New Zealand Law Society
Te Kāhui Ture o Aotearoa

Level 4, 17–21 Whitmore Street, Wellington
PO Box 5041, Wellington 6140 · DX SP20202, Wellington
04 472 7837 · inquiries@lawsociety.org.nz

lawsociety.org.nz

29 August 2025

Ministry of Business, Innovation and Employment (MBIE)
Wellington

By email: consumerdataright@mbie.govt.nz

Tēnā koe

Consultation on exposure draft of open banking regulations under the Customer and Product Data Act

1 Introduction

1.1 The New Zealand Law Society Te Kāhui Ture o Aotearoa (**Law Society**) welcomes the opportunity to provide feedback on two exposure drafts of new open banking regulations provided by MBIE for public consultation, being the:

(a) Customer and Product Data (Banking and other Deposit Taking) Regulations 2025, which will designate the banking sector; and

(b) Customer and Product Data (General Requirements Regulations) 2025, which prescribe general requirements for regulated data services provided under the Customer and Product Data Act 2025 (**Act**).

1.2 This submission has been prepared with input from the Law Society's Human Rights and Privacy and Commercial and Business Law Committees.[1] There are important unresolved concerns with privacy arising from the proposed regulations, other gaps in the regulations that will affect their workability for both business and enforcement purposes, and some drafting queries.

(a) From a privacy perspective, key gaps in the proposed regulations include:

(i) no process for identity verification;

(ii) inadequate provision relating to consent;

(iii) the need to ensure that there are meaningful obligations and consequences for privacy breaches by an accredited requestor.

(b) In the Banking regulations, the unduly broad scope of designated customer data, arising from the definition of "designated data", could lead to privacy compliance risks.

(c) Beyond privacy matters, there are further issues and gaps, including a number of concerns with enforcement:

---

1 More information about our law reform committees is available on the Law Society's website: https://www.lawsociety.org.nz/branches-sections-and-groups/law-reform-committees/.

(i) clear liabilities in the event that false and/or misleading information is provided through an intermediary;

(ii) remedies for losses banking customers have suffered as a result of scams or fraud;

(iii) the draft regulations do not currently specify penalty tiers or quantum for non-compliance by accredited requestors or data holders;

(iv) the draft regulations grant the Chief Executive discretion to assess compliance and revoke accreditation, but lack defined escalation pathways or formal enforcement tools.

(d) "Designated actions" in the Banking regulations as presently drafted do not capture payments requiring the authority of two or more persons, which will limit their application in many business contexts.

(e) While the drafts refer to "systems," "electronic facilities," and "security safeguards," they do not specify minimum technical standards.

2 General comment

2.1 The Law Society considers that, at best, the issues identified in the draft proposals and listed above leave the new consumer data right (**CDR**) scheme undesirably uncertain. In likelihood, if these matters are not addressed, they will heighten the risk of privacy breaches and interferences, and risk undermining public confidence in and workability of the new scheme. This would be a lost opportunity and could undermine the benefits of these otherwise widely supported and important new proposals.

2.2 The Law Society notes the unusually short time of a fortnight that has been allowed for this consultation, indicating that work continues to proceed at pace. We urge MBIE to frontload the investment of time in developing the regulations, to ensure that the regulatory framework is watertight and workable, even if that requires taking slightly more time to progress the proposals. In the Law Society's 2024 submission on the Consumer and Product Data Bill,[2] we raised concerns about the significant amount of detail delegated to secondary legislation and the risks of doing so. Those concerns have not been alleviated by these draft regulations, which are lacking depth, consistency, and robustness. To the contrary, the draft regulations are significantly 'lighter touch' than their Australian counterpart, exacerbating those concerns.[3] In the Law Society's submission on the Bill, we referred to the Australian version for consideration of its privacy safeguards. The reasons are unclear for departing so significantly from the Australian example, which could be a valuable guide. The four major banks in New Zealand are all subsidiaries of Australian parental entities, meaning that the parent entities are already subject to the CDR regime in Australia. Closer alignment of New Zealand's regulation with Australia's could reduce the compliance burden on these entities.

---

2 New Zealand Law Society Customer-and-Product-Data-Bill.pdf (5 September 2024).

3 Competition and Consumer (Consumer Data Right) Rules 2020 (Aus).

3 Identity verification

3.1 The Act says that when a data holder receives a request, they must verify the identity of the person who made the request "in the manner (if any) prescribed by the regulations and standards".[4] However, as proposed, neither of the draft regulations provide for this process. The absence of any regulations or standards as contemplated by the Act, prescribing how identity is to be verified, means the duty in section 45 exists in principle but has no operational detail. This is an undesirable position, because it creates uncertainty for everyone and is likely to lead to inconsistent, and potentially ineffective, methods of identity verification.

3.2 Given the sensitivity of financial data and the risks of fraud and unauthorised disclosure, it is important that the regulations prescribe minimum identity verification requirements (such as by requiring alignment with existing strong customer authentication under AML/CFT and online banking protocols). Leaving the matter to the discretion of data holders risks inconsistent approaches, erosion of customer trust, and potential breaches of the Privacy Act 2020 (**Privacy Act**). For comparison, we understand that the Australian CDR has an explicit framework for identity verification, provided for through Data Standards.[5]

3.3 In New Zealand, even if it were considered that Information Privacy Principle (**IPP**) 2(1) imposes a relevant requirement,[6] this would be confined to individuals, not other types of entities. This leads to a more general concern, which the Law Society raised in its earlier submissions. Given the limitations of the Act and (now) proposed regulations, affected persons may well need to rely on existing legal protections outside of the Act (if available). For example, for privacy breaches relating to personal information, the individual customer may have a claim under the Privacy Act. For other kinds of customers or data, including corporate data, the customer may have a claim due to a breach of contract or breach of the common law rules around breach of confidence. The Crimes Act 1961 may also apply (through the prohibition against causing loss by deception) to the person perpetrating a fraud, if they can be identified.

3.4 However, this patchwork approach leaves significant legal uncertainty. It would be better, both as a legal matter and for ease of users, for the regulations or the Act to clarify obligations and liabilities. The same concern about the Privacy Act's limitations in this context extends to other features of the CDR scheme, such as the scope of information collected, as we discuss further below. Even where the Privacy Act goes some way in some circumstances, such as preventing scope creep by requiring that personal information (that is, relating to an identifiable individual, thus not a sufficient safeguard in respect of all entities) collected is necessary for the intended purpose, the regulations should provide a 'belt and braces'. In the Law Society's view, they should set out key matters, including privacy safeguards, clearly as a code.

3.5 It should be noted that, compared to New Zealand, the Australian privacy legislative regime has more "teeth" (in other words, is already providing a stronger framework

---

4 Customer and Product Data Act 2025, s 45(3).

5 See Data Standards Body.

6 Privacy Act 2020, s 22. IPP 2(1) provides that "If an agency collects personal information, the information must be collected from the individual concerned."

for privacy protection). It then is further reinforced by Australia's more comprehensive and explicit CDR standards.

4 Quality of consent

4.1 MBIE's policy documents relating to the CDR scheme emphasise informed, express consent and consumer control over data sharing. Customers can withdraw consent at any time.

4.2 However, the Law Society is concerned there is a lack of clarity in the Act as to what consent looks like, and the regulations do not provide further detail. For instance:

(a) Is consent granular (by data type, by duration, by purpose)? For comparison, we note Australia's approach of defining different types of consents, including: a collection consent, a use consent, a disclosure consent, a direct marketing consent, and so on.[7] There is no such equivalent — or provision relating to consent at all — in the proposed regulations.

(b) Are consents time-limited or automatically expiring, or reusable across parties? Judging by the provision referring to re-notification at 12-monthly intervals,[8] it does not appear that a time limit is proposed, and this poses a significant risk to consumers, requiring of them substantially more diligence. By contrast, see the Australian ongoing notification requirement of 90 days.[9]

(c) Do mechanisms respect joint account holders and corporate accounts? Special rules in Australia, involving additional requirements, apply to joint accounts with two or more individual account holders.[10] As we further discuss below, the draft provisions also have a potentially significant gap in this respect when defining "designated actions".

4.3 Overall, the Law Society is concerned that a blanket and open-ended approach to consent in the CDR scheme:

(a) poses an oversharing risk to consumers who may not understand, or be able to understand, the nature of the consent they are providing; and

(b) exposes agencies involved in the CDR scheme to risk of non-compliance with the Privacy Act, for example by obtaining information without consent or other lawful basis, and/or retaining information longer than it can be lawfully used.

---

7 Competition and Consumer (Consumer Data Right) Rules 2020 (Aus), r 1.10A; see also r 4.11(1) (asking CDR consumer to give consent), which refers to "allow[ing] the CDR consumer to actively select or otherwise clearly indicate the particular types of CDR data to which the consent will apply".

8 Customer and Product Data (General Requirements) Regulations 2025, reg 10.

9 Competition and Consumer (Consumer Data Right) Rules 2020 (Aus), r 4.20; compare further the clear process for amending consents, withdrawing consents, consent duration, consent expiry: rr 4.12A–4.14.

10 Competition and Consumer (Consumer Data Right) Rules 2020 (Aus), Pt 4A.

4.4 The Law Society recommends reconsidering the omission to consider and/or provide for these issues. The alternative leaves significant gaps in the regime, not consistent with the Ministry and Minister's publicly stated policy intentions.

5 Accredited requestor obligations

5.1 Another gap in the regulations relates to accredited requestor obligations. Accredited requestors[11] should be subject to meaningful obligations and consequences for privacy breaches commensurate with the scope of their authority to act on behalf of consumers. The Law Society is concerned that, as proposed, the regulations do not address this and there is no provision for privacy compliance standards or ongoing oversight of privacy compliance behaviours for accredited requestors.

5.2 Ways of addressing the concern could include requiring:

(a) privacy impact assessments to be completed by applicants before they receive accreditation;

(b) incident response protocols for accreditation (e.g. for notifiable breach compliance); and/or

(c) ongoing oversight of accredited requestors to ensure a continued commitment to privacy compliance (e.g. periodic compliance audits).

5.3 Additional provisions of this nature would sit naturally in the General Requirements regulations. They would be in keeping with, for example, reg 10 (accredited requestor must periodically notify customer about authorisations) and reg 13 (accreditation matters relating to reasonably adequate cover for liabilities).

6 Scope of designated customer data and oversharing risk

6.1 Although customer consent is the "trigger" for information sharing under this regime, the regulatory definition of "designated data" determines the default menu of information that must be released when consent is given.[12] If the definition is too expansive, consent becomes less meaningful and accredited requestors could face downstream Privacy Act compliance risks.

6.2 Even though the customer has requested the data:

(a) The breadth of what counts as "designated data" still matters. The regime will likely require the customer to consent to all of the designated data types for a given service request, not necessarily to pick and choose line items. If the definition of designated data is very wide, the risk of "bundled" consent arises: in other words, customers being forced to release more information than is reasonably necessary to access a service. Some of the information such as loyalty programme data or cashbacks may reveal behaviour or lifestyle patterns that go beyond typical banking data. From a practical privacy

11 Referred to in both sets of draft regs but primarily the Customer and Product Data (General Requirements) Regulations 2025.

12 Customer and Product Data (Banking and other Deposit-Taking) Regulations 2025, reg 7 (designated data).

perspective, customers may not realise that "transaction history" or "loyalty programmes" or "data about insurance or travel benefits" could contain highly sensitive inferences (about, for instance, health-related purchases, gambling, or political donations). If the designation is too wide, consent risks being uninformed or misleading.

(b) If the designation sweeps too broadly, it puts requestors in a difficult position too, as they may be receiving personal information they cannot justify retaining or using. IPPs 1 (purpose of collection) and 8 (accuracy) still apply. Even if consent is the legal basis, accredited requestors must only collect what is necessary for the stated purpose.

6.3 For these reasons, reg 7 of the Banking and other Deposit-Taking Regulations is concerning as presently drafted. Reconsidering the breadth and approach of this regulation would be advisable.

6.4 For comparison: the Australian Rules include rule 1.8, defining a "data minimisation principle". The rule provides:

> (1) The collection of CDR data by an accredited person complies with the ***data minimisation principle*** if, when making a consumer data request on behalf of a CDR consumer, the accredited person does not seek to collect:
>
> (a) more CDR data than is reasonably needed; or
>
> (b) CDR data that relates to a longer time period than is reasonably needed;
>
> in order for it, or a relevant CDR representative, to provide the goods or services requested by the CDR consumer.
>
> (2) The use or disclosure of CDR data by an accredited person or a CDR representative complies with the ***data minimisation principle*** if, when providing the requested goods or services, or doing any other thing that constitutes a permitted use or disclosure of collected CDR data, the use or disclosure of the collected data, or any CDR data directly or indirectly derived from it, does *not* go beyond what is reasonably needed in order to provide the requested goods or services or to effect the permitted use or disclosure.

6.5 Regulation 7(1)(d) is an example where an equivalent provision would assist in containing the otherwise broad scope of the "designated data" definition. This paragraph of the definition includes: "particulars of each transaction for a relevant account that occurred during the 2-year period before the time of the request under section 15 of the Act": a swathe of information that some types of services may require, but in many other types of cases will not be relevant.

7 Enforcement

Accreditation matters when an intermediary is acting: company liability for providing false or misleading information

7.1 It is unclear what liability the accredited requestor will bear in practice (if any) in relation to a client to whom it is providing an intermediary service. One can anticipate issues arising if the Chief Executive of MBIE is provided with false and misleading due diligence materials relating to a particular company or, if in practice, that company fails to keep the customer data secure or fails to prevent fraudulent requests. There is no distinct liability framework under the Act that regulates the company in such a

scenario. The intermediary accredited requestor has liability for contravening the Act, but also defences (if the contravention was due to the reasonable reliance on information supplied by another person or if the contravention was beyond its control and the accredited requestor took reasonable precautions and exercised due diligence to avoid the contravention). This leaves a gap, which should be addressed.

Remedies for affected persons

7.2 There remains uncertainty around:

(a) whether customers will have accessible remedies for losses suffered as a result of scams or fraud perpetuated through mandatory payment initiation APIs; and

(b) what steps the industry will need to take to address this risk and to support confidence in the system.

Penalties

7.3 The draft regulations do not currently specify penalty tiers or quantum for non-compliance by accredited requestors or data holders. This absence risks undermining deterrence and creates uncertainty for regulated entities. Enforcement relies heavily on discretionary powers and external statutes (such as the Privacy Act), which may not be tailored to the specific risks of data misuse under this regime. In contrast, Australia's CDR regime provides clear civil penalty provisions, including fines up to $2.5 million for serious breaches. The Law Society recommends establishing a structured penalty framework within the regulations.

Defined enforcement pathways

7.4 The draft regulations grant the chief executive discretion to assess compliance and revoke accreditation, but lack defined escalation pathways or formal enforcement tools (e.g. infringement notices, enforceable undertakings, or public sanctions). This limits the regulator's ability to respond proportionally to non-compliance and creates uncertainty. By comparison, Australian regulators (the ACCC and OAIC) are empowered to issue infringement notices, accept enforceable undertakings, and initiate proceedings.

8 Other gaps

Designated actions

8.1 As defined in the Banking and other Deposit-Taking Regulations, "designated actions" does not currently capture payments that require the authorisation of two or more persons.[13]

8.2 This will limit its use in some personal and business situations and the Law Society queries whether this omission (without, seemingly, any alternative provision) is intended.

---

13 Customer and Product Data (Banking and other Deposit-Taking) Regulations 2025, reg 8(2)(d).

Minimum technical standards

8.3 While the drafts refer to "systems", "electronic facilities" and "security safeguards", they do not specify minimum technical standards (e.g. encryption, authentication protocols, API specifications). There are no mandated secure protocols to apply in the implementation — for example, OAuth 2.0, OpenID Connect, TLS 1.3, and AES-256 encryption for data exchanges. This leaves room for inconsistent implementation and interpretation. By contrast, Australia's CDR regime is underpinned by a comprehensive technical framework maintained by the Data Standards Body. This includes mandatory use of secure authentication protocols (OAuth 2.0, OpenID Connect), encryption standards (TLS 1.2+, AES-256), and standardised data formats (JSON, RESTful APIs), specified in Consumer Data Standards.

9 Drafting points

Ambiguous wording of regulation 3 (overview)

9.1 Regulation 3, in both the General and Banking draft regulations, provides:

(a) in 3(1), an overview of the purposes of each regulation; and

(b) in 3(2), a cross-reference to the other regulation.

9.2 In both, a following clause then says: "This regulation is only a guide to the general scheme and effect of these regulations and [the other regulation]".[14]

9.3 We assume that the drafting intent in referring to "this regulation" is a reference to the 'overview' provision, regulation 3, being a general guide to "these regulations" (the whole instrument). That may be self-evident to those versed in drafting conventions; however, the Law Society queries whether it is advisable to rely on this quite technical distinction being easily understood by all those who will seek to use and rely on the CDR scheme. If rewording were possible, it would avoid ambiguity and any resulting risk of misinterpretation, and therefore could be desirable. One option may be to refer more narrowly to the specific preceding parts of the regulation (eg, reg 3(1) and (2)) that are only provided as a guide.

Correcting typos

9.4 The General Requirements regulations have the following errors, which should be corrected:

(a) In reg 6(2)(b), correct "reasonable" to "reasonably".

(b) In reg 10(2)(b), correct "12-months" to "12 months".

(c) In reg 14(2)(b), delete the word "each".

(d) In reg 14(4), correct "facilities" to "facilitates".

---

14 Customer and Product Data (General Requirements) Regulations 2025, reg 3(3); Customer and Product Data (Banking and other Deposit-Taking) Regulations 2025, reg 3(4).

10 Next steps

10.1 We hope this feedback is useful. Please feel free to get in touch with me via the Law Society's Senior Law Reform and Advocacy Advisor, Claire Browning (claire.browning@lawsociety.org.nz) if you have any questions or wish to discuss the feedback further.

Nāku noa, nā

David Campbell
Vice-President