of section 95 of the Electricity Industry Act 2010.

51 Rules of scheme may be changed to provide for complaints about regulated data services

(1) The person responsible for a scheme may, in the manner prescribed in the regulations, change the rules of a scheme to—

(a) allow customers to make complaints about the conduct of a data holder or an accredited requestor (**A**) in connection with regulated data services that A provides or requests; and

(b) provide for how those complaints must be investigated and otherwise dealt with; and

(c) otherwise facilitate the scheme dealing with those complaints.

(2) The regulations may disapply any requirement or restriction imposed under any other legislation in connection with a change to the rules of a scheme.

(3) A change made under this section is effective despite anything to the contrary in any other legislation, including anything relating to the consent or approval of any person to the making of the change.

(4) In this section, **scheme** means a dispute resolution scheme established, approved, or otherwise authorised for any purpose under any other legislation.

Privacy Act 2020

52 Access request not IPP 6 request but contravention is interference with privacy

(1) This section applies to a request that a data holder provide data under **section 14 or 15** to the extent that the request relates to personal information.

(2) The request is not a request made under IPP 6 and, accordingly, nothing in subpart 1 of Part 4 of the Privacy Act 2020 applies.

(3) However, if a data holder contravenes **section 14, 15, or 16(2)**, the action of the data holder must be treated as being an interference with the privacy of an individual for the purposes of Parts 5 and 6 of the Privacy Act 2020.

53 Certain contraventions relating to storage and security treated as breaching information privacy principle 5

(1) If, in relation to any personal information, a data holder contravenes a CPD storage and security requirement, the data holder 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.

(2) In this section, **CPD storage and security requirement** means any of the following:

(a) **section 38(3) or 44(2)**:

(b) a requirement that is imposed under this Act in connection with 1 or more of the following and that is specified by the regulations for the purposes of this section:

(i) protecting data against loss:

(ii) protecting data against access, use, modification, or disclosure that is not authorised by the data holder or an accredited requestor:

(iii) protecting data against other misuse.

Part 4
Regulatory and enforcement matters

Subpart 1—Regulatory powers

54 Chief executive may require person to supply information or produce documents

(1) If the chief executive considers it necessary or desirable for the purposes of performing or exercising their functions, powers, or duties under this Act, the chief executive may, by written notice served on any person, require the person—

(a) to supply to the chief executive, within the time and in the manner specified in the notice, any information or class of information specified in the notice; or

(b) to produce to the chief executive, or to a person specified in the notice acting on their behalf in accordance with the notice, any document or class of documents specified in the notice (within the time and in the manner specified in the notice); or

(c) if necessary, to reproduce, or assist in reproducing, in usable form, information recorded or stored in any document or class of documents specified in the notice (within the time and in the manner specified in the notice).

(2) Information supplied in response to a notice under **subsection (1)(a)** must be—

(a) given in writing; and

(b) signed in the manner specified in the notice.

(3) If a document is produced in response to a notice, the chief executive, or the person to whom the document is produced, may—

(a) inspect and make records of that document; and

(b) take copies of the document or extracts from the document.

(4) *See* **sections 139 and 140**, which provide for notice requirements.

Compare: 2011 No 5 s 25

55 Person has privileges of witness in court

Every person has the same privileges in relation to providing information and documents under **section 54** as witnesses have in a proceeding before a court.

Compare: 2011 No 5 s 56(1)

56 Effect of proceedings

(1) If a person commences a proceeding in any court in respect of the exercise of any powers conferred by **section 54**, until a final decision in relation to the proceeding is given,—

(a) the powers may be, or may continue to be, exercised as if the proceeding had not been commenced; and

(b) no person is excused from fulfilling their obligations under that section by reason of the proceeding.

(2) However, the High Court may make an interim order overriding the effect of **subsection (1)**, but only if it is satisfied that—

(a) the applicant has established a prima facie case that the exercise of the power in question is unlawful; and

(b) the applicant would suffer substantial harm from the exercise or discharge of the power or obligation; and

(c) if the power or obligation is exercised or discharged before a final decision is made in the proceeding, none of the remedies specified in **subsection (3)**, or any combination of those remedies, could subsequently provide an adequate remedy for that harm; and

(d) the terms of that order do not unduly hinder or restrict the chief executive in performing or exercising their functions, powers, or duties under this Act.

(3) The remedies are as follows:

(a) any remedy that the High Court may grant in making a final decision in relation to the proceeding (for example, a declaration):

(b) any damages that the applicant may be able to claim in concurrent or subsequent proceedings:

(c) any opportunity that the applicant may have, as defendant in a proceeding, to challenge the admissibility of any evidence obtained as a result of the exercise or discharge of the power or obligation.

Compare: 2011 No 5 s 57

57 Effect of final decision that exercise of powers under section 54 unlawful

(1) This section applies in any case where it is declared, in a final decision given in any proceeding in respect of the exercise of any powers conferred by **section 54**, that the exercise of any powers conferred by that section is unlawful.

(2) To the extent to which the exercise of those powers is declared unlawful, the chief executive must ensure that, immediately after the decision of the court is given,—

(a) any information obtained as a consequence of the exercise of powers declared to be unlawful and any record of that information are destroyed; and

(b) any documents, or extracts from documents, obtained as a consequence of the exercise of powers declared to be unlawful are returned to the person previously having possession of them, or previously having them under their control, and any copies of those documents or extracts are destroyed; and

(c) any information derived from or based on such information, documents, or extracts is destroyed.

(3) However, the court may, in the court's discretion, order that any information, record, or copy of any document or extract from a document may, instead of being destroyed, be retained by the chief executive subject to any terms and conditions that the court imposes.

(4) No information, and no documents or extracts from documents, obtained as a consequence of the exercise of any powers declared to be unlawful and no record of any such information or document—

(a) are admissible as evidence in any civil proceeding unless the court hearing the proceeding in which the evidence is sought to be adduced is satisfied that there was no unfairness in obtaining the evidence:

(b) are admissible as evidence in any criminal proceeding if the evidence is excluded under section 30 of the Evidence Act 2006:

(c) may otherwise be used in connection with the exercise of any power conferred by this Act unless the court that declared the exercise of the powers to be unlawful is satisfied that there was no unfairness in obtaining the evidence.

Compare: 2011 No 5 s 58

58 Offence for failing to comply with notice to supply information or produce documents

(1) A person commits an offence if the person—

(a) refuses or fails, without reasonable excuse, to comply with a notice under **section 54**; or

(b) in purported compliance with a notice under **section 54**, supplies information, or produces a document, knowing it to be false or misleading in a material particular.

(2) A person that commits an offence against **subsection (1)** is liable on conviction to a fine not exceeding—

(a) $100,000 in the case of an individual:

(b) $300,000 in any other case.

Compare: 2011 No 5 s 61

Subpart 2—Duties to take remedial action

59 Data holder or accredited requestor must take prescribed steps to avoid, mitigate, or remedy loss or damage caused by contravention

(1) This section applies if—

(a) a person (**A**) contravenes a duty imposed under this Act; and

(b) A is a data holder or an accredited requestor; and

(c) a person (**B**) referred to in **subsection (3)** has suffered, or is likely to suffer, loss or damage because of the contravention.

(2) A must take the steps that are prescribed by the regulations to avoid, mitigate, or remedy that loss or damage.

(3) For the purposes of **subsection (1)(c)**, B is any of the following:

(a) a customer:

(b) a data holder or an accredited requestor (other than A).

(4) *See* **section 126(2)**, which relates to the regulations.

60 Person who has suffered loss or damage may recover amount as debt due

(1) This section applies if regulations made for the purposes of **section 59** require a person (**A**) to pay an amount to a person referred to in **section 59(3)** (**B**).

(2) B may recover the amount from A in any court of competent jurisdiction as a debt due to B.

Examples

Example 1

A data holder (**A**) contravenes this Act. The contravention causes a customer (**B**) to miss a payment. As a result, B is liable to pay a penalty charge to a third party. The regulations may require A to reimburse B for the penalty. B may recover the amount from A as a debt due.

Example 2

An accredited requestor (**A**) contravenes this Act. The contravention causes a customer to suffer a loss. A data holder (**B**) is a party to the relevant transaction, but was not in contravention of this Act. However, under an industry code, B is required to pay compensation to the customer. The regulations may require A to reimburse B for the compensation that B pays to the customer. B may recover the amount from A as a debt due.

61 Other remedies or powers not limited

Sections 59 and 60 do not limit—

(a) any other remedy that a person may obtain for the loss or damage that has been, or is likely to be, suffered because of the contravention referred to in **section 59**; or

(b) the powers of the chief executive or a court in respect of the contravention.

Subpart 3—Prohibition against taking certain actions against customer

62 When subpart applies

This subpart applies if a data holder or an accredited requestor contravenes a duty imposed under this Act in connection with a transaction involving a customer.

63 Prohibition against taking certain actions against customer

(1) The persons referred to in **subsection (2)** must not, in the circumstances prescribed in the regulations,—

(a) impose a financial penalty on a customer referred to in **section 62** (**C**) in connection with the transaction (for example, a penalty fee or penalty interest); or

(b) exercise a right, power, or remedy under a security interest in connection with the transaction; or

(c) take steps to enforce a debt incurred in connection with the transaction.

(2) The persons are the following:

(a) the data holder or accredited requestor that contravened the duty as referred to in **section 62** (**A**):

(b) another person that is a data holder or an accredited requestor (**B**).

(3) If, but for **subsection (1)**, B would have been able to impose a financial penalty on C, A must reimburse B for the amount of the penalty in the circumstances prescribed in the regulations.

(4) B may recover the amount from A in any court of competent jurisdiction as a debt due to B.

(5) In this section, **security interest** means an interest in property created or provided for by a transaction that in substance secures payment or performance of an obligation, without regard to—

(a) the form of the transaction; and

(b) the identity of the person who has title to the collateral.

Subpart 4—Prohibition against holding out

64 Prohibition against holding out

A person must not hold out that the person, or another person,—

(a) is an accredited requestor if that is not the case; or

(b) is lawfully able to do any of the following if that is not the case:

(i) make a particular kind of request in connection with a regulated data service; and

(ii) provide particular kinds of goods or services in connection with a regulated data service.

Subpart 5—Infringement offences

65 Infringement offences

(1) A person that is alleged to have committed an infringement offence may—

(a) be proceeded against by the filing of a charging document under section 14 of the Criminal Procedure Act 2011; or

(b) be issued with an infringement notice under **section 66**.

(2) Proceedings commenced in the way described in **subsection (1)(a)** do not require the leave of a District Court Judge or Registrar under section 21(1)(a) of the Summary Proceedings Act 1957.

(3) *See* section 21 of the Summary Proceedings Act 1957 for the procedure that applies if an infringement notice is issued.

66 When infringement notice may be issued

The chief executive may issue an infringement notice to a person if the chief executive believes on reasonable grounds that the person is committing, or has committed, an infringement offence.

67 Revocation of infringement notice before payment made

(1) The chief executive may revoke an infringement notice before—

(a) the infringement fee is paid; or

(b) an order for payment of a fine is made or deemed to be made by a court under section 21 of the Summary Proceedings Act 1957.

(2) The chief executive must take reasonable steps to ensure that the person to whom the notice was issued is made aware of the revocation of the notice.

(3) The revocation of an infringement notice before the infringement fee is paid is not a bar to any further action as described in **section 65(1)(a) or (b)** against the person to whom the notice was issued in respect of the same matter.

68 What infringement notice must contain

An infringement notice must be in the form prescribed in the regulations and must contain the following particulars:

(a) details of the alleged infringement offence that fairly inform a person of the time, place, and nature of the alleged offence:

(b) the amount of the infringement fee:

(c) the address of the chief executive:

(d) how the infringement fee may be paid:

(e) the time within which the infringement fee must be paid:

(f) a summary of the provisions of section 21(10) of the Summary Proceedings Act 1957:

(g) a statement that the person served with the notice has a right to request a hearing:

(h) a statement of what will happen if the person served with the notice neither pays the infringement fee nor requests a hearing:

(i) any other matters prescribed in the regulations.

69 How infringement notice may be served

(1) An infringement notice may be served on the person that the chief executive believes is committing or has committed the infringement offence by—

(a) delivering it to the person or, if the person refuses to accept it, bringing it to the person's notice; or

(b) leaving it for the person at the person's last known place of residence with another person who appears to be of or over the age of 14 years; or

(c) leaving it for the person at the person's place of business or work with another person; or

(d) if the person is a body corporate, delivering it to a director or an employee of the body corporate at its head office, principal place of business or work, or registered office, or by bringing it to the director's notice or the employee's notice if that person refuses to accept it; or

(e) sending it to the person by prepaid post addressed to the person's last known place of residence or place of business or work; or

(f) sending it to an electronic address of the person in any case where the person does not have a known place of residence or business in New Zealand.

(2) If the person is a body corporate,—

(a) **subsection (1)(a) to (c)** does not apply (but *see* **subsection (1)(d)** instead); and

(b) the infringement notice (or a copy of it) sent in accordance with **subsection (1)(e) or (f)** must be sent for the attention of a director or an employee of the body corporate.

(3) Unless the contrary is shown,—

(a) an infringement notice (or a copy of it) sent by prepaid post to a person under **subsection (1)** is to be treated as having been served on that person on the fifth working day after the date on which it was posted; and

(b) an infringement notice sent to a valid electronic address is to be treated as having been served at the time the electronic communication first entered an information system that is outside the control of the chief executive.

70 Payment of infringement fees

All infringement fees paid for infringement offences must be paid to the chief executive.

71 Reminder notices

A reminder notice must be in the form prescribed in the regulations and must include the same particulars, or substantially the same particulars, as the infringement notice.

Subpart 6—Civil liability

72 Civil liability remedies available under this subpart

(1) The following remedies (**civil liability remedies**) are available under this subpart:

(a) a pecuniary penalty order (with 2 tiers of penalties):

(b) a declaration of contravention:

(c) a compensatory order:

(d) an injunction.

(2) In this Act, **civil liability provision**—

(a) means any provision referred to in **section 74(1) or 75(1)**; and

(b) includes **section 63** (except for the purposes of **sections 73 to 79**).

Pecuniary penalty order

73 When High Court may make pecuniary penalty order

(1) The High Court may, on the application of the chief executive, order a person to pay to the Crown the pecuniary penalty that the court determines to be appropriate if the court is satisfied that the person has—

(a) contravened a civil liability provision; or

(b) attempted to contravene a civil liability provision; or

(c) been involved in a contravention of a civil liability provision.

(2) However, an order may not be made for a contravention, an attempted contravention, or an involvement in a contravention, of the following:

(a) a specified disclosure requirement (*see* **section 35**):

(b) a specified policy requirement (*see* **section 48**):

(c) a specified annual report requirement (*see* **section 114**).

(3) In this subpart, **relevant conduct** means the conduct giving rise to the contravention, attempted contravention, or involvement in the contravention referred to in **subsection (1)**.

74 Maximum penalty (Tier 1)

(1) This section applies to a contravention, an attempted contravention, or an involvement in a contravention of any of the following:

(a) **section 27** (data holder must operate electronic system for providing regulated data services):

(b) **section 42** (only customer, secondary user, or accredited requestor may request regulated data services):

(c) **section 44** (verification of identity of person who makes request).

(2) The maximum amount of a pecuniary penalty is—

(a) $500,000 for a contravention, an attempted contravention, or an involvement in a contravention by an individual; or

(b) $2,500,000 in any other case.

75 Maximum penalty (Tier 2)

(1) This section applies to a contravention, an attempted contravention, or an involvement in a contravention of any of the following:

(a) **section 14** (data holder must provide customer data to customer):

(b) **section 15** (data holder must provide customer data to accredited requestor if authorisation is confirmed):

(c) **section 18** (data holder must perform certain actions on customer's request):

(d) **section 19** (data holder must perform certain actions on accredited requestor's request if authorisation is confirmed):

(e) **section 21** (how data holders and accredited requestors must deal with joint customers):

(f) **section 22** (data holder must provide product data to any person):

(g) **section 24** (how data holders and accredited requestors must deal with secondary users):

(h) **section 28** (electronic system must comply with prescribed technical or performance requirements):

(i) **section 31** (data holders must comply with requirements for requests, providing services, and making information available):

(j) **section 33** (accredited requestors must comply with requirements for dealing with data and making information available):

(k) **section 38** (customer's authorisation must be confirmed):

(l) **section 39** (customer or secondary user must be able to control authorisation):

(m) **section 40** (accredited requestor must comply with prescribed duties in respect of authorisation):

(n) **section 41** (authorisation must not be required as condition of providing product):

(o) **section 47** (data holders and accredited requestors must have customer data, product data, and action performance policies):

(p) **section 49** (data holders and accredited requestors must have customer complaints process):

(q) **section 50** (data holder or accredited requestor must be member of dispute resolution scheme (if scheme has been prescribed)):

(r) **section 59** (data holder or accredited requestor must take prescribed steps to avoid, mitigate, or remedy loss or damage caused by contravention):

(s) **section 64** (prohibition against holding out):

(t) **section 112** (annual reporting by data holders):

(u) **section 113** (annual reporting by accredited requestors):

(v) **section 119** (persons that will become data holders when designation comes into force must provide information to chief executive):

(w) **section 120** (other data holders must provide information to chief executive).

(2) The maximum amount of a pecuniary penalty is—

(a) $200,000 for a contravention, an attempted contravention, or an involvement in a contravention by an individual; or

(b) $600,000 in any other case.

76 Considerations for court in determining pecuniary penalty

(1) In determining an appropriate pecuniary penalty that a person (**A**) must pay, the court must have regard to all relevant matters, including—

(a) the nature and extent of A's conduct; and

(b) the nature and extent of any loss or damage suffered by any person because of A's conduct; and

(c) any gains made or losses avoided by A; and

(d) whether a person has paid an amount of compensation, reparation, or restitution, or taken other steps to avoid, mitigate, or remedy any loss or damage suffered by another person because of A's conduct; and

(e) the circumstances in which A's conduct took place; and

(f) whether A has previously been found by a court in a proceeding under this Act, or any other legislation, to have engaged in any similar conduct.

(2) In this section, **A's conduct** means the conduct of A for which A is liable to the pecuniary penalty.

Declaration of contravention

77 Declaration of contravention

(1) The High Court must, on an application under **section 73**, make a declaration of contravention if it is satisfied that a person has contravened, or been involved in a contravention of, a civil liability provision.

(2) The High Court may also, on the application of the chief executive or any other person, make a declaration of contravention if it is satisfied that a person has contravened, or been involved in a contravention of, a civil liability provision.

78 Purpose and effect of declaration of contravention

(1) The purpose of a declaration of contravention is to enable an applicant for a compensatory order to rely on the declaration of contravention in the pro-

ceeding for that order, and not be required to prove the contravention or involvement in the contravention.

(2) Accordingly, a declaration of contravention is conclusive evidence of the matters that must be stated in it under **section 79**.

79 What declaration of contravention must state

A declaration of contravention must state the following:

(a) the provision to which the contravention or involvement in the contravention relates; and

(b) the person that engaged in the contravention or was involved in the contravention; and

(c) the conduct that constituted the contravention or involvement in the contravention.

Compensatory orders

80 When court or Disputes Tribunal may make compensatory orders

(1) The court or the Disputes Tribunal may make a compensatory order, on application by the chief executive or any other person, if the court or the Disputes Tribunal is satisfied that—

(a) a person has contravened a civil liability provision; and

(b) another person (the **aggrieved person**) has suffered, or is likely to suffer, loss or damage because of the contravention.

(2) The court or the Disputes Tribunal may make a compensatory order whether or not the aggrieved person is a party to the proceeding.

Guidance note

Section 95 provides for the Disputes Tribunal's jurisdiction under this section. In particular, the Disputes Tribunal may hear and determine an application for compensation only if the amount claimed does not exceed $30,000.

81 Terms of compensatory orders

(1) If **section 80** applies, the court or the Disputes Tribunal may make any order it thinks just to compensate an aggrieved person in whole or in part for the loss or damage, or to prevent or reduce the loss or damage, referred to in that section.

(2) An order may include an order to direct a relevant person to pay to the aggrieved person the amount of the loss or damage (in whole or in part).

(3) **Subsection (2)** does not limit **subsection (1)**.

(4) In this section, **relevant person** means—

(a) any person in contravention; or

(b) any person involved in the contravention.

Injunctions

82 Court may grant injunctions

The court may, on application by the chief executive or any other person, grant an injunction—

(a) restraining a person from engaging or continuing to engage in conduct that constitutes or would constitute a contravention, an attempted contravention, or an involvement in a contravention of a civil liability provision; or

(b) requiring a person to do an act or a thing if—

(i) that person has refused or failed, is refusing or failing, or is proposing to refuse or fail to do that act or thing; and

(ii) the refusal or failure was, is, or would be a contravention of a civil liability provision.

83 When court may grant restraining injunctions

(1) The court may grant an injunction restraining a person from engaging in conduct of a particular kind if—

(a) it is satisfied that the person has engaged in conduct of that kind; or

(b) it appears to the court that, if an injunction is not granted, it is likely that the person will engage in conduct of that kind.

(2) The court may grant an interim injunction restraining a person from engaging in conduct of a particular kind if in its opinion it is desirable to do so.

(3) **Subsections (1)(a) and (2)** apply whether or not it appears to the court that the person intends to engage again, or to continue to engage, in conduct of that kind.

(4) **Subsections (1)(b) and (2)** apply whether or not—

(a) the person has previously engaged in conduct of that kind; or

(b) there is an imminent danger of substantial damage to any other person if that person engages in conduct of that kind.

84 When court may grant performance injunctions

(1) A court may grant an injunction requiring a person to do an act or a thing that the person is required to do under a civil liability provision if—

(a) it is satisfied that the person has refused or failed to do that act or thing; or

(b) it appears to the court that, if an injunction is not granted, it is likely that the person will refuse or fail to do that act or thing.

(2) The court may grant an interim injunction requiring a person to do an act or a thing that the person is required to do under a civil liability provision if in its opinion it is desirable to do so.

(3) **Subsections (1)(a) and (2)** apply whether or not it appears to the court that the person intends to refuse or fail again, or to continue to refuse or fail, to do that act or thing.

(4) **Subsections (1)(b) and (2)** apply whether or not—

(a) the person has previously refused or failed to do that act or thing; or

(b) there is an imminent danger of substantial damage to any other person if the person refuses or fails to do that act or thing.

85 Chief executive's undertaking as to damages not required

(1) If the chief executive applies to the court for the grant of an interim injunction under this subpart, the court must not, as a condition of granting an interim injunction, require the chief executive to give an undertaking as to damages.

(2) In determining the chief executive's application for the grant of an interim injunction, the court must not take into account that the chief executive is not required to give an undertaking as to damages.

Rules of procedure

86 Rules of civil procedure and civil standard of proof apply

A proceeding under this subpart is a civil proceeding and the usual rules of court and rules of evidence and procedure for civil proceedings apply (including the standard of proof).

87 Limit on proceedings

(1) A proceeding under this subpart may be commenced within 3 years after the conduct giving rise to the contravention, attempted contravention, or involvement in the contravention was discovered or ought reasonably to have been discovered.

(2) However, no proceeding under this subpart may be commenced 10 years or more after the conduct giving rise to the contravention, attempted contravention, or involvement in the contravention occurred.

Relationship between proceedings and orders

88 More than 1 civil liability remedy may be given for same conduct

The court may grant a civil liability remedy of one kind against a person even though the court has granted another civil liability remedy of a different kind against the person for the same conduct.

Example

The court may make a compensatory order and a pecuniary penalty order for the same conduct.

89 Only 1 pecuniary penalty order may be made for same conduct

If conduct by a person constitutes a contravention, an attempted contravention, or an involvement in the contravention of 2 or more provisions,—

(a) a proceeding may be brought against that person for the contravention, attempted contravention, or involvement in the contravention of any 1 or more of the provisions; but

(b) no person is liable to more than 1 pecuniary penalty order for the same conduct.

90 No pecuniary penalty and criminal penalty for same conduct

A person cannot be ordered to pay a pecuniary penalty and be liable for a fine or to imprisonment under this Act or any other Act for the same conduct.

Defences

91 General defences for person in contravention

(1) In any proceeding under this subpart against a person (**A**) for a contravention of a civil liability provision, it is a defence if A proves that—

(a) A's contravention was due to reasonable reliance on information supplied by another person; or

(b) both of the following apply:

(i) A's contravention was due to the act or default of another person, or to an accident or to some other cause beyond A's control; and

(ii) A took reasonable precautions and exercised due diligence to avoid the contravention.

(2) For the purposes of **subsection (1)(a) and (b)**, **another person** does not include a director, an employee, or an agent of A.

(3) **Subsection (1)(b)** does not apply to a contravention of—

(a) **section 27**; or

(b) **section 28** to the extent that it requires a data holder to comply with a CPD reliability and availability requirement.

(4) In this section and **section 92**, **CPD reliability and availability requirement** means a requirement that is prescribed by the regulations or standards in connection with reliability or availability (or both) and that is specified by those regulations or standards for the purposes of this section.

92 Defence for contraventions due to technical fault

(1) In any proceeding under this subpart against a data holder (**A**) for a contravention of any of the provisions listed in **subsection (2)**, it is a defence if A proves that—

(a) A's contravention was due to a technical fault in its electronic system referred to in **section 27**; and

(b) A took reasonable precautions and exercised due diligence to avoid the contravention; and

(c) A is in compliance with **section 27** and the CPD reliability and availability requirements (*see* **section 91(4)**).

(2) The provisions are as follows:

(a) **sections 14, 15, 18, 19, and 22** (duties for data holder to provide data or perform actions):

(b) **section 38(2)** (duty for data holder to confirm authorisation):

(c) **section 44(2)** (duty for data holder to verify identity of person who makes a request).

Jurisdiction

93 Jurisdiction of High Court

The High Court may hear and determine the following matters:

(a) applications for orders, or for a court to exercise any other power, under any provision of this subpart:

(b) appeals arising from any proceeding in the District Court under this subpart.

94 Jurisdiction of District Court

The District Court may hear and determine applications for orders, or for a court to exercise any other power, under any of the provisions of **sections 80 to 85** if—

(a) the amount claimed does not exceed $350,000; or

(b) no amount is claimed; or

(c) the occasion for the making of the order or the exercise of the power arises in the course of civil proceedings properly before the court; or

(d) the parties consent, under section 81 of the District Court Act 2016, to the District Court having jurisdiction to hear and determine the application.

95 Jurisdiction of Disputes Tribunal

(1) The Disputes Tribunal established under section 4 of the Disputes Tribunal Act 1988 may hear and determine applications for orders to pay compensation under **sections 80 and 81** if the amount claimed does not exceed $30,000.

(2) An order of the Disputes Tribunal under this Act must not—

(a) require a person to pay an amount exceeding $30,000; or

(b) declare a person not liable to another person for an amount exceeding $30,000.

(3) An order of the Tribunal that exceeds any restriction specified in **subsection (2)** is entirely of no effect.

Part 5
Administrative matters

Subpart 1—Chief executive's functions

96 Chief executive's functions

The chief executive's functions under this Act are as follows:

(a) to act as the regulator of regulated data services, including by—

(i) issuing warnings, reports, or guidelines, or making comments, about any matter relating to regulated data services or persons engaged in conduct relating to those services (including in relation to 1 or more particular persons); and

(ii) accrediting persons as accredited requestors; and

(iii) issuing standards; and

(iv) keeping the register; and

(v) monitoring compliance with and enforcing this Act, including by investigating conduct that constitutes or may constitute a contravention, an attempted contravention, or an involvement in a contravention; and

(vi) taking appropriate action in respect of persons that have contravened, are contravening, have attempted to contravene, or are likely to contravene this Act, or have been involved, are involved, or are likely to be involved in a contravention of this Act; and

(vii) performing and exercising any other powers and duties conferred or imposed on the chief executive under this Act:

(b) to provide, or facilitate the provision of,—

(i) information to customers, data holders, accredited requestors, and the public generally that is relevant to the purpose of this Act; and

(ii) other information in connection with the functions or powers conferred or imposed on the chief executive under this Act:

(c) to co-operate with any other law enforcement or regulatory agency that carries out a role in relation to regulated data services:

(d) to keep under review the law and practices that are relevant to the chief executive's other functions under this section (including overseas law and practices).

Subpart 2—Designation regulations

97 Designation regulations

(1) The Governor-General may, by Order in Council, on the recommendation of the Minister, make regulations that set out matters referred to in **section 100** (**designation regulations**).

(2) Regulations made under this section are secondary legislation (*see* Part 3 of the Legislation Act 2019 for publication requirements).

98 Minister must have regard to certain matters

(1) Before recommending that designation regulations be made, the Minister must have regard to the following:

(a) the interests of customers, including Māori customers:

(b) any likely costs and benefits for the person or class of persons that are proposed to become data holders:

(c) whether the regulations promote the implementation of secure, standardised, and efficient regulated data services:

(d) the likely benefits and risks associated with the proposed designation regulations in relation to—

(i) the security, privacy, confidentiality, or other sensitivity of customer data and product data; and

(ii) any intellectual property rights that may exist in relation to customer data or product data.

(2) In this section, **intellectual property rights** includes patents, designs, trade marks, copyrights, plant variety rights, know-how, confidential information, trade secrets, and similar rights.

99 Minister must consult on proposed designation

(1) Before recommending that designation regulations be made, the Minister must consult the following about the proposed designation:

(a) the persons, or representatives of the persons, that the Minister considers will be substantially affected by the proposed designation regulations:

(b) the Privacy Commissioner:

(c) 1 or more people who have expert knowledge of te ao Māori approaches to data (for example, approaches to data access, use, or protection).

(2) The Minister must decide which people to consult under **subsection (1)(c)** after taking into account the particular subject matter of the proposed designation regulations.

(3) **Subsection (1)(c)** does not apply to regulations that amend other regulations if the Minister is satisfied that the amendments—

(a) are only correcting minor errors; or

(b) are otherwise of a minor or technical nature only.

(4) A failure to comply with this section does not affect the validity of the designation regulations.

100 Contents of designation regulations

(1) Designation regulations may set out all or any of the following:

Designated persons: data holders

(a) the persons or classes of persons (or both) being designated for the purposes of **section 6**:

Designated data

(b) the customer data or classes of customer data (or both) being designated as designated customer data for the purposes of 1 or more provisions of this Act:

(c) the product data or classes of product data (or both) being designated as designated product data for the purposes of 1 or more provisions of this Act:

(d) matters for the purposes of **sections 8(3)(b) and 9(3)(b)**:

Designated actions

(e) the action or classes of action (or both) being designated as designated actions for the purposes of 1 or more provisions of this Act:

Classes of accreditation

(f) the classes of accreditation that may be granted in relation to the designation regulations:

Secondary users

(g) the persons or classes of persons (or both) being designated as secondary users (including specifying approval or other requirements or eligibility criteria to be met before a person may be a secondary user).

(2) For the purposes of **subsection (1)(c)**, data or classes of data may be designated as designated product data only to the extent that they relate to any of the following:

(a) a description of a product or any feature of the product:

(b) any criteria for being eligible to acquire the product:

(c) any terms or conditions for the supply of the product:

(d) the price of the product:

(e) any other data about the product that is of a kind that is ordinarily publicly available.

(3) For the purposes of **subsection (1)(f) and (g)**, a class of accreditation or a class of secondary user may be defined by reference to any 1 or more of the following:

(a) data holders or any class of data holders:

(b) customers or any class of customers:

(c) designated customer data or any class of that data:

(d) designated product data or any class of that data:

(e) designated actions or any class of those actions:

(f) any matters relating to the business, operation, or management of an accredited requestor or secondary user to which the class applies (for example, the services that an accredited requestor may provide to a customer):

(g) limits or restrictions on the classes of—

(i) requests that an accredited requestor may make:

(ii) requests or authorisations (or both) that a secondary user may make or give:

(h) any other circumstances in which—

(i) an accredited requestor may make a request:

(ii) a secondary user may make a request or give an authorisation.

(4) *See* **section 119**, which requires persons that will become data holders to provide information to the chief executive.

Example

Designation regulations may designate—

- banks for the purposes of **section 6** (data holders):
- the transaction histories of a bank's customers as a class of designated customer data:
- the home loan interest rates offered by a bank as a class of designated product data:

- making payments or opening a new account as classes of designated actions.

Subpart 3—Accreditation of requestors

101 Application for accreditation

A person may apply to the chief executive to be accredited as an accredited requestor.

102 How application is made

The application must—

(a) specify 1 or more designation regulations in relation to which the accreditation is requested; and

(b) specify the classes of accreditation requested; and

(c) specify the applicant's New Zealand Business Number; and

(d) contain the information specified by the regulations (if any); and

(e) be accompanied by the fee prescribed by the regulations (if any); and

(f) otherwise be made in the manner prescribed by the regulations (if any).

103 Application may be made before designation regulations fully in force

(1) A person may apply for accreditation in relation to designation regulations before those regulations fully come into force.

(2) For the purposes of dealing with the application, any provisions of the designation regulations that are relevant to the matter and that are not yet in force must be treated as if they were in force.

104 Chief executive must verify applicant's identity

The chief executive must take reasonable steps to verify each applicant's identity so that the chief executive is satisfied that they know who the applicant is.

105 Decision by chief executive

(1) The chief executive must—

(a) have regard to the matters specified in the regulations (if any) before making a decision; and

(b) otherwise make the decision in the manner prescribed in the regulations (if any).

(2) The chief executive may accredit an applicant if—

(a) the application meets the requirements of **section 102**; and

(b) they know who the applicant is under **section 104**; and

(c) the applicant meets the criteria or other requirements prescribed by the regulations (if any); and

(d) the applicant's directors, senior managers, proposed directors, and proposed senior managers meet the criteria or other requirements prescribed by the regulations (if any); and

(e) if **section 50** will apply to the applicant, the applicant is, or will be, a member of a dispute resolution scheme for the purposes of that section on and from commencing to act as an accredited requestor.

(3) The chief executive may grant the application—

(a) in full or in part; and

(b) on the terms and conditions that they think fit, including—

(i) specifying the date of expiry of the accreditation; and

(ii) specifying the class or classes of accreditation; and

(iii) imposing conditions relating to the matters, criteria, and requirements referred to in **subsection (1)(a) and (2)(c)** (for example, to ensure that the criteria or requirements continue to be satisfied and to require verification that those criteria and requirements continue to be satisfied).

(4) Those terms and conditions may be more limited or restrictive than those requested in the application (for example, more restrictive as to the classes of accreditation that are granted).

106 Notice of decision

(1) The chief executive must give notice of their decision to the applicant.

(2) If the chief executive declines the application (whether in full or in part) or imposes terms or conditions that are more limited or restrictive than those requested in the application, the chief executive must also set out their reasons for doing so.

(3) If an application is successful (whether in full or in part), the chief executive must also give the applicant the following information:

(a) the name of the designation regulations in relation to which the accreditation is granted:

(b) the classes of accreditation granted.

107 Application to modify accreditation

(1) An accredited requestor may apply to the chief executive to modify the terms or conditions of its accreditation, including—

(a) to add or remove designation regulations in relation to which the accreditation is granted; and

(b) to add or remove classes of accreditation.

(2) After deciding the application, the chief executive must give the applicant the information specified in **section 106(3)**.

(3) **Sections 102 to 106** apply to the making of an application under this section as if it were an original application for accreditation (except to the extent that this Act or the regulations provide different requirements for applications for modifications).

108 Duration of accreditation

(1) An accredited requestor's accreditation starts when the accreditation is registered and ends when the accreditation is removed from the register.

(2) The chief executive must remove an accreditation from the register as soon as practicable after—

(a) the accredited requestor tells the chief executive that it no longer wishes to remain accredited as an accredited requestor; or

(b) the chief executive cancels the accreditation; or

(c) the date of expiry of the accreditation (unless **section 109(2)** applies); or

(d) the chief executive decides not to renew the accreditation on a renewal application referred to in **section 109(2)**.

109 Renewal of accreditation

(1) An accredited requestor may apply to renew its accreditation.

(2) If a renewal application is made on or before the date of expiry of an accredited requestor's accreditation, the accreditation continues to have effect until the renewal application is decided by the chief executive.

(3) If the accredited requestor's accreditation expires before a renewal application is made, instead of a renewal application, the accredited requestor must make a fresh application for accreditation under **section 101**.

(4) A renewal application must be made in the manner prescribed by the regulations (if any).

(5) **Sections 102 to 106** apply to the making of a renewal application under this section as if it were an original application for accreditation (except to the extent that this Act or the regulations provide different requirements for renewal applications).

110 When chief executive may suspend or cancel accreditation

The chief executive may suspend (for a specified period or until a specified requirement is met) or cancel an accreditation if—

(a) the accredited requestor, by written notice, requests the chief executive to do so; or

(b) the requirements referred to in **section 105(2)(b) to (e)** are no longer met in respect of the accredited requestor; or

(c) the chief executive is satisfied that the accredited requestor is incapacitated, has ceased to exist, or has become subject to an insolvency event within the meaning of section 6(4) of the Financial Markets Conduct Act 2013; or

(d) the chief executive is satisfied that the accredited requestor has materially contravened a term or condition of the accreditation or any other requirement imposed under this Act.

Subpart 4—Appeals

111 Appeals against accreditation decisions

A person may appeal to the High Court against a decision of the chief executive under **subpart 3** to—

(a) decline to grant accreditation to a person; or

(b) decline to renew a person's accreditation; or

(c) impose terms or conditions on a person's accreditation; or

(d) decline an application to modify a person's accreditation; or

(e) suspend or cancel a person's accreditation.

Subpart 5—Annual reporting by data holders and accredited requestors

112 Annual reporting by data holders

(1) A data holder must give to the chief executive, before 31 October in each year, an annual report.

(2) The report must—

(a) relate to the preceding 12-month period ending on 30 June; and

(b) set out—

(i) a summary of the complaints made about the data holder's conduct in connection with regulated data services that it provides; and

(ii) the information prescribed by the regulations for the purposes of this paragraph (if any).

(3) The data holder must otherwise provide the report in the manner prescribed by the regulations (if any).

113 Annual reporting by accredited requestors

(1) An accredited requestor must give to the chief executive, before 31 October in each year, an annual report.

(2) The report must—

(a) relate to the preceding 12-month period ending on 30 June; and

(b) set out—

(i) a summary of the complaints made about the accredited requestor's conduct in connection with regulated data services that it requests; and

(ii) a description of the goods or services that the accredited requestor provides in connection with the regulated data services that it requests; and

(iii) the information prescribed by the regulations for the purposes of this paragraph (if any).

(3) The accredited requestor must otherwise provide the report in the manner prescribed by the regulations (if any).

114 Contravention of specified annual report requirement is infringement offence

(1) A person that contravenes a specified annual report requirement commits an infringement offence and is liable to—

(a) an infringement fee of $20,000; or

(b) a fine imposed by a court not exceeding $50,000.

(2) In this section and **section 73**, **specified annual report requirement** means a requirement imposed under **section 112 or 113** that is specified by the regulations for the purposes of this section.

Subpart 6—Crown organisations

115 Crown organisations may be customer, data holder, or accredited requestor

(1) An instrument of the Crown that is a Crown organisation (whether or not a body corporate)—

(a) must be treated as if it were a separate legal personality for the purpose of complying with this Act; and

(b) may be a customer, a data holder, or an accredited requestor in its own right.

(2) An instrument of the Crown that is neither a Crown organisation nor a body corporate—

(a) does not have separate legal personality; and

(b) cannot be a customer, a data holder, or an accredited requestor in its own right.

(3) In this section, **Crown organisation** has the same meaning as in section 4 of the Crown Organisations (Criminal Liability) Act 2002.

Compare: 2015 No 70 s 5

Subpart 7—Register

116 Register of participants in customer and product data system

A register called the register of participants in the customer and product data system is established.

117 Purposes of register

The purposes of the register are to—

(a) enable any person to—

(i) confirm whether a person is a data holder or an accredited requestor; and

(ii) obtain certain information about data holders and accredited requestors; and

(b) enable data holders and accredited requestors to access certain information about each other; and

(c) assist any person in the performance or exercise of the person's functions, powers, or duties under this Act or any other legislation.

118 Operation of register

(1) The chief executive must, in accordance with the regulations, keep the register as an electronic register.

(2) The register must be operated at all times unless—

(a) the chief executive suspends the operation of the register, in whole or in part, in accordance with **subsection (3)**; or

(b) otherwise provided in regulations.

(3) The chief executive may refuse access to the register or otherwise suspend the operation of the register, in whole or in part, if the chief executive considers that it is not practicable to provide access to the register.

119 Persons that will become data holders when designation comes into force must provide information to chief executive

(1) This section applies if—

(a) designation regulations have been made but a provision under **section 100(1)(a)** (designated persons) has not yet come into force; and

(b) a person (**A**) knows, or ought reasonably to know, that it is likely to become a data holder when the provision comes into force.

(2) A must, in the manner prescribed by the regulations (if any), provide the following information to the chief executive at least 20 working days before the provision under **section 100(1)(a)** comes into force:

(a) A's name and New Zealand Business Number:

(b) a physical address for service in New Zealand for A:

(c) the designation regulations in relation to which A is likely to be designated:

(d) the identifying information and contact details for A that are prescribed by the regulations:

(e) the information prescribed by the regulations to be included in the register under **section 121**:

(f) the information prescribed by the regulations to be included in the register under **section 122**.

120 Other data holders must provide information to chief executive

(1) This section applies to a person (**A**) that is a data holder under designation regulations unless A has previously complied with **section 119** in respect of those regulations.

(2) A must, in the manner prescribed by the regulations (if any), provide the following information to the chief executive within 20 working days after it becomes aware that it has become a data holder:

(a) A's name and New Zealand Business Number:

(b) a physical address for service in New Zealand for A:

(c) the designation regulations in relation to which A is designated:

(d) the identifying information and contact details for A that are prescribed by the regulations:

(e) the information prescribed by the regulations to be included in the register under **section 121**:

(f) the information prescribed by the regulations to be included in the register under **section 122**.

121 Contents of register that is publicly available

(1) The register must contain—

(a) the following information about each data holder (**A**):

(i) A's name and New Zealand Business Number:

(ii) the designation regulations in relation to which A is designated:

(iii) the classes of customer data and product data that A has to provide and the dates from which A must do so:

(iv) the classes of action requests that A has to perform and the dates from which A must do so:

(v) how customers may make a complaint about A's conduct in connection with regulated data services that A provides:

(vi) how customers may contact A about those services; and

(b) the following information about each accredited requestor (**B**):

(i) B's name and New Zealand Business Number:

(ii) the designation regulations in relation to which B is accredited:

(iii) each class of accreditation held by B:

(iv) how customers may make a complaint about B's conduct in connection with regulated data services that B requests:

(v) how customers may contact B about those services; and

(c) the information prescribed for the purposes of this paragraph (if any).

(2) The chief executive must ensure that the information referred to in this section is publicly available.

122 Contents of register that is available to data holders and accredited requestors (other than information publicly available under section 121)

(1) The register must contain the information prescribed by the regulations for the purposes of this section.

(2) The chief executive must ensure that the information prescribed by the regulations for the purposes of this section is reasonably available to data holders and accredited requestors.

Subpart 8—Information sharing

123 Sharing of information with certain law enforcement or regulatory agencies

(1) The chief executive may provide to a person or an agency specified in **subsection (2)** any information that the chief executive—

(a) holds in relation to the performance or exercise of the chief executive's functions, powers, or duties under this Act; and

(b) considers may assist the person or agency to perform or exercise the person's functions, powers, or duties under any legislation.

(2) The persons or agencies are any of the following:

(a) the Commerce Commission:

(b) the Department of Internal Affairs:

(c) the Ministry of Justice:

(d) the Privacy Commissioner:

(e) the Trust Framework Authority established under section 58 of the Digital Identity Services Trust Framework Act 2023:

(f) a person or an agency that is prescribed by the regulations for the purposes of this section.

(3) The chief executive may use any information provided to it by any person or agency referred to in **subsection (2)** in the chief executive's performance or exercise of their functions, powers, or duties under this Act.

(4) This section applies despite anything to the contrary in any contract, deed, or document.

(5) This section does not limit any provision of this Act or any other legislation that allows the chief executive to use or disclose information.

124 Conditions that may be imposed on providing information under this subpart

(1) The chief executive may impose any conditions in relation to providing information under this subpart.

(2) The chief executive must, in considering what conditions to impose, have regard to whether conditions are necessary or desirable in order to protect the privacy of any individual.

(3) The conditions may include, without limitation, conditions relating to—

(a) maintaining the confidentiality of anything provided (in particular, information that is personal information within the meaning of the Privacy Act 2020):

(b) the storing of, the use of, or access to anything provided:

(c) the copying, returning, or disposing of copies of documents provided:

(d) payment of the costs incurred by the chief executive in providing any information under this subpart.

125 Restriction on publication, disclosure, or use

If information is provided to a person or an agency under this subpart, the person or agency may publish, disclose, or use the information only if the publication, disclosure, or use—

(a) is authorised by the chief executive and is in accordance with any conditions imposed by the chief executive; or

(b) is for the purposes of, or in connection with, the functions, powers, or duties of a person under any legislation.

Subpart 9—Regulations, standards, and exemptions

Regulations

126 General regulations

(1) The Governor-General may, by Order in Council, on the recommendation of the Minister, make regulations for all or any of the following purposes:

(a) providing for anything that this Act says may or must be provided for by regulations:

(b) prescribing, for the purposes of any provision of this Act that requires a thing to be done in a manner prescribed by the regulations, the manner in which the thing must be done, including prescribing—

(i) by whom, when, where, and how the thing must be done:

(ii) the form that must be used in connection with doing the thing:

(iii) what information or other evidence or documents must be provided in connection with the thing:

(iv) requirements with which information, evidence, or documents that are provided in connection with the thing must comply:

(c) authorising the chief executive to determine or prescribe by notice any of the matters under **paragraph (b)**:

(d) prescribing matters for the purposes of **section 59** (remedial actions):

(e) prescribing procedures, requirements, and other matters, not inconsistent with this Act, for the register, including matters that relate to—

(i) the operation of the register:

(ii) the form of the register:

(iii) the information to be contained in the register:

(iv) access to the register:

(v) search criteria for the register:

(vi) circumstances in which amendments must be made to the register:

(f) specifying requirements about how the standards may be made (for example, matters that the chief executive must have regard to):

(g) if this Act says that anything may or must be provided for by regulations or standards, prescribing limits or restrictions on providing for that thing in standards (*see* **section 133**):

(h) providing for anything incidental that is necessary for carrying out, or giving full effect to, this Act.

(2) If the regulations under **subsection (1)(d)** require a data holder or an accredited requestor (**A**) to pay an amount to, or on account, of a person referred to in **section 59(3)** (**B**), the Minister may make a recommendation only if the Minister is satisfied that—

(a) the amount is to reimburse or compensate B for a cost or an expense that B has incurred as a result of a contravention of a duty imposed under this Act; and

(b) the nature and extent of the cost or expense is readily ascertainable; and

(c) there is a reasonably close connection between the contravention and the cost or expense that has been incurred.

(3) Regulations made under this section are secondary legislation (*see* Part 3 of the Legislation Act 2019 for publication requirements).

(4) If regulations made under **subsection (1)(c)** authorise the chief executive to determine or prescribe matters by notice,—

(a) a notice made under the regulations is secondary legislation (*see* Part 3 of the Legislation Act 2019 for publication requirements); and

(b) the regulations must contain a statement to that effect.

127 Regulations relating to fees and charges

(1) The Governor-General may, by Order in Council, on the recommendation of the Minister, make regulations for all or any of the following purposes:

(a) requiring the payment to the chief executive of fees and charges—

(i) by any accredited requestor in connection with the performance or exercise by the chief executive of any function, power, or duty under this Act:

(ii) on an application or a request from any person to the chief executive to perform or exercise any function, power, or duty under this Act:

(b) prescribing the amounts of those fees and charges or the manner in which those fees and charges are to be calculated.

(2) Regulations may authorise the chief executive to refund or waive, in whole or in part and on any conditions that may be prescribed, payment of the fee or charge in relation to any 1 or more named persons.

(3) Regulations made under this section are secondary legislation (*see* Part 3 of the Legislation Act 2019 for publication requirements).

128 Miscellaneous provisions relating to fees and charges

(1) The chief executive may refuse to perform a function or exercise a power until the prescribed fee or charge is paid.

(2) Any fee or charge payable to the chief executive under this Act is recoverable by the chief executive in any court of competent jurisdiction as a debt due to the chief executive.

129 Levies payable by data holders and accredited requestors

(1) Every person that is included in a prescribed class of specified persons must pay to the Crown, or a prescribed person on behalf of the Crown, a levy prescribed by the regulations.

(2) In this section and **section 130**, **specified person** means—

(a) a data holder; and

(b) an accredited requestor.

(3) The Governor-General may, by Order in Council, on the recommendation of the Minister, make regulations providing for the levies.

(4) Levies must be prescribed on the basis that the following costs should be met fully out of the levies:

(a) a portion of the costs of the chief executive in performing or exercising their functions, powers, and duties under this Act, where the size of the portion to be met by levies under this Act is determined by the Minister; and

(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)**; and

(c) the costs of collecting the levy money.

(5) Levies may be prescribed on the basis that any actual cost that could have been, but has not been, recovered as a levy shortfall for a year may be recovered (along with any financing charge) over any period of up to 5 years.

(6) The regulations may—

(a) specify the class or classes of specified persons that are required to pay a levy:

(b) specify the amount of levies, or method of calculating or ascertaining the amount of levies:

(c) include in levies, or provide for the inclusion in levies of, any shortfall in recovering the actual costs:

(d) refund, or provide for refunds of, any over-recovery of the actual costs:

(e) provide for the payment and collection of levies:

(f) provide different levies for different classes of specified persons:

(g) specify the financial year or part financial year to which a levy applies, and apply that levy to that financial year or part financial year and each subsequent financial year until the levy is revoked or replaced:

(h) require payment of a levy for a financial year or part financial year, irrespective of the fact that the regulations may be made after that financial year has commenced:

(i) authorise a person to whom a levy is payable to refund or waive, in whole or in part and on the conditions that may be prescribed, payment of the levy by 1 or more named persons.

(7) Regulations made under this section are secondary legislation (*see* Part 3 of the Legislation Act 2019 for publication requirements).

130 Miscellaneous provisions relating to levies

(1) If a person is in 2 or more classes of specified persons in respect of which different levies have been prescribed under **section 129**, the person must pay each of those levies (unless the regulations provide otherwise).

(2) The amount of any unpaid levy is recoverable in any court of competent jurisdiction as a debt due to the chief executive, or to any other person prescribed for the purposes of this subsection, on behalf of the Crown.

(3) The chief executive, or any other person prescribed for the purposes of this subsection, must ensure that each levy payment is paid into a Crown Bank Account and is separately accounted for.

131 Minister must consult on proposed regulations

(1) Before recommending that regulations be made under this subpart, the Minister must consult the following about the proposed regulations:

(a) the persons, or representatives of the persons, that the Minister considers will be substantially affected by the proposed regulations:

(b) the Privacy Commissioner:

(c) 1 or more people who have expert knowledge of te ao Māori approaches to data (for example, approaches to data access, use, or protection).

(2) The Minister must decide which people to consult under **subsection (1)(c)** after taking into account the particular subject matter of the proposed regulations.

(3) **Subsection (1)(c)** does not apply to regulations made under **section 129**.

(4) **Subsection (1)(c)** does not apply to regulations that amend other regulations if the Minister is satisfied that—

(a) the amendments are only correcting minor errors; or

(b) the amendments are otherwise of a minor or technical nature only; or

(c) it is necessary or desirable in the public interest that the amendments be made urgently.

(5) This section does not apply to regulations made under **section 126(1)(c) or (f)**.

(6) A failure to comply with this section does not affect the validity of the regulations.

Standards

132 Standards

(1) The chief executive may make 1 or more standards—

(a) providing for anything that this Act says must or may be provided for by the standards; and

(b) prescribing, for the purposes of any provision of this Act that requires a thing to be done in a manner prescribed by the standards, the manner in which the thing must be done, including prescribing—

(i) by whom, when, where, and how the thing must be done:

(ii) the form that must be used in connection with doing the thing:

(iii) what information or other evidence or documents must be provided in connection with the thing:

(iv) requirements with which information, evidence, or documents that are provided in connection with the thing must comply.

(2) If the standards are inconsistent with the regulations, the regulations prevail to the extent of the inconsistency.

(3) Standards made under this section are secondary legislation (*see* Part 3 of the Legislation Act 2019 for publication requirements).

133 Chief executive must comply with prescribed requirements and be satisfied that standards are consistent with any prescribed limits or restrictions

Before making a standard, the chief executive must—

(a) comply with any requirements prescribed by the regulations under **section 126(1)(f)**; and

(b) be satisfied that the standards are consistent with any limits or restrictions prescribed by the regulations (*see* **section 126(1)(g)**).

134 Chief executive's consultation on proposed standards

(1) Before making a standard, the chief executive must consult the following:

(a) the persons, or representatives of the persons, that the chief executive considers will be substantially affected by the issue of the proposed standard:

(b) the Privacy Commissioner:

(c) 1 or more people who have expert knowledge of te ao Māori approaches to data (for example, approaches to data access, use, or protection).

(2) The chief executive must decide which people to consult under **subsection (1)(c)** after taking into account the particular subject matter of the proposed standards.

(3) **Subsection (1)(c)** does not apply to a standard that amends another standard if the chief executive is satisfied that—

(a) the amendment is only correcting a minor error; or

(b) the amendment is otherwise of a minor or technical nature only; or

(c) it is necessary or desirable in the public interest that the amendment be made urgently.

(4) If the chief executive relies on **subsection (3)(c)**, the chief executive must publish a statement of their reasons for acting under that paragraph.

(5) A failure to comply with this section does not affect the validity of the standards.

Exemptions

135 Exemptions

(1) The Governor-General may, by Order in Council, made on the recommendation of the Minister, make regulations exempting (on terms and conditions, if any) classes of persons from any requirement under this Act.

(2) Before making a recommendation, the Minister must—

(a) have regard to the purpose of this Act as specified in **section 3**; and

(b) be satisfied that the extent of the exemption is not broader than is reasonably necessary to address the matters that gave rise to the regulations.

(3) The Minister's reasons for making the recommendation (including why an exemption is appropriate) must be published together with the regulations.

(4) Regulations made under this section are secondary legislation (*see* Part 3 of the Legislation Act 2019 for publication requirements).

136 Effect of breach of term or condition of exemption

A breach of a term or condition of an exemption granted under this subpart is a breach of the obligation for which the exemption applies (unless the terms of the exemption otherwise provide).

Subpart 10—Miscellaneous

137 No contracting out

(1) This Act has effect despite any provision to the contrary in any agreement.

(2) A data holder that purports to contract out of any provision of this Act commits an offence against section 13(i) of the Fair Trading Act 1986.

Example

A data holder enters into a contract with a customer. Under the contract, the data holder purports to contract out of its duty to provide data to the customer under **section 14**.

The data holder commits an offence.

138 Chief executive's warnings, reports, guidelines, or comments protected by qualified privilege

For the purposes of clause 3 of Part 2 of Schedule 1 of the Defamation Act 1992, any warning, report, guideline, or comment issued or made by the chief

executive in the course of the performance or intended performance of their functions must be treated as an official report made by a person holding an inquiry under the authority of the Parliament of New Zealand.

139 Notices

(1) A notice served by the chief executive for the purposes of **section 29 or 54** is sufficiently served if it is—

(a) in writing; and

(b) served in accordance with **section 140**.

(2) All documents purporting to be signed by or on behalf of the chief executive must, in all courts and in all proceedings under this Act, be treated as having been so signed with due authority unless the contrary is proved.

Compare: 2011 No 5 s 62

140 Service of notices

(1) A notice required or authorised to be served on any person for the purposes of **section 29 or 54** may—

(a) be served on an individual—

(i) by delivering it personally or by an agent (such as a courier) to the person; or

(ii) by sending it by post addressed to the person at the person's usual or last known place of residence or business; or

(iii) by sending it by email to the person's email address provided by the person for the purpose; or

(iv) in any other manner a District Court Judge directs:

(b) be served on a company, within the meaning of the Companies Act 1993, in a manner provided for in section 388 of that Act:

(c) be served on an overseas company in a manner provided for in section 390 of the Companies Act 1993:

(d) be served on any other body corporate in a manner in which it could be served if the body corporate were a company within the meaning of the Companies Act 1993.

(2) In the absence of proof to the contrary, a notice sent to a person in accordance with—

(a) **subsection (1)(a)(ii)** must be treated as having been served on the person when it would have been delivered in the ordinary course of post; and, in proving the delivery, it is sufficient to prove that the notice was properly addressed and posted:

(b) **subsection (1)(a)(iii)** must be treated as having been served on the person on the second working day after the day on which it is sent.

(3) Section 392 of the Companies Act 1993 applies for the purposes of **subsection (1)(b) to (d)**.

(4) If a person is absent from New Zealand, a notice served on the person's agent in New Zealand in accordance with **subsection (1)** must be treated as having been served on the person.

(5) If a person has died, the notice may be served, in accordance with **subsection (1)**, on their personal representative.

Compare: 2011 No 5 s 63

Subpart 11—Consequential amendments

Amendment to Disputes Tribunal Act 1988

141 Principal Act

Section 142 amends the Disputes Tribunal Act 1988.

142 Schedule 1 amended

In Schedule 1, Part 2, insert in its appropriate alphabetical order:

Customer and Product Data Act **2024**

Amendments to Privacy Act 2020

143 Principal Act

Sections 144 and 145 amend the Privacy Act 2020.

144 Section 75 amended (Referral of complaint to another person)

After section 75(1)(d), insert:

(e) the chief executive within the meaning of **section 5** of the Customer and Product Data Act **2024**.

145 Section 208 amended (Consultation)

After section 208(1)(d), insert:

(e) the chief executive within the meaning of **section 5** of the Customer and Product Data Act **2024**.

Amendment to Summary Proceedings Act 1957

146 Principal Act

Section 147 amends the Summary Proceedings Act 1957.

147 Section 2 amended (Interpretation)

In section 2(1), definition of **infringement notice**, after paragraph (ba), insert:

(bb) **section 66** of the Customer and Product Data Act **2024**; or

Schedule 1
Transitional, savings, and related provisions

s 12

Part 1
Provisions relating to this Act as enacted

There are no transitional, savings, or related provisions in this Act as enacted.

Wellington, New Zealand:
Published under the authority of the New Zealand Government—2024