MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT
HĪKINA WHAKATUTUKI

COVERSHEET

Minister	Hon Dr David Clark	**Portfolio**	Commerce and Consumer Affairs
Title of Cabinet paper	Further decisions on the consumer data right	**Date to be published**	19 December 2022

List of documents that have been proactively released		
Date	**Title**	**Author**
27 July 2022	Further decisions on the consumer data right	Office of the Minister of Commerce and Consumer Affairs
27 July 2022	DEV-22-MIN-0151 - Consumer Data Right: Further Decisions	Cabinet Office
15 March 2022	2122-2226 - Updated Consumer Data Right	MBIE
July 2022	Supplementary Regulatory Impact Statement: Further decisions on establishing a consumer data right	MBIE

Information redacted **YES**

Any information redacted in this document is redacted in accordance with MBIE's policy on Proactive Release and is labelled with the reason for redaction. This may include information that would be redacted if this information was requested under Official Information Act 1982. Where this is the case, the reasons for withholding information are listed below. Where information has been withheld, no public interest has been identified that would outweigh the reasons for withholding it.

MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT
HĪKINA WHAKATUTUKI

Supplementary Regulatory Impact Statement: Further decisions on establishing a consumer data right

Section 1: General information

Purpose
The Ministry of Business, Innovation and Employment is solely responsible for the analysis and advice set out in this Regulatory Impact Statement, except as otherwise explicitly indicated. This analysis and advice has been produced for the purpose of informing policy decisions to be taken by Cabinet.

Key Limitations or Constraints on Analysis
On 5 July 2021 the Government agreed to establish a Consumer Data Right (**CDR**), to give consumers greater choice and control over their data. The CDR will require businesses that hold data (**data holders**) to share prescribed data that they hold about consumers (**CDR data**) with trusted third parties (**data recipients**), at the consumer's request and with their consent. The CDR will be rolled out on a sector-by-sector basis via designations made by the responsible Minister. This RIS summarises our analysis on some of the remaining policy decisions, as below, and should be read alongside MBIE's June 2021 RIS titled *Regulatory Impact Statement: Establishing a Consumer Data Right*: • Institutional arrangements • Enforcement and penalties • Cost recovery The analysis in this RIS is informed by public consultation on a discussion paper in August 2020, and informal meetings with stakeholders, including private sector organisations, Government departments and Crown entities. We have not publicly consulted on some of the detailed matters set out in the RIS, but it is intended that there will be public consultation on an exposure draft of the Consumer Data Right Bill (**the Bill**)prior to introduction.

Responsible Manager
Authorised by: Glen Hildreth Competition & Consumer Policy Ministry of Business, Innovation and Employment 04 May 2022

Section 2: Problem definition and objectives

2.1 What is the policy problem or opportunity?

In August 2020, MBIE released a discussion document on options for establishing a consumer data right in New Zealand. The term 'consumer data right' describes a mechanism for consumers to securely share data that is held about them with trusted third parties. The third party could be another product or service provider or a separate entity such as a fintech. The data would be shared in a machine-readable format so that it can be utilised by the third party for the consumer's benefit.

This will allow consumers to securely share data that is held about them with trusted third parties, using standardised data formats and interfaces.

2.2 Who is affected and how?

A consumer data right will provide significant benefits for consumer welfare and economic development. Over time, it will give individuals and businesses access to a wider range of products and services, reduce search and switch costs, facilitate competition, encourage innovation, increase productivity and help build the digital economy. A consumer data right will also strengthen existing privacy protections by giving consumers greater choice and control of their data.

On 5 July 2021, Cabinet decided to implement a new legislative framework for a consumer data right. Cabinet agreed to the main features of the legislative framework. It also agreed that the CDR regime would be rolled out on a sector-by-sector basis, with the Minister designating individual markets, industries and sectors to which it applies. The cost recovery institutional arrangements, consumer redress, and compliance and enforcement settings are yet to be decided by Cabinet.

2.3 Are there any constraints on the scope for decision making?

This RIS is intended to support decisions on the outstanding policy issues, namely the institutional arrangements, enforcement and penalties regime, and cost recovery. It does not analyse the options for establishing a consumer data right, which was included in MBIE's 2021 RIS, nor which sectors of the economy this should apply to, which will be analysed prior to Cabinet taking decisions on a designation, or the detailed CDR rules which will be designed in the future.

Section 3: Institutional arrangements

3.1 Background

Institutional arrangements set out the functions of the regime and define and delegate specific responsibilities. They are intended to ensure the smooth and pragmatic operation of the CDR regime. The functions include policy functions (advising on designations, secondary legislation, whether a prospective sector meets the statutory test for designation, setting data standards); service delivery functions (accreditation of data recipients, providing the registry, promotion of the CDR); compliance and enforcement functions; and redress and consumer dispute resolution functions.

We considered whether it was appropriate for these functions to sit within one or more private sector organisations, but ultimately favoured options for these functions to sit within government. This is to increase consumer confidence and participation in data portability, and to maximise the potential for interoperability across multiple sectors, as discussed further below.

3.2 Criteria

The following criteria are important in deciding institutional arrangements:

- Functions should sit with a department unless good reasons exist to do otherwise.
- In choosing a specific body to carry out a function, relevant factors to consider include fit with existing functions, competency, cost, and promoting trust and confidence.
- The legislative regime should be designed flexibly.

3.3 Options

Each function could be carried out by a department, Crown entity, or other entity. Different options have different levels of Ministerial oversight. As shown in the diagram below, the entities on the left (public service agencies) have full Ministerial oversight and accountability. The entities on the right have full independence, with the least Ministerial oversight. There are a range of intermediate options.

Full Ministerial oversight	**In between**	**Full independence/least Ministerial oversight**
Public service agencies/departments For example: MBIE, Department of Internal Affairs *Allows full Ministerial oversight and accountability*	Other options, such as autonomous Crown entities, Crown agents, departmental agencies (operationally autonomous but hosted by a department)	Independent Crown entities For example: Commerce Commission, Privacy Commissioner *Used if an independent decision-maker is required or where government needs to be held to account*

3.3 Analysis

Analysis: policy and service delivery functions to be carried out by administering department

We consider that the administering department for CDR should be responsible for advising on secondary legislation (including designations and regulations), licensing data recipients, providing registry services and promoting the CDR regime. This gives Ministers full oversight over these functions.

Having these policy and service delivery functions together will enable close collaboration, which is important to ensure that the CDR system works for consumers. The implementation of the CDR regime will be very technical in nature. It is critical that the teams developing and maintaining these technical elements collaborate closely together to ensure that the system works from a technical and customer experience perspective. This can best be achieved if the teams are in the same department. This is consistent with advice from staff at the Australian Competition and Consumer Commission (**ACCC**), who advised us to keep the policy and service delivery elements together given the linkages between them.

Having these functions in the same department will also be simpler for CDR participants, giving them a single point of contact when they get accredited and begin to participate in the regime.

It is likely that the Ministry of Business, Innovation and Employment (MBIE) would provide the closest functional fit as an administering department. MBIE has a strong focus on regulatory systems relating to consumers and small businesses, as well as on competition, productivity and innovation in the economy, all of which are relevant to implementing a consumer data right. In addition, MBIE is already working to develop the CDR legislative framework. MBIE also currently performs functions that fit well with CDR functions, including a range of licensing and registry functions.

We note that the Bill would assign the functions to the "chief executive of the department that, with the authority of the Prime Minister, is responsible for the administration of this Act". As the administering department is decided by the Prime Minister's office, it is not necessary at this stage to specify the department.

Analysis: data standards body within administering department

We consider that the data standards should be made by a statutory officer within the administering department. This will create good continuity between a CDR Act and regulations (high-level and moderately detailed policy) and the creation of data standards (very detailed policy). These will need to work well together for a successful regime, and we have heard that having multiple entities involved in these different functions has caused confusion in Australia. Australia initially assigned the data standards function to their Commonwealth Scientific and Industrial Research Organisation but has since moved that function to Treasury (which carries out the other policy functions as well).

This is the same arrangement as Australia, whose Chair of the Data Standards Body is a statutory officer. The creation of a statutory officer would safeguard the function. It would also enable it to move to different agencies over time.

As data standards are very technical, it will be crucial that the development process provides for wider input at a technical and sector level. The CDR legislation will require consultation so that this input can be made (for example, from industry and sector experts and the Privacy Commissioner).

We considered whether a sector-by-sector arrangement would be appropriate for the data standards function and consider such an arrangement unsuitable for the following reasons:

- While some of the data standards will be sector specific (for example, technical rules about the form of data), other data standards will be the same across sectors (including information security, customer experience, and many standards relating to how participants interact with each other in the CDR ecosystem ("endpoints").
- A sector-specific approach would make interoperability more difficult, especially as the CDR regime gets bigger. Data may not be able to be shared across sectors if the data standards are

different for each sector.

- Given how technical the data standards are, it will be important for the regulations, data standards, accreditation systems and registry to be developed in close collaboration (as previously discussed). This will be more difficult if the data standards are developed in each sector.

We also considered whether the data standards should be made by an entity outside government.

Analysis – compliance and enforcement for the CDR system to be carried out by the Commerce Commission

We consider that the agency best placed to carry out the compliance and enforcement functions for the CDR system is the administering department.

This is consistent with guidance from the Cabinet Manual which states that "a decision to assign government activity or function to a Crown entity indicates that the function should be carried out at "arm's length" from the government."

We consider that the CDR functions are a good fit with MBIE's functions – the likely administering agency. MBIE has a focus on service delivery and the ease of doing business. MBIE's functions also have links to consumer protection and support for small businesses.

While our preference for the compliance and enforcement regulator is the administering department, another option for the compliance and enforcement agency is the Commerce Commission, which is a strong regulator with a competition and consumer focus. However, this will increase the complexity of the regime and add functions to the Commission that go beyond their existing expertise, adding overall costs to the regime.

We note that the CDR enforcement agency would not deal with enforcement of privacy issues. These would fall under the jurisdiction of the Privacy Commissioner. A memorandum of understanding between the two agencies will likely be required to provide clarity to the sector about the respective roles of the agencies.

The full set of obligations under the Privacy Act will apply to data holders and data recipients. The Privacy Commissioner will be able to exercise all their existing functions and powers in relation to persons participating in CDR. The Bill will state this for the avoidance of doubt.

Analysis: consumer redress function to be carried out by the Office of the Privacy Commissioner

Consumers need to have avenues to resolve complaints and disputes about CDR that remain unresolved despite complaining to the data holder or data recipient.

This will be important to build and maintain trust in the CDR regime. A mechanism for redress for consumers will further promote confidence and informed participation in the CDR by consumers, and encourage fairness, honesty and professionalism by the parties providing CDR services. A redress system will also provide a mechanism, alongside the compliance and enforcement function, to address and reduce systemic risks and improve industry standards of conduct.

Most of the complaints that consumers will have about the CDR are likely to be privacy related. That is, consumers will be most concerned about consent to data being shared, and how their information is collected, used, disclosed, and stored.

The consumer redress function in relation to personal information could be provided by the Privacy Commissioner and Human Rights Review Tribunal (HRRT), using their existing powers, processes and functions. These powers will not change but be extended to the CDR set of privacy-related obligations. The Privacy Commissioner and the enforcement agency will have overlapping jurisdiction over some of the same provisions, though they will only be involved in their respective areas. For example, the Privacy Commissioner would concern itself with breaches of personal information and the enforcement agency with aspects regarding the integrity of the CDR rules and system as a whole.

We consider the best option is that consumers be able to go to the Privacy Commissioner for privacy-related breaches of the CDR obligations. These are obligations that prescriptively state how information must be used, collected, disclosed or stored in the specific context of CDR, over and above the obligations in the Privacy Act 2020.

This proposal is consistent with the principle that privacy issues should go to the Privacy Commissioner, regardless of the way in which information flows (letter, email, CDR system). The proposal does not impose additional costs on businesses to be part of a disputes resolution scheme (unless this were separately levied). It also maintains the current focus of the Privacy Commissioner (and HRRT) on individual privacy rights.

One way this could be implemented would be to provide that Part 5 of the Privacy Act (complaints, investigations and proceedings) applies to breaches of certain CDR obligations as if they were breaches of relevant information privacy principles. This is analogous to section 22F(4) of the Health Act

The powers, processes and remedies available to the Privacy Commissioner will not change – they will remain the same and be extended to a different set of privacy-related obligations. For example, the Privacy Commissioner will not issue infringement notices under the CDR Act.

It is the case that the Privacy Commissioner and enforcement agency will have overlapping jurisdiction over some of the same provisions. However, the enforcement agency would be concerned about such breaches in the context of protecting the integrity of the CDR system and ensuring that CDR participants are following the rules of the CDR system, rather than on privacy implications of those obligations.

For example, take an obligation to get consent from consumers in the form specified by CDR data standards. A breach of this requirement may be of interest to the enforcement agency where a failure in the data recipient's systems for obtaining consents threatens the integrity of the CDR system. It would also be of interest to the Privacy Commissioner where there are specific privacy implications for individual consumers.

We anticipate that the CDR enforcement agency will not seek to resolve individual privacy complaints. Such complaints will be referred to the Privacy Commissioner. Similarly, patterns of misconduct would be reported to the enforcement agency by the Privacy Commissioner. A memorandum of understanding between the enforcement agency and the Privacy Commissioner will likely be required to provide clarity to the sector about the respective roles of the agencies.

The Privacy Commissioner will not deal with complaints from legal entities, such as companies. Neither will it deal with non-privacy related breaches of the CDR. These will be dealt with by the CDR enforcement agency or by existing redress mechanisms in the industry.

Two alternative institutional arrangements for providing consumer redress in relation to CDR privacy breaches were considered:

- A new centralised disputes resolution scheme: Under this option, a new disputes resolution scheme would be established with jurisdiction over breaches of CDR obligations across all designated sectors. Like the Privacy Commissioner, this would provide a centre of expertise for dealing with CDR complaints and reduce potential 'forum shopping' compared to a more dispersed disputes resolution scheme. However, establishing a new scheme would likely create confusion for consumers as to whether they should refer their disputes to existing industry dispute resolution schemes, the Privacy Commissioner or the new scheme. A new scheme is also likely to be much more expensive than using existing consumer redress arrangements.
- Using existing industry dispute resolution schemes: Under this option, data holders and data recipients would be required to be members of an approved external independent dispute resolution scheme. This could include one of the many industry-specific dispute resolution schemes that already exist, such as the Banking Ombudsman and other financial services schemes and Utilities Disputes Limited. As these arrangements tend to be less formal than Privacy Act processes, this option may be more efficient and accessible. However, many of

these bodies do not currently consider privacy complaints, and instead refer them to the Privacy Commissioner. This means there would need to be significant upskilling of industry disputes bodies to handle these types of disputes. This option is also likely to create consumer confusion about the appropriate forum in situations where conduct breaches both the Privacy Act (which would continue to be handled by the Privacy Commissioner) and the CDR regime (which would be dealt with by an industry dispute resolution scheme and referred to the CDR enforcement agency in serious cases).

Section 4: Enforcement and penalties

4.1 Background

The CDR compliance and enforcement system is intended to help regulate behaviour and address non-compliance with the CDR requirements. This will ensure the CDR regime continues to effectively drive competition, innovation, productivity and consumer welfare in the New Zealand economy.

4.2 Criteria

The following criteria were applied:

a. *Effectiveness and efficiency*. This criterion was used to assess whether the option would deter non-compliance or adequately punish non-compliance.

b. *Appropriate to the harm caused or the nature of the conduct*. This criterion was used to assess whether the option is appropriate with respect to the level of harm that may result from the prohibited conduct and the nature of the conduct.

c. *Practical to implement and apply*. This criterion was used to assess whether the option has any practical impediments that would make it unworkable.

d. *Fair and consistent with natural justice*. This criterion was used to assess whether the option is fair and consistent with the principle of natural justice.

4.3 Options

Criminal Regime	Hybrid Regime	Civil Pecuniary Regime
Criminal Penalty Regime This would include traditional criminal penalties, along with lessor infringement offences (no conviction).	A combined approach, where the regime encapsulates both criminal (including infringement offences) and civil pecuniary penalties.	Pecuniary penalties This would utilise a range of pecuniary penalties to deal with the largely commercial CDR Regime.

We consider that a hybrid regime is appropriate, for the reasons set out below.

4.3 Analysis

Breaches of CDR requirements could result in infringement offences, pecuniary penalties or criminal offences, depending on the nature of the breach

We concluded that penalties for the CDR regime should be based on a combination of criminal offences, pecuniary penalties and infringement offences. This decision was influenced by New Zealand's authoritative source for guidance on designing legislation (including when certain kinds of penalties may be appropriate), the Legislation Design and Advisory Committee's Legislation Guidelines (2021 edition).

The alternative options of having a strictly criminal or civil pecuniary regime were considered in depth. Pecuniary penalties are a valid tool for regulatory enforcement, providing an intermediate penalty between criminal and infringement offences. They are quasi-criminal in that they are a form of penalty and a tool of enforcement. In many instances they provide the most appropriate means to penalise commercial misconduct. On the other hand, infringement offences provide a more suitable means to capture conduct of relatively low seriousness that does not justify the full imposition of the criminal law or large monetary fines. Additionally, criminal offences would allow the regime to substantially deter and punish conduct at the more serious end of the spectrum.

It was determined that although these regimes provided robust enforcement capabilities, neither set of penalties on their own provided a sufficiently pervasive coverage of the wide range of CDR misconduct that might occur under the CDR regime. In light of this, the combined approach based on both criminal and civil pecuniary penalties was chosen, which will provide the regime with a more flexible and effective toolkit to deal with misconduct.

Analysis: The CDR liability and penalties regime be based on an escalating hierarchy of liability

The liability and penalties regime comprise a hierarchy of four tiers. They reflect the broad circumstances in which each infringement offences, pecuniary penalties or criminal offences will apply, as well as the maximum penalty for each. They are as follows:

- Tier 1: Infringement notices up to $20,000, infringement offences up to $50,000;
- Tier 2: Pecuniary penalty of up to $200,000 for an individual and up to $600,000 for a body corporate, plus compensation orders;
- Tier 3: Pecuniary penalty of up to $500,000 for an individual and up to $2,500,000 for a body corporate, plus compensation orders;
- Tier 4: Imprisonment for a term of up to 5 years and/or a fine of up to $1,000,000 for an individual. For a body corporate, the greater of $5,000,000 or either (a) three times the value of any commercial gain or (b) 10% of the turnover in the period/s in which the breach occurred if commercial gain cannot be ascertained.

Tier 1 breaches are infringement offences. They represent contraventions of basic 'compliance' obligations or prohibited conduct that is of concern to the community, but which does not justify the imposition of a criminal conviction, significant fine, or imprisonment.

Infringement fees are usually set at, or below, $1000 as per the Legislative Design and Advisory Committee (LDAC) Legislative Guidelines. This higher amount is believed as appropriate in the CDR context to enable sufficient deterrence and provide cost effectiveness for the regulator in pursuing enforcement action.

Tier 2 and 3 breaches relate to conduct that is more serious than infringement offences, yet not sufficiently egregious to warrant the use of serious criminal offences. Tier 2 and 3 breaches can be enforced through civil proceedings which may result in considerable pecuniary penalties if guilt is proved on the balance of probabilities. Additionally, under civil law actions, the courts can make compensation orders to rectify any harm caused by a breach.

In these circumstances, the nature of the offending does not warrant the denunciatory and

stigmatising effects of a criminal conviction (e.g., the conduct does not have an element of intent, dishonesty or recklessness, having regard to the harm that may be caused), and a monetary penalty is thought to be sufficient to deter or punish breaches.

Tier 4 breaches involve egregious contraventions where the conduct is morally blameworthy in that it is done recklessly, knowingly, or intentionally. This reflects our view that criminal offences should be applicable to the CDR regime in very limited circumstances due to their serious nature and having regard to the proportionality of the harm caused. Tier 4 includes the use of custodial sentences which are the strongest tools available in criminal law. To balance this, custodial sentences are set to only apply sparingly to Tier 4 and the most serious and egregious misconduct. It is important to note that at trial, their availability would not preclude a courts' ability to impose lesser sanctions where necessary.

In proposing these tiers, we have considered the approaches to penalties taken in existing competition, consumer and other relevant commercial laws. We have also considered that the CDR will be gradually applied across many sectors of the economy and play an important future role in driving competition, innovation and productivity in the economy and increasing consumer welfare. The strong penalties will promote trust in the CDR regime, which is necessary for the regime's success.

Section 5: Cost recovery

5.1 Background

It is proposed that the Bill will include the power to charge fees and levies.

Fees are proposed to recover costs for the accreditation of data recipients. Data recipients will need to apply for approval before they can participate in the CDR. Approvals will expire after a set period, requiring renewal. There will be some degree of 'tiered' licensing (depending on risk) and approvals may also need to be amended at times (e.g., to change tier). Specific fee levels for licensing would be set in secondary legislation, and decisions made when designating the first sector.

Levies are proposed, which could be imposed on a sector-by-sector basis. Decisions about whether a levy would be charged, and the size of the levy, would be set out in secondary legislation.

5.2 Policy Rationale: Why a user charge? And what type is most appropriate?

Fees for accreditation application charges

Cost recovery is appropriate for the accreditation application charge as the persons to whom it will apply directly gain and benefit from being able to operate in the CDR regime. As a result, it is appropriate for those persons to bear the cost of assessing and ensuring that they meet the criteria for accreditation.

This is consistent with registration and licensing fees throughout the economy. The goods are both rivalrous (resources spent approving one person cannot be spent approving another) and excludable (approvals legally only extend to one person), and they tend to be treated as private goods.

It is anticipated that the fees would be on a full cost recovery basis. This is because the costs to applicants are likely to be minimal in comparison to the benefit gained by operating in the market, while the costs involved to the administering agency are likely to be large when the total number of applications are taken into account.

We also note that, due to the sector-by-sector way that the CDR will be rolled out across the economy, full cost recovery will not be initially feasible, and some Crown funding will be required for the accreditation regime. Implementing an accreditation regime will have high up-front costs but the CDR will initially apply to only a small part of the economy. Accordingly, imposing full cost recovery

would result in fees being imposed on the initial sectors for designation that do not reflect their private benefit and that may discourage participation in the CDR regime.

As the charge for accreditation is imposed on specific persons for a service which is directly provided for and benefits the person, by allowing them to participate in the CDR regime as a data recipient, it is most appropriately classed as a cost recovery fee.

Firms that are prospective data recipients will pay the fee. We do not currently have estimates of how many firms this would be, as it would depend on the sectors participating in CDR and uptake.

Levies

Levy funding (for example, for the development and maintenance of standards and consumer information) has benefits over funding from general taxation. It can drive greater accountability as the levy is directly tied to the delivery of the required outputs being standards and consumer information. Market participants have a greater ability to question non-delivery when they have been directly charged for a product or service. In contrast, funding from general taxation can result in underfunding of key outputs and insufficient funding overall.

a. The use of a levy can also help defray some of the upfront costs of designating a sector under the CDR regime (including by recovering depreciation costs of infrastructure for the regime). As a sector is brought within the regime there are costs in preparing and administering standards and parts of these will be different for each sector. A levy may be used to recover costs associated with sector-specific elements of these standards.

5.3 High level cost recovery model (the level of the proposed fee and its cost components)

High-level cost recovery model for accreditation fees

We estimate that fees would be $3600-$4500 per application.

These estimates have been calculated on the assumption that the initial investigation would take 40-50 hours per application. This was estimated by taking a mid-range from the closest equivalent to CDR that MBIE assesses (accreditation under the Weights and Measures Act). The hourly rate used ($90) is the same as the rate at which MBIE charges for similar assessments (based on the cost of a typical technical regulatory FTE).

The main cost drivers of accreditation are the operational investigation/assessment time spent by staff assessing applications and the overhead cost of setting up and maintaining systems which mange and contribute to the management of assessments.

Both direct costs (such as salaries) and indirect costs (such as corporate overheads, HR, and equipment and office space) are encapsulated in the hourly rate figure of $90.

A major assumption underlying the fee estimates is that the hourly rate will reflect MBIE's rate used for the estimates. Another major assumption is the length of time it would take to investigate and assess applications for CDR accreditation, which is an estimate given that the process and criteria for the application process is not clear yet. There is a high degree of uncertainty about these estimates, as the criteria for accreditation of data recipients has not yet been determined. Should these estimates be too low/high the actual costs and thus the fee associated with assessing an application would be higher/lower than the estimates.

We consider that this proposal is consistent with the Treasury's Guidelines for Setting Charges in the Public Sector.

High-level cost recovery model for levies

The CDR Bill would enable levies to be charged, including sector-specific levies where appropriate. Decisions about whether a levy would be charged, and the size of the levy, would be set out in secondary legislation.

A levy would provide for cost recovery for a wide range of activities that benefit users of the CDR (data recipients and consumers) as a group, and which would otherwise be funded out of general taxation. This could comprise, for example:

a. the development and ongoing maintenance of CDR rules and technical data standards

b. information and education

c. monitoring and enforcement.

In terms of estimated charge levels, these would depend on the sectors that are participating in CDR, and the scope of the levy.

Confidential information entrusted to the Government

[redacted]

Section 6: Stakeholder views

6.1 What do stakeholders think about the problem and the proposed solution?

In August 2020, MBIE released a discussion document on options for establishing a consumer data right in New Zealand. We sought feedback on the possible institutional arrangements, but feedback was not sought on the other issues discussed this RIS.

We have met a range of stakeholders regarding the CDR, including privacy sector businesses, such as banks, energy retailers, telecommunications companies and FinTechs, as well as Government departments and Crown entities. We have also met with Payments NZ and a FinTech to discuss cost recovery in relation to the financial sector. Payments NZ provided information about the fees that they currently charge to data holders (banks) and users to fund the development of standards and Payment NZ's oversight of open banking.

The exposure draft process will be an opportunity for stakeholders and the public to engage and provide feedback on cost recovery proposals through the Select Committee process. There will be a further opportunity for engagement and feedback when the CDE Bill is progressed through the legislative process, through the Select Committee process.

Section 7: Implementation and operation

7.1 How will the new arrangements be given effect?

Primary legislation will be introduced to establish the CDR. This will provide the framework for designating individual sectors of the economy as subject to the CDR, which will occur via secondary legislation. Data standards and rules will also be prescribed in secondary legislation.

The implementation of the CDR is set out in more detail in MBIE's June 2021 RIS.

Section 8: Monitoring, evaluation and review

8.1 How will the impact of the new arrangements be monitored?
The monitoring and evaluation activities MBIE will carry out is set out in more detail in MBIE's June 2021 RIS.