New Zealand Law Society
Te Kāhui Ture o Aotearoa

# Customer and Product Data Bill

Submission of the New Zealand Law Society Te Kāhui Ture o Aotearoa

5 September 2024

## 1 Introduction

1.1 The New Zealand Law Society Te Kāhui Ture o Aotearoa (**Law Society**) welcomes the opportunity to comment on the Customer and Product Data Bill (**Bill**).

1.2 The Law Society is generally supportive of the Bill's intention to improve consumers' control and portability of data and drive innovation and competition, and considers that subject to amendments to improve it, the Bill should proceed. However, there are concerns with the Bill as presently drafted.

1.3 The Bill delegates a significant amount of detail to secondary legislation. Matters to be addressed in regulations include what industries and data are captured by the framework, and some key privacy safeguards. The Law Society acknowledges the intention of relying on regulations is to enable flexibility in the provisions that will be made in future for different designated industries. However, further consideration is needed around which matters are set out in the primary legislation, as opposed to regulations. Additionally, the Law Society has concerns about workability and drafting, particularly in areas of potential overlap with the Privacy Act 2020.

1.4 This submission has been prepared with assistance from the Law Society's Commercial and Business Law and Human Rights and Privacy Committees.[1]

1.5 The Law Society **wishes to be heard** on this submission.

## 2 General comment

2.1 The Bill aims to enable greater access to, and sharing of, customer and product data between businesses. The Bill will create a 'consumer data right' (**CDR**) which enables a consumer to have greater control over the use and access of their data. The right will also facilitate improved competition, innovation, and services across designated industries.

2.2 The Regulatory Impact Statement (**RIS**) and the explanatory note to the Bill note that a CDR or open banking has been introduced in Australia, the United Kingdom, and Europe.

2.3 The Bill proposes that businesses holding designated customer data (called 'data holders') will be required to act in response to requests from customers and accredited third parties to open accounts, make payments, or change customer plans.

2.4 The framework will encapsulate separate privacy safeguards, with the intention that they will complement, rather than replace, existing safeguards in the Privacy Act 2020.

## 3 Key concerns

### Overreliance on regulations

3.1 While the Law Society agrees it is a sensible proposition to roll out the framework on an industry-by-industry basis as suggested in the Bill, there remains concern about the lack of

[1] More information on the Law Society's law reform committees and sections can be found here: https://www.lawsociety.org.nz/branches-sections-and-groups/law-reform-committees/

detail in the Bill regarding general principles, comprehensive and appropriate definitions, and a number of key matters such as:

(a) what data may be captured by the CDR;

(b) what data holders are captured;

(c) what actions data holders will be obliged to perform;

(d) who are secondary users;

(e) what is needed to make a valid request; and

(f) the requirements systems must meet, and what systems.

3.2 As a general point, the Law Society considers that too much of the detail of the framework is left to be determined by way of regulations and that this, in combination with the lack of general principles in the Bill, could lead to a lack of consistency and an unreasonable compliance burden. Regulations do not require a full Parliamentary process to make or amend them. They are consequently not subject to the same level of scrutiny as Bills that pass through the House, and this means that there will not be the same level of consultation that is afforded to a primary legislative process. Nor do they have the same degree of certainty as primary legislation.

3.3 In respect of privacy, in particular, the Law Society recommends further consideration is given to dealing with key matters in the Bill. Privacy safeguards contained in the Bill are incomplete. This is, in part, because the Bill is intended to complement rather than replace provisions in the Privacy Act 2020. However, there are gaps that the Bill, not regulations, should address, and the relationship with the Privacy Act is inadequately clarified.

3.4 In the Law Society's view, moving privacy safeguards into secondary legislation is likely to diminish their perceived importance and risks undermining public trust in the CDR framework. The proposal to develop regulations subsequently also risks resulting in heightened and overlapping regulatory compliance burdens for companies that need to comply with both the Privacy Act 2020 and the CDR framework. In the Law Society's view, more consideration and clarification of the interface between the respective statutory frameworks is needed in the Bill. In particular, primary legislation, not supporting security standards, should set the boundaries on exchanging customer data. To address this point, the Law Society recommends that the Bill should, as a minimum, contain:

(a) a deletion requirement;

(b) expectations around de-identification; and

(c) who is responsible for data in transit especially in the event of a breach.

3.5 The comparable Australian Consumer Data Right (**ACDR**) legislation may assist in crafting provisions relating to this requirement.[2] As noted below, the privacy safeguards section of that legislation may warrant more general consideration as a possible model for strengthening and expanding the Bill's provisions.

---

2 Contained in the Competition and Consumer Act 2010 (Aus): compare s 56EO (Privacy safeguard 12—security of CDR data, and destruction or de-identification of redundant CDR data).

3.6 As currently drafted, the Bill leaves too much of the privacy safeguards to later regulations. There does not appear to be a practical need for this approach, and the Law Society notes that the regimes enacted in other countries have addressed these issues within primary legislation, with a greater degree of certainty.

## A need for general guiding principles

3.7 The Bill does not currently set out general principles that clearly identify the parameters of the CDR framework. These would be beneficial to provide regulatory bodies with clear guidance as to what can and cannot be included in the regulations and standards set for the industries they control. It would also ensure a more certain understanding of what is required of businesses.

3.8 The Law Society recommends that the Select Committee consider whether the Bill should contain general principles that will guide how the framework will be determined to ensure consistency and clarity, perhaps in a similar way to the Information Privacy Principles (**IPPs**) in the Privacy Act 2020.[3] This would assist both in framing future regulations, and providing businesses with a framework which could guide them, for example, in meeting the requirement to publish and maintain a CDR policy as proposed in clause 47.

## Further key privacy concerns

### Unclear relationship with the Privacy Act

3.9 The Bill is intended to work alongside and integrate with the Privacy Act 2020 without (as presently drafted) adequately clarifying how they interact. The respective Acts will contain overlapping compliance frameworks. However, matters in the Bill that potentially overlap with or could conflict with the Privacy Act are neither adequately identified nor clarified in the Bill.

3.10 Again, the Law Society is concerned about the complexity and compliance challenges that this could pose for agencies that need to meet the requirements of both regulatory frameworks. As it stands, the Law Society considers that if this issue is not better addressed in the Bill, the need to navigate the overlapping frameworks will impose a high compliance burden on businesses. It will make it challenging for them to clearly understand and comply with CDR requirements.

3.11 It appears the only clauses addressing the relationship of this Bill to the Privacy Act 2020 are clauses 52 and 53. These address only limited matters. The approach of the Bill in this regard can be compared with the approach taken in equivalent Australian legislation, establishing Australia's CDR scheme.[4] Section 56EC of the Competition and Consumer Act 2010 (Aus) expressly addresses the relationship with the Privacy Act 1988 (Aus), including:[5]

3 Privacy Act 2020, s 22.
4 Competition and Consumer Act 2010 (Aus), pt IVD.
5 Competition and Consumer Act 2010 (Aus), s 56EC(3)–(5) (Relationship with other laws).

(a) when the Australian Privacy Principles do not apply to those handling CDR data; and

(b) affirming the application of the Privacy Principles in other cases, such as to a 'data holder' or 'designated gateway'.

3.12 The Law Society recommends including a comparable provision to section 56EC in the Bill. Some further examples may serve to illustrate the need for greater clarification in the Bill about its interface with the Privacy Act, giving rise to concerns about workability if the issues were not addressed.

*Customer authorisation*

3.13 The CDR framework is premised on "customer authorisation".[6] In other words, the Bill is reliant on customers giving their consent (which they may, equally, choose to withdraw). As data collection and transmission is not typically authorised by consent in the Privacy Act, a key issue is what happens if consent is withdrawn under the Bill. When this occurs, there may not be adequate Privacy Act enforcement measures. For example, if a customer withdrew their consent under the Bill, there would be no breach of an IPP and therefore no enforcement avenue available.

3.14 The Law Society is not aware of any proposal to reassess the role of consent in the Privacy Act. To address the issue identified, the Bill should have specific enforcement provisions around consent. As discussed further below, these are not currently present.

*Data held 'on behalf'*

3.15 Clause 11 of the Bill provides for product data or customer data to be held on behalf of the data holder.[7] Where customer or product data is held 'on behalf', as the Bill is presently drafted, it is unclear where the privacy obligations will fall, and a gap arises in the Bill compared to the Privacy Act.

3.16 Under section 11 of the Privacy Act, 'held by or on behalf of' is further defined to mean that where an agency holds personal information 'on behalf' of another agency then it is held by that other agency.[8] The Law Society recommends clarification to align with the Privacy Act, by including a new clause equivalent to section 11. This will provide clarity for the purposes of both enforcement and compliance.

*Extraterritorial application*

3.17 The Bill is intended to have extraterritorial application.[9] It will be important for the Bill to clarify whether IPP12 of the Privacy Act, which relates to the disclosure of personal

6 General Policy Statement at 2, see e.g. clauses 15, 19 and 36–41.

7 Cl 11.

8 See Privacy Act 2020, s 11(1)–(2): if an agency (A) holds information for or on behalf of another agency (B) (for example, the information is held by A as a representative or agent of B, or for safe custody or processing on behalf of B), the personal information is to be treated as being held by B, and not A for the purposes of the Act.

9 Cl 11: the Bill applies to overseas agencies in relation to conduct in the course of carrying on business in New Zealand. Additionally, those holding product data or customer data on behalf of the data holder and therefore governed by the CDR provisions may be outside New Zealand.

information outside New Zealand, is intended to apply. IPP12, if applicable, will only apply to international transfers of personal information (which in turn, as defined in the Privacy Act, relates to an 'identifiable individual').[10] It is not clear how that sits alongside the Bill which is dealing with more than just 'personal information' being transferred outside New Zealand.[11] Transfer of customer data comprising personal information by an entity under the Bill to a third party outside of New Zealand that does not have comparable privacy or data protection laws may also engage IPP12, and be inconsistent with para (f) of that principle.[12]

3.18 The Law Society invites the select committee to further consider how the Bill can clarify these matters.

## Minimum privacy safeguards

*Possible legislative model*

3.19 Contrasting with the Bill, the equivalent legislative framework in Australia, the Consumer Data Right,[13] spells out privacy safeguards which are both clear and comparatively comprehensive.[14] Part 3 of the Bill ('Protections') includes a Privacy Act 2020 subpart.[15] However, the two clauses that it contains are significantly less comprehensive than the comparable division of the Australian Act setting out 13 privacy safeguards.[16]

3.20 Consideration could therefore be given to including a privacy safeguards part in the Bill, of broader scope than the present few provisions, which strengthens and makes more explicit the ways in which the Bill addresses privacy. The Law Society recommends that the Select Committee invite officials to further consider the extent to which the Australian example could provide a useful model, including (for example) the prohibition on the use of data for direct marketing, and the inclusion of 3, 6 or 12-month consent periods. As a minimum, the Law Society recommends the Bill should include the following safeguards.

*No use of data for direct marketing*

3.21 In Australia, the use of data for direct marketing is prohibited by CDR legislation.[17] Section 56EJ of the Competition and Consumer Act 2010 (Aus) provides that an accredited data recipient of CDR data or designated gateway for CDR data must not use or disclose it for direct marketing unless doing so is otherwise authorised or required under the consumer data rules. The Law Society recommends that the Bill should contain a provision mirroring the Australian requirements.

*Restraint on uses of data by outsourced providers*

10 Privacy Act 2020, ss 7 and 22.
11 Cl 8(2) "customer data".
12 Privacy Act 2020, s 22, IPP12(f).
13 Competition and Consumer Act 2010 (Aus), pt IVD.
14 Competition and Consumer Act 2010 (Aus), pt IVD, Division 5—Privacy safeguards.
15 Pt 3, cls 52–53.
16 Competition and Consumer Act 2010 (Aus), ss 56ED–56EP.
17 Competition and Consumer Act 2010 (Aus), s 56EJ (Privacy safeguard 7—use or disclosure of CDR data for direct marketing by accredited data recipients or designated gateways).

3.22 As discussed above, the Bill intends to apply to an agency in respect of designated customer (or product) data held by or on behalf of that agency. In addition to the need identified at paras 3.15–3.16 to clarify where privacy obligations fall when data is held on behalf of an agency, the Bill should be clear that, when acting on behalf of the data holder or accredited requestor, a service provider is not permitted to use designated data for any purposes other than the authorised purposes. The Law Society recommends a provision mirroring section 11 of the Privacy Act — albeit applying more broadly to 'data' (which includes, but is not limited to, 'personal information').

### Enforcement provisions

3.23 There is little mention of enforcement in the Bill, aside from what can be enforced through the Privacy Act. However, there are limitations in what the Privacy Act will be able to address. For example, to the extent that 'customer data' is not 'personal information' (such as when the data pertains to an entity other than an individual)[18] the Privacy Act does not provide adequate enforcement options. Further, the Privacy Act is not equipped to enforce obligations relating to real-time data exchanges.

3.24 The Law Society recommends that further consideration be given to the question of enforcement. As with other matters raised above, we consider enforcement provisions should be addressed in the Bill, not secondary legislation.

## 4 Specific clauses

### Definitions

#### "Data', 'information' and 'customer data'

4.1 'Data' is simply and broadly defined in the Bill as 'includes information'.[19]

4.2 The definition of 'customer data' is similarly drafted in very broad terms. The definition states that 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)'.[20]

4.3 In practical terms, the breadth of data potentially captured within such a definition of 'customer data' could include data or intellectual property that may not rightfully belong to the customer or be within the customer's control to begin with. The Law Society considers that such a broad definition is undesirable and recommends that the select committee consider narrowing the definition of customer data to apply only to data that belongs to or is within the customer's control to begin with.

4.4 The definition of 'data' may also require reconsideration. There is a lack of clarity as to how 'data' and 'information' are used in the Bill, and what one term means in relation to the other, given that these are not terms used in a standardised manner in practice. The definition of 'data' as including information has the potential for varying interpretations to

18 Privacy Act 2020, s 7: personal information means information about an identifiable individual.
19 Clause 5.
20 Clause 8.

be applied in practice, which could lead to future uncertainty. It is also unclear how personal information fits in.

4.5 The Law Society recommends further consideration and clarification of the relationship between 'data' and 'information', including how 'personal information' is incorporated into the two definitions and what the points of difference are.

### Differentiating 'customer data' and 'product data'

4.6 In the Law Society's view, distinguishing between 'customer data' and 'product data' may also be challenging: it would be desirable to clarify in the Bill the intended distinction between these terms. Absent that clarification, we suggest that any product data exchanged in the context of an individual customer will be customer data (because it is information about an identifiable customer).

### 'Derived data'

4.7 Further, clause 33(3) defines 'derived data' as:

> "... data that is wholly or partly derived from –
>
> (a) designated customer data; or
>
> (b) other derived data."

4.8 Given that practical concerns arise about the risk of undermining intellectual property rights and decreasing innovation by including derived data in the CDR framework, the Law Society considers that the definition of data and derived data should be connected to the consumer and product data intended to be captured by the CDR framework. Further, jointly covering both terms in the 'data' definition ensures that there is an appropriate level of certainty and clarity about data that is captured by the CDR framework to minimise the risk of unintended consequences.

4.9 For comparison, the Australian legislation defines CDR data as:[21]

> "… information that:
>
> (a) is within a class of information specified, as described in paragraph 56AC(2)(a), in an instrument designating a sector under subsection 56AC(2); or
>
> (b) is not covered by paragraph (a) of this subsection, but is wholly or partly derived from information covered by:
>
> (i) paragraph (a) of this subsection; or
>
> (ii) a previous application of this paragraph."

4.10 The Law Society recommends the Select Committee consider including a fuller definition of 'data' that includes derived data.

### The 'secondary users' category

4.11 The 'secondary users' category is another important term not defined in the Bill.[22] The Bill presently contemplates the persons or classes of persons (or both) being designated as

21 Competition and Consumer Act 2010 (Aus), s 56AI.
22 Cls 24 and 25.

secondary users (including specifying approval or other requirements or eligibility criteria to be met before a person may be a secondary user) being dealt with in designation regulations.[23]

4.12 If the Bill proceeds as proposed, this group will have unlimited access to data, making it important to precisely define the category in the interests of privacy and clarity, and to provide greater certainty. More certainty will improve business and consumer confidence in the CDR framework.

4.13 The Law Society recommends that the category is precisely defined in the legislation.

### Ability to refuse access

4.14 Clause 16 outlines the ability of the data holder to refuse access to data if the 'data holder reasonably believes that the disclosure of the data would be likely to have a materially adverse effect on the security, integrity or stability' of the data holder's own IT systems.

4.15 The Law Society notes that this exception does not specify that the materially adverse effect needs to arise from the data requester's system lacking security or functionality. If a data holder fails to prioritise the work needed to ensure that their systems can cope with and respond to data access requests, they could then rely on this exception despite the prescribed electronic system requirements for data holders set out in clauses 27 and 28.

4.16 We query whether, rather than relying on enforcement and infringement powers to oblige a data holder to make data available, the Chief Executive could instead be given the power to direct that data holders take remedial actions in relation to deficiencies in their systems within specified timeframes and given the ability to levy penalties against the data holder if they do not.

### Designated actions

4.17 Clause 18(1)(c) provides that a designated action is one that a data holder would ordinarily perform in the course of the data holder's business. Subsection (2) then provides that in determining whether the action is one that the data holder would ordinarily perform, regard must be had to the matters prescribed in the regulations and standards.

4.18 The Law Society considers it is likely that requests for data may be made for the purpose of providing new functions and services to customers that the data holder does not offer. However, the wording of limb (c) may mean that despite an action being a designated action for the purposes of this section, a data holder could escape the obligation to provide access to that data by saying 'I would not ordinarily perform this action'.

4.19 The language of limb (c) is unclear in its meaning and value when read alongside clause 18(1)(a), (b) and (d). The lack of clarity risks ambiguity over whether a data holder would be able to refuse access to data on the basis outlined above.

---

23 Cl 100(1)(g).

4.20 The Law Society queries whether this is what is intended and suggests the select committee consider redrafting this limb to clarify the intention.

### Storage and security of personal information

4.21 Clause 53 sets out that certain contraventions relating to the storage and security of personal information will be treated as a breach of IPP 5.

4.22 In practical terms, this means that if a data holder's stored CDR data is accessed, lost, used, disclosed, or modified in an unauthorised manner, such as a cyber-attack, then the only recourse available is the remedies set out in the Privacy Act 2020.

4.23 The Law Society considers that this is an undesirable level of protection, given that the Privacy Act 2020 penalties are fairly low and the likely impact of a breach of this kind is high for all the consumers whose personal information is stored with that data holder.

4.24 The Law Society recommends this clause be amended to include a penalty appropriate to the likely impact a breach of this section would have on consumers, especially consumer confidence in the framework.

### 'Reasonably informed' consent and safe harbour provision

4.25 Clause 36 requires a customer giving authorisation to another person to be reasonably informed. Otherwise, authorisation is required to be given in the manner prescribed by the relevant regulations or standards. Clause 40 subsequently provides that an accredited requestor must take the prescribed steps to ensure the customer is reasonably informed about the matter to which the authorisation relates.

4.26 The Bill should give clear guidance about what 'reasonably informed' means. Given the intention of the Bill is to improve the transferability of customer data, the Law Society considers it may be worth including an explicit safe harbour provision that clearly explains what constitutes a reasonably informed customer. It appears to be implicit in clause 40, but making it explicit will likely reduce the need for a case-by-case assessment of whether a customer has been reasonably informed.

Nāku noa, nā

David Campbell
**Vice-President**