Financial Services Council NZ

Grow the financial confidence and wellbeing of New Zealanders

March 2025

FSC Debrief – Customer Product Data Act

Background:

This Act follows an exposure draft on a Customer and Product Data Bill which the FSC provided feedback on in July 2023 and options for establishing a Consumer Data Right in 2020.

You can view the Report of the Economic Development, Science and Innovation Select Committee of 23 December 2024 here and the final Act here.

Overall:

- **Addressed:** Lead-in time and sequencing for implementation; dispute resolution membership.
- **Partially Addressed:** Customer authorisation obligations, safe harbour for accredited requestors and some alignment with Privacy Act.
- **Not Addressed:** Definition of "ordinarily publicly available" data, detailed de-identification requirements, expansion of refusal grounds, regulator independence, retention/deletion obligations, cross-border transfers, damage caps and explicit alignment with DISTFA.

Proposal	FSC Submission Recommendation	Final amendments	Outcome indicator Poor Medium Good
Product Data – "ordinarily publicly available" (Part 2, cl. 100(2))	We submitted that clarity was required on what constitutes "ordinarily publicly available" product data, given penalties for non-compliance.	The Act allows regulations to specify designated product data but does not define "ordinarily publicly available".	
De-identification requirements (Part 2, cl. 34)	We submitted that regulations or standards include what is considered de-identified, methods to manage re-identification risk.	The Act provides that regulations and standards may specify requirements for handling and de-identifying data but does not prescribe definitions or methods. Detail deferred to regulations	
Customer authorisation	We submitted that "reasonably informed"	The Act sets out requirements for customer authorisation and	

Level 17, Commercial Bay Tower | 11-19 Customs Street West | Auckland 1010 | New Zealand
P +64 (09) 802 1532 | E fsc@fsc.org.nz | W fsc.org.nz

"reasonably informed" (Part 3, cl. 36)	must include details of what data is collected, how it is used, who can access it, for how long, and how authorisation can be withdrawn.	obligations once authorisation ends but does not define "reasonably informed" in detail. Likely to be fleshed out in regulations.	
Right to refuse requests. Harm exemptions (Part 2, cls. 16 & 20)	We submitted that refusal grounds should be expanded and that data holders should not be obliged to proactively check for harm in every request.	The Act retains refusal provisions where harm is likely but does not expand grounds significantly or relieve holders of proactive assessment obligations.	
Complaints and dispute resolution (Part 3, cls. 49–53 and 112)	We sought clarity on complaints processes between MBIE and the Privacy Commissioner. We requested a definition of complaints, and that existing dispute resolution schemes be used.	The Act requires accredited requestors and data holders to meet dispute resolution scheme requirements. Complaints processes are not fully defined in the Act. Overlap with Privacy Act unresolved.	
Privacy Act alignment (Part 3, cls. 52–53, IPPs 5–9)	We submitted that the Bill should clarify the relationship with the Privacy Act, include data retention/deletion requirements, address cross-border transfers, and consider a dedicated CDR privacy code.	The Act confirms certain contraventions will be treated as interferences with privacy under the Privacy Act. No explicit retention/deletion obligations or cross-border provisions were included. No separate privacy code created.	
Regulator powers and independence (Part 4, cls. 96–100)	We submitted that MBIE's powers should be ring-fenced, with clearer limits on urgent changes, and a separate regulatory unit should be considered.	The Act confirms MBIE's role as regulator with broad powers, including setting standards and technical infrastructure. No additional safeguards or ring-fencing were introduced.	
Safe harbour and liability (Part 4, Subpart 2)	We submitted that safe harbour protection should apply when acting in accordance with standards, and intermediaries should be held responsible.	The Act provides a defence for accredited requestors where they could not reasonably know an authorisation had ended. Obligations for intermediaries are expected via regulations but not detailed in the Act.	

Consultation, sequencing, and lead-in time (Part 5, cls. 131 etc.)	We submitted that consultation rights should include all affected data holders, that "substantially affected" be clarified, and that sufficient lead-in time be provided.	The Act requires consultation with "substantially affected" parties but does not define the term. Lead-in times for banking have been set (Dec 2025–2026), providing time for compliance.	
Digital Identity alignment (cl. 44)	Verification under the Digital Identity Services Trust Framework Act (DISTFA) should satisfy verification requirements.	The Act requires data holders to verify identities but does not expressly recognise DISTFA compliance as sufficient. Alignment may be achieved via regulations. Not addressed.	
Penalty regime and damages (Part 3, cls. 52–53)	We submitted that the Bill should set caps on damages for contraventions deemed "interferences with privacy".	The Act retains the open-ended Privacy Act damages regime and includes fines for certain contraventions but does not set a cap on damages. Not addressed.	