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.

In Confidence

Office of the Minister of Commerce and Consumer Affairs

Cabinet Economic Development Committee

Further decisions on the consumer data right

Proposal

1. This paper seeks agreement to the remaining decisions needed to complete drafting of the Consumer Data Right (**CDR**) Bill. This includes recommendations on institutional responsibilities, cost recovery, compliance and enforcement, and consumer redress. This paper also seeks agreement for banking to be the first sector to be designated under the new CDR Bill.

Relation to government priorities

2. A consumer data right will help to achieve the government's priority to grow an economy that works for all New Zealanders and to improve the wellbeing of New Zealanders and their families.

3. In their joint statement of 31 May 2021, the New Zealand and Australian Prime Ministers instructed officials to continue work towards interoperability on improving government services, payment practices policies and the consumer data right.[1]

Executive summary

4. On 5 July 2021, Cabinet agreed to establish a consumer data right legislative framework [DEV-21-MIN-0145]. 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**), on the consumer's request and consent. The CDR will be rolled out on a sector-by-sector basis via designations made by the responsible Minister.

5. In this paper, I propose that banking be the first sector to be assessed for designation against criteria set out in the CDR legislation. If the banking sector meets the criteria, it would be the first sector to which the CDR would apply.

6. Cabinet invited me to report back on certain remaining design elements of the legislative framework. This paper seeks decisions on these matters, so that a CDR Bill can be drafted. I propose that:

    6.1. Most CDR functions be performed by the administering department for CDR, including advice on designations and rules, approval of data recipients, registry functions, and promotion of the CDR regime.

    6.2. The Commerce Commission carry out the CDR compliance and enforcement function.

[1] https://www.beehive.govt.nz/release/joint-statement-prime-ministers-jacinda-ardern-and-scott-morrison

6.3. Data standards be made by a statutory officer appointed within the administering department, in consultation with interested persons.

6.4. In addition to their existing functions, the Privacy Commissioner and Human Rights Review Tribunal be empowered to investigate and provide redress for complaints relating to breaches of CDR privacy and information security safeguards over personal information, in line with Privacy Act 2020 processes.

6.5. There be a comprehensive compliance and enforcement regulatory toolkit, including the use of criminal offences (such as custodial sentences), pecuniary penalties and infringement offences.

6.6. Along with fees paid by those seeking to become approved data recipients, a levy power (to be further provided for in regulations) will partly fund CDR functions and will be able to be applied to designated sectors.

7. I expect to publish an exposure draft of the Bill later this year to obtain feedback and further refine the CDR regime Confidential advice to Government Confidential advice to Government

Background

8. Many businesses across the economy collect and hold significant volumes of consumer data when providing goods and services. The collection and use of data have accelerated as businesses develop sophisticated means of collecting data, and as New Zealanders increasingly conduct transactions and participate in society online.

9. On 5 July 2021, Cabinet agreed to establish a legislative framework for a consumer data right (**CDR**) [DEV-21-MIN-0145]. The CDR will require businesses that hold data (**data holders**) to share prescribed consumer data (**CDR data**) with approved third parties (**data recipients**), on the consumer's request and consent. Consumers may be individuals, companies or other entities, and data will have to be shared using standardised data formats and interfaces. To protect consumers, data recipients will be accredited and there will be a range of further safeguards.

10. The CDR will be rolled out on a sector-by-sector basis, with the Minister of Commerce and Consumer Affairs designating individual markets, industries and sectors to which the CDR applies. The designation itself will be a legislative instrument that will set out details of how the CDR will apply to the sector. The designation will specify the types of data and functionality that is covered and will be accompanied by rules and standards that govern the transfer of the data.

11. The CDR will support competition, productivity and innovation in the economy and increase consumer welfare. Giving consumers more control over their data will make it easier for them to shop for services, such as banking, electricity and telecommunications, and give them access to new and innovative products and services. The CDR will also allow consumers to have greater trust that when their data is shared, this is done safely and for their benefit, with their prior knowledge and consent.

12. The CDR is expected to unlock particular efficiencies for small businesses, because data recipients will be able to provide better, more integrated, day-to-day services to them (for example, business monitoring, inventory management, reporting, e-commerce, and payment systems).

13. While Cabinet has agreed to the main parts of the legislative framework, DEV invited me to report back on the remaining high-level design elements. These relate to institutional responsibilities, cost recovery, compliance, enforcement and consumer redress. This paper seeks decisions on these matters, which will enable an exposure draft Bill to be prepared.

Proposals

Banking should be the first sector nominated for designation under the CDR

14. To accelerate the implementation of the CDR, I propose that Cabinet agree now to nominate the first sector to be assessed for designation against statutory criteria. This will give interested parties more certainty as to how the CDR will likely be implemented. It will also enable work to begin on the designation requirements while the Bill is before the House.

15. Following this nomination, designation will be made only after the assessment process as set out in the CDR legislation (once enacted) has been followed. This assessment will involve extensive consultation with industry.

16. The options for nomination considered by officials were banking, insurance, other financial services, energy (electricity and gas), health, the primary sector, telecommunications, and loyalty schemes. The following criteria were applied:

    16.1. The opportunities or benefits that a designation could realise and problems it could solve or mitigate in the sector.

    16.2. The ease and speed with which the CDR could be implemented in the sector.

    16.3. Whether data sharing in the sector is likely without regulatory intervention.

17. The banking sector received the highest overall score against these criteria (see **Appendix 1**), for the following reasons:

    17.1. If designated, a banking CDR (**open banking**) would enable customers to consent to their data being shared securely with third parties that provide value-added services (for example, via applications that enable the initiation of payments on behalf of a bank's customer or analysis of banking transactions to help a customer make better informed financial decisions).

    17.2. The industry has already made significant progress towards open banking, but progress has stalled and there are presently obstacles to banks entering into the necessary bilateral agreements with fintechs. A CDR could build on existing industry progress while removing known obstacles to open banking.

18. Accordingly, I propose that banking be nominated first for the designation assessment process. Other sectors that ranked highly, such as financial services, energy and health, could be logical next steps.

Most CDR functions to sit with the administering department

19. I propose that the administering department be responsible for advising on secondary legislation (including designations and regulations), licensing data recipients, providing registry services and promoting the CDR. Having these policy and service delivery functions together will enable close collaboration, which is important to ensure that the CDR system works for businesses and consumers.

20. I consider that the Ministry of Business, Innovation and Employment (MBIE) is likely to 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 CDR. 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.

Data standards to be made by a statutory officer within the administering department

21. In addition to the Act and Regulations, the data standards for designated sectors will set out the detailed rules for participating in the CDR regime. I propose that data standards be made by a statutory officer appointed within the administering department. This will ensure that the standards are consistent and interoperable between designated sectors.

22. I expect that any standards will build on work done by industry. For example, if banking is designated first, the standards that have been developed by the Payments New Zealand API Centre would be the natural starting point for the banking-related standards.

23. 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 therefore require consultation (for example, from industry and sector experts and the Privacy Commissioner).

Enforcement and dispute resolution mechanisms

24. I propose that the Bill provide enforcement powers (for the Commerce Commission) to ensure the integrity of the CDR system, as well as enforcement powers (for the Privacy Commissioner) for any privacy-related safeguards over and above those contained in the Privacy Act. Consumer dispute resolution is to be carried out by Privacy Commissioner and existing industry mechanisms.

25. Examples of the powers of the Privacy Commissioner and Commerce Commission as they apply to different types of obligations are provided in **Appendix 2**. Examples of the kinds of breaches subject to the regime are included as part of the penalty table in **Appendix 3**.

Enforcement to ensure the integrity of the CDR system

26. It will be important to have a strong and effective enforcement agency to foster trust and participation in the CDR system. I propose that the CDR enforcement function be carried out by the Commerce Commission, which has a proven track record in dealing with competition and consumer matters.

27. I propose that the CDR Bill provide for a full range of compliance and enforcement powers, from powers aimed at supporting willing compliance (for example, education, advocacy and outreach powers) to more intrusive powers capable of deterring and adequately penalising non-compliance (for example, investigatory powers and powers to commence penalty actions and seek proportionate remedies, including through criminal offences, pecuniary penalties, infringement offences and compensation orders).

28. In addition to having a CDR enforcement agency, I note that the licensing/accreditation system (which has been previously agreed by Cabinet) is an important tool for monitoring and regulating the behaviour of data recipients and ensuring their compliance with the CDR rules. If data recipients breach CDR obligations, licences may be suspended or revoked by the licensing agency, or have additional conditions placed on them.

29. The CDR enforcement agency would not deal with privacy matters. These would be 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.

Enforcement and redress to ensure privacy of consumers

30. 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 CDR Bill will state this for the avoidance of doubt.

31. In addition, the Privacy Commissioner will have enforcement and redress powers over any obligations in the CDR legislation that relate to privacy safeguards. These are described in the next section of this paper.

Privacy-related consumer dispute resolution to be carried out by Privacy Commissioner

32. A CDR will strengthen existing privacy protections by giving consumers greater choice and control over access to and use of their data. In order to ensure appropriate safeguards, consumers need to have avenues to escalate and resolve complaints and disputes about CDR that are not resolved at the level of the data holder or data recipient.

33. This will be important to build and maintain trust in the CDR regime. A mechanism for dispute resolution 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 dispute resolution system

will also provide a mechanism, alongside the compliance and enforcement function, to address and reduce systemic risks and improve industry standards of conduct.

34. Most of the disputes 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.

35. I propose 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.

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

37. 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 1956.

38. 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.

39. The Office of the Privacy Commissioner (OPC) 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.

40. For example, a breach of an obligation to seek consumer consent in the form specified by CDR data standards may be of interest to the enforcement agency where the breach of this obligation 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.

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

Non-privacy-related dispute resolution to be carried out by industry mechanisms

42. 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 dispute resolution mechanisms in the industry (such as the Banking Ombudsman).

Alternative options considered for dispute resolution functions

43. Two alternative institutional arrangements for providing consumer dispute resolution in relation to CDR privacy breaches were considered:

    43.1. *A new centralised disputes resolution scheme:* Under this option, a new dispute 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 dispute 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.

    43.2. *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).

Next steps

44. Officials will continue to work with the Privacy Commissioner and the Commerce Commission in drafting the CDR Bill and regulations to ensure that the arrangements are workable and appropriate.

Confidential advice to Government

Penalties for breaches of CDR requirements

45. I propose that the CDR liability and penalties regime be based on an escalating hierarchy of liability, with the most egregious breaches involving deliberate or reckless behaviour being subject to serious criminal offences while other, lesser breaches are dealt with through pecuniary penalties (with or without compensation orders) and infringement offences.

46. I propose that the liability and penalties regime comprise a hierarchy of four tiers as follows:

    46.1. Tier 1: Infringement notices up to $20,000, infringement offences up to $50,000;

    46.2. Tier 2: Pecuniary penalty of up to $200,000 for an individual and up to $600,000 for a body corporate, plus compensation orders;

    46.3. 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;

    46.4. 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 periods in which the breach occurred if commercial gain cannot be ascertained.

47. Tier 1 breaches are infringement offences. They represent contraventions with basic ‘compliance’ obligations and where the contravening conduct is clear-cut and does not have serious consequences. Enforcement can occur either by issuing an infringement notice including a fee to be paid, or instead by the enforcement agency prosecuting a case in court, which may result in a fine. Infringement offences are a type of criminal offence, but there is no criminal conviction.

48. I note that the low-level fines can effectively become just the cost of doing business and therefore have a relatively minor deterrent effect in a commercial context. It is also important to demonstrate to businesses and the public that the government takes privacy breaches seriously. I have therefore proposed infringement fees of up to $20,000 and fines of up to $50,000 be included in the CDR Bill. Actual fees for specific infringement offences could be set in regulations up to a maximum amount of $20,000. Setting the maximum infringement fee at $20,000 also provides the flexibility to prescribe a hierarchy of infringement fees to deal with more or less serious infringement offences.

49. Tier 2 and 3 breaches relate to conduct that is more serious than infringement offences. However, the conduct is 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.

50. Tier 4 breaches involve egregious contraventions where the conduct is morally blameworthy in that it is done recklessly, knowingly or intentionally. Enforcement is through court action. Conviction can result if guilt is proved beyond reasonable doubt. I propose that it is appropriate for the courts to have the option of imposing a custodial sentence for the most serious and injurious Tier 4 breaches.

51. In proposing these tiers, I have considered the approaches to penalties taken in existing competition, consumer and other relevant commercial laws. I have also taken into account that the CDR gradually applied across many sectors of the economy will have 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.

52. **Appendix 3** provides examples of the types of breaches I propose would come within each liability tier. The full list of breaches that will come within each tier will be determined during drafting of the CDR Bill and subsequent regulations.

53. In identifying which breaches should come within each tier, consideration will be given to matters including:

    53.1. whether the breach should be subject to strict liability (i.e. whether it is relatively minor and clear-cut and the plaintiff is best placed to prove their lack of culpability);

    53.2. the seriousness of the breach compared to other breaches and when considered against the objectives of the CDR regime; and

    53.3. the appropriateness of criminalising certain types of conduct.

54. The final categorisation of penalties will be tested during consultation on the exposure draft of the CDR Bill.

Cost recovery

55. Many of the elements of the CDR have significant costs. These include designating sectors to which the CDR will apply, developing sector-specific rules, designing and maintaining technical data standard, monitoring and enforcing CDR obligations, dispute resolution, providing registry services, and accrediting participants.

56. While a few of these elements, in particular accreditation, will involve direct cost recovery from participants through fees, other elements will need to be funded by the Crown, supported by either general taxation or levies. I propose that the CDR Bill provide for any fees and levies that are to be charged for the purposes of cost recovery. These fees and levies will be set by regulations and may need to take into account New Zealand's trade obligations.

Accreditation fees

57. Data recipients will need to apply for an accreditation from an accreditation body. This may expire after a period, requiring renewal. There is likely to be some form of

'tiered' accreditation (depending on risk) and accreditations may also need to be modified at some point in their life (for example, to change tier).

58. I propose that a fee be charged to data recipients when applying for or changing an accreditation. This reflects the fact that an accreditation is of exclusive benefit to the data recipient and its customers. This is consistent with charging practices for registration and licensing in other regulatory systems.

Sector levies

59. Levies may be appropriate to fund services that are not purchased by individual persons, but which benefit a particular group of persons, or where a particular group of persons is creating risks that a regulatory scheme addresses.

60. I propose that the CDR Bill enable levies to be charged on a sector-by-sector basis. Decisions about whether a levy would be charged, and the size of the levy, would be made when a sector was designated.

61. A levy would provide for cost recovery for activities that benefit users of the CDR as a group, and which would otherwise be funded out of general taxation. Data recipients and their customers are the main beneficiaries of the CDR regime. Data recipients receive access to customer data on more favourable terms than they would otherwise, and their customers receive goods and services based on that data. Data holders also benefit to the extent that they are data recipients themselves.

62. Activities that could be levy-funded include:

    62.1. the development and ongoing maintenance of sector-specific CDR rules and data standards;

    62.2. information and education, and monitoring and enforcement to promote consumer trust and confidence in the CDR.

Confidential information entrusted to the Government

64. The provision of consumer information and education would help to build trust and understanding of the CDR and support confidence in the system. Greater trust in the system will foster greater uptake and participation, the direct economic benefits of which will largely accrue to the data recipients and their customers. Therefore, levy funding for the provision of consumer information and education is justifiable as the costs are borne by those who most benefit.

65. Levy funding 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.

66. The use of a levy can also help defray some of the upfront costs of designating a sector under the CDR 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.

67. The level of any levy will need to be carefully set for each sector to avoid disincentivising participation in the CDR regime. It will also be important that levies avoid sectoral cross-subsidisation – for example, levies should not recover CDR establishment costs from the first designated sector that will also benefit subsequent sectors.

Financial implications

68. Officials are carrying out further work to estimate the financial implications of implementing a CDR regime.

Confidential advice to Government

70. There are no financial implications of creating the CDR Act itself – the CDR will not be operational until it is "turned on" through a delegation.

71. I previously reported that the Australian Government had committed $211.3 million in funding to implement a Consumer Data Right. I understand that further funding has since been required in addition. It is not yet clear whether similar levels of investment will be required here. It may be that the regime can be designed in a way that enables meaningful cost savings as compared with Australia. There are also significant inflationary pressures in the global economy, from which New Zealand is not exempt, which may impact on the overall costs. I have directed officials to continue to explore opportunities for cost-effective solutions (for example, in relation to the design of registry services, or by utilising existing initiatives such as the data standards developed in the banking sector).

Confidential advice to Government

Legislative Implications

Confidential advice to Government

74. I consider that an exposure draft Bill process will be useful for obtaining feedback to assist with the development of the proposal. A CDR is highly technical and is

intended to be applicable to any sector of the economy that is designated. While the public has commented on the issues to be addressed by the Bill at a high-level through a discussion document, this will be the first opportunity for interested parties to consider how the detailed implementation of the overall CDR regime is expected to work.

75. It is likely that, following consultation on the exposure draft Bill, significant refinement of the Bill will be needed. The Bill is likely to be most successful if these changes are made prior to its introduction in the House and referral to the select committee process, rather than trying to identify and address all significant issues during the latter stages.

76. I anticipate that an exposure draft Bill will be released in Q4 2022.

Impact Analysis

77. A Regulatory Impact Statement (RIS) was submitted at the time Cabinet approval was sought to establish a Consumer Data Right [DEV-21-MIN-0145 refers]. To support the further decisions in this Cabinet paper, a supplementary Regulatory Impact Statement has been prepared, which is attached in **Appendix 4**.

78. MBIE's Regulatory Impact Analysis Review Panel has reviewed the attached Regulatory Impact Statement prepared by MBIE. The Panel considers that the information and analysis meet the criteria necessary for Ministers to make informed decisions on the proposals in this paper.

Population Implications

79. I have not identified any population implications in relation to the proposals in this paper. In relation to CDR in general, there are the following population implications, which were also referred to in the previous Cabinet paper for CDR [DEV-21-MIN-0145]:

    79.1. *Māori interest in data:* Māori have a particular interest in data. For example, a te ao Māori lens emphasises the whakapapa of data associated with a person, and therefore data may need culturally appropriate infrastructure and safeguards to reduce any risk of it being mishandled. As part of the exposure draft process, officials will seek feedback on how a Te Tiriti and te ao Māori lens might shape the CDR, and how a CDR might present unique opportunities and risks to Māori individuals, communities and businesses.

    79.2. *Vulnerable and technologically illiterate consumers:* The CDR poses a risk of exclusion for some consumers. A lack of digital literacy could increase an individual's susceptibility to online risks. However, it is likely that individuals with limited digital literacy may already be exposing themselves to risk which a CDR might prevent or mitigate. It is important to maintain a focus on digital inclusion to ensure that all New Zealanders have what they need to participate in a digital world. The ability to receive services online can reduce the isolating effects of living in more rural or remote areas, and the ability to access and compare services could enable consumers to negotiate on

behalf of their own interests or seek better deals, provided these communities have access to the internet.

79.3. *Consumers with disabilities:* The CDR may benefit the participation of people with disabilities in the digital era. If implemented with due consideration of accessibility requirements, it can give people with disabilities confidence that they are able to manage their personal data by ensuring that informed authorisation and consent decisions are made. However, 17.2% of disabled people do not have access to the internet, compared to 4.7% of non-disabled people.[2] As with other vulnerable consumers, it is important to be cognisant of the digital exclusion experienced by a significant proportion of disabled people, including Māori disabled/tāngata whaikaha.

Human Rights

80. The proposals in this paper are consistent with the New Zealand Bill of Rights Act 1990 and the Human Rights Act 1993.

Consultation

81. The Department of the Prime Minister and Cabinet, Department of Internal Affairs, Treasury, Ministry of Justice, Statistics New Zealand, Ministry of Health, Commerce Commission, Office of the Privacy Commissioner, Electricity Authority and the Financial Markets Authority were consulted on this Cabinet paper.

82. The Office of the Privacy Commissioner is supportive of the CDR regime and broadly comfortable with the role proposed for it in the paper, subject to appropriate resourcing being provided for it. However, further design work is required to ensure that there is clarity about roles and responsibilities across the range of regulators who and, how they will work together to ensure coherence. The Privacy Commissioner will work with MBIE and other relevant agencies to progress this work with urgency.

Communications

83. The decisions taken from this paper will be published on MBIE's website, and an update sent to stakeholders.

Proactive Release

84. I propose to publish this paper on MBIE's website, subject to appropriate redactions, within 30 business days.

Recommendations

The Minister of Commerce and Consumer Affairs recommends that the Committee:

1. **note** that, on 5 July 2021, Cabinet:

    1.1. agreed to establish a consumer data right (CDR) legislative framework;

[2] Department of Internal Affairs, *Digital inclusion and wellbeing in New Zealand* (2019).

1.2. authorised the Minister of Commerce and Consumer Affairs to issue drafting instructions to Parliamentary Counsel Office for that framework;

1.3. invited the Minister of Commerce and Consumer Affairs to report back to DEV by 30 November 2021 (extended to May 2022 by the Cabinet Office) on institutional responsibilities, cost recovery, compliance, enforcement, and consumer redress for the consumer data right framework [DEV-21-MIN-0145; CAB-21-MIN-0254];

2. **note** that the CDR will give consumers the ability to share data held about them by businesses (data holders) with trusted third parties (licensed data recipients) using common standards and interfaces;

3. **note** that Cabinet agreed that the CDR be implemented gradually, whereby sectors of the economy can be 'designated' through Order in Council on the recommendation of the Minister of Commerce and Consumer Affairs;

4. **agree** that banking be the first sector assessed for designation under criteria to be set out in the CDR Bill;

Institutional responsibilities

5. **agree** that the department responsible for administration of the CDR Bill will be responsible for:

5.1. developing and advising on secondary legislation;

5.2. licensing of data recipients;

5.3. provision of registry services;

5.4. education and promotion of the CDR to consumers and prospective data recipients;

6. **agree** that the Commerce Commission will be responsible for the CDR enforcement function;

7. **agree** that the data standards be made by a statutory officer within the administering department;

Consumer redress

8. **agree** that the Privacy Commissioner and Human Rights Review Tribunal be empowered to investigate and provide redress for complaints relating to breaches of CDR privacy and information security safeguards involving personal information, in line with Privacy Act 2020 processes;

9. **note** that consumer dispute resolution and redress will be provided by existing industry mechanisms;

Compliance and enforcement

10. **agree** that the CDR Bill provide for a range of compliance and enforcement regulatory powers for the CDR enforcement agency, including the power to educate, advocate, issue warnings, investigate potential breaches, monitor participants, compel compliance, and enable information sharing or collaboration with other regulators;

11. **agree** that the CDR Bill provide for a liability and penalties regime for breaches of CDR requirements and include a combination of criminal offences, pecuniary penalties and infringement offences;

12. **agree** that, subject to drafting, there be four main tiers of penalties, as outlined in Appendix 3;

13. **agree** that the enforcement agency will have the power to issue an infringement notice for offences in the first tier of penalties;

Cost recovery

14. **agree** that fees (to be set in regulations) may be charged to persons who apply for an accreditation or for an amendment to an accreditation;

15. **agree** that the CDR Bill include a levy-making power (to be set in regulations) that will permit recovery of the cost, or part of the cost, of regulatory functions under the CDR Bill, from data holders and/or accredited data recipients;

Confidential advice to Government

17. **invite** the Minister of Commerce and Consumer Affairs to issue drafting instructions to the Parliamentary Counsel Office to give effect to the above recommendations;

18. **authorise** the Minister of Commerce and Consumer Affairs to make decisions on minor or technical matters, consistent with the policy in this paper, on any issues that arise during drafting and passage through the House;

Confidential advice to Government

Authorised for lodgement

Hon Dr David Clark

Minister of Commerce and Consumer Affairs

Appendix 1: Rationale for proposing the banking sector as the first sector to be formally assessed for designation under a CDR

Criteria	Summary comments

Criterion 1: Opportunities or benefits that a designation could realise and problems it could solve or mitigate in the sector	• There are potential significant competition benefits from open banking:
	  • CDR can address problems of market concentration (where the sector is dominated by a few large banks), information asymmetries, complex nature of products and services, and high switching costs.
	  • Data is seen as a source of competitive advantage; banks are therefore reluctant to share it with potential competitors.
	  • CDR can reduce barriers to entry, allowing competitors to enter with different business models and ideas for innovation, and increase sector efficiency.
	• Use cases that would benefit consumers include product comparison, payments initiation and money transfers, financial planning, transaction monitoring, compliance and accounting tools.
	• Sharing of consumer banking data is already happening using risky methods such as screen scraping - a CDR would make sharing of sensitive data safe and secure for consumers.

Criterion 2: Ease and speed of implementation	• Opportunity for CDR to build on current industry-led and market-driven work to establish open banking, which would reduce CDR implementation time and cost compared to greenfield implementation. • Implementation could be complicated due to need to accommodate sensitive data, but risk can be adequately managed through data security and protection measures included in CDR.
Criterion 3: Whether data sharing in the sector is likely without regulatory intervention	• Current industry-led and market-driven initiative to implement open banking is slow-moving, resulting in delay of a vibrant open banking sector which could deliver tangible benefits for consumers and the economy; regulatory intervention would set statutory deadlines to speed up progress. • Process for third parties (e.g. fintechs) entering into bilateral agreements with banks expected to be challenging; CDR would remove barriers. • Delays in industry-led work has created uncertainty for third parties, allegedly resulting in a number of start-up businesses failing.

Appendix 2: Examples of the powers of the Privacy Commissioner and CDR enforcement agency as they apply to different types of obligations

Type of breach	**Breach of Privacy Act 2020**	**Breach of obligation in the CDR legislation related to privacy safeguards**		**Breach of obligation in CDR legislation not related to privacy safeguards**
Example of breach	Data recipient fails to tell consumer why they are collecting information	Data recipient fails to follow specific requirements in the CDR legislation about how consent must be given by consumers		Failure by data holder to accept action initiation request
Agency with jurisdiction	Privacy Commissioner	Privacy Commissioner	Commerce Commission	Existing redress for sector (e.g. Banking Ombudsman)
Rationale for agency having jurisdiction	Privacy issues should go to the Privacy Commissioner	Protecting against harms to personal privacy	Protecting against harms to the CDR system, ensuring trust in the CDR system	It is a dispute with the bank about their obligations to follow consumer instructions. CDR is just the form in which those instructions are given
Powers, processes and remedies available for agency with jurisdiction	Existing powers, processes and remedies under the Privacy Act	Existing powers processes and remedies under the Privacy Act	Powers, processes and remedies under the CDR Act	Existing powers and processes under rules for the particular dispute resolution body

Appendix 3: Proposed liability and penalty tiers for CDR legislation

Liability tier	Penalty	Examples of breaches that may be covered
Tier 1	Infringement notice of up to **$20,000**. Infringement offence of up to **$50,000**.	Failure to maintain transaction records. Breach of notification or disclosure requirements (for example, notification about how consumers make a complaint, notification that transfer of data is complete).
Tier 2	For a body corporate, a pecuniary penalty of up to **$600,000**. For an individual, a pecuniary penalty of up to **$200,000**.	Failure to have adequate internal complaint processes. Data holder fails to disclose CDR data in the required form in response to a valid request. Data holder fails to properly authenticate the identity of a consumer or data recipient. Data recipient discloses CDR data for a use that is prohibited under the CDR rules. Failure to meet regulatory reporting requirements.
Tier 3	For a body corporate, a pecuniary penalty of up to **$2,500,000**. For an individual, a pecuniary penalty of up to **$500,000**.	Data holder fails to provide a CDR service to consumers and accredited persons. A person misleads or deceives another person into believing either that a person is a CDR consumer for CDR data, or a person is making a valid request for the disclosure of CDR data.
Tier 4	For a body corporate, punishable on conviction by a fine of not more than the greater of **$5,000,000** or either: • if it can be readily ascertained that the contravention occurred in the course of producing a commercial gain, **three times the value of any commercial gain** resulting from the contravention, or • if the commercial gain cannot readily be ascertained, **10% of the turnover** of the person and its interconnected bodies corporate in each accounting period in which the contravention occurred. For an individual, punishable on conviction by **imprisonment** of not more than **5 years**, a fine of up to **$1,000,000**, or both.	A person knowingly/intentionally/ recklessly misleads or deceives another person into believing either that a person is a CDR consumer for CDR data, or a person making a valid request for the disclosure of CDR data. A person fraudulently holds out that they are an accredited person (or a particular type of accredited person).

Appendix 4: Impact Statement