Māori data governance expert advice on open banking

5th September 2025

From: Ernestynne Walsh (Māori Data Service Lead, Nicholson Consulting)

To: Personal information

Ko te pae tawhiti whāia kia tata, ko te pae tata whakamaua kia tina

Pursue the distant horizons so they may become close, and secure the achievements that are already at hand

Purpose

1. The Government has drafted regulations that would enable open banking under the Customer and Product Data Act 2025. The regulations would require specified data holders in the banking sector to share customer and/or product data with accredited data requestors, with the customer's approval.
2. The Act requires consultation on proposed regulations with someone who has expert knowledge of te ao Māori approaches to data. Nicholson Consulting's Māori data team, who have experience in the banking sector, has been commissioned to write a short report for MBIE that analyses the proposed regulations that will enable a consumer data right in the banking sector.
3. This report assesses:
    a. How proposed regulations align or support Māori data governance (MDG),
    b. How the Payments NZ API Centre Banking Standards can be used to support MDG and,
    c. Considerations to better align with the MDG model and otherwise support te ao Māori approaches to data

Summary of findings

4. The purpose of this report was to look at regulatory and API Centre Standards alignment with MDG and to identify whether there were further areas for improvement. Table 1 provides a summary of the findings. The Customer and Data Product Regulation provides clear alignment from a MDG perspective with regards to data collection, protection, access, sharing and use.

Table 1: Summary of MDG alignment and areas for improvement

Pou	Regulation Alignment	API Centre Standards Alignment	Areas for further improvement
Pou 1: Data capacities and workforce development			⚠
Pou 2: Data infrastructure			⚠
Pou 3: Data Collection	✓	✓	
Pou 4: Data Protection	✓	✓	⚠
Pou 5: Data access, sharing and repatriation	✓	✓	
Pou 6: Data use	✓	✓	⚠
Pou 7: Data quality and system integrity		✓	⚠
Pou 8: Data classification			⚠

5. The Payments NZ API Centre has strong consent mechanisms to ensure that there is appropriate access to account information and that payment initiation has also been consented separately. The regulation provides a detailed set of data that data holders are required to provide and the data requested seems appropriate for the potential purposes.
6. There are strong security features in place to ensure data is protected. However, the API Centre Standard v3.0.1 does contain major upgrades to the security profile which would be beneficial to adopt longer-term. Further considerations should be given to data jurisdiction with a reference around storage in Aotearoa being preferred where practical. This statement could be added to the Operating Standards.

7. Longer term considerations around middleware providers should be explored to ensure that negative consequences of a fragmented system are reduced. This could help organisations reduce the learning curve and enable them to focus on functionality rather than integration.
8. Whilst many general use-cases are covered there are specific scenarios that require more than one person to authorise which are out of scope. These are more likely to impact complex collective structures that are seen in te ao Māori such as whenua trusts. Longer term, the scope of the regulation should include these complex examples that require multiple authorisations. The API Centre Standards would need to be updated to cater for multi-authorisation consent and would also need to be mindful of collective privacy which would likely require mandating unique immutable identifiers for protection purposes.
9. A more profound change that could be explored is the monitoring of system equity for Māori. This would require determining the appetite for such change and then a lot of foundational work to explore new consent mechanisms, standards, and new data capture to identify Māori customers and Māori businesses for equity monitoring purposes.

Approach to the review

10. This review uses the MDG model published by Te Kāhui Raraunga to analyse the proposed regulations. It contains eight pou/pillars that include: data capacities and workforce development, data infrastructure, data collection, data protection, data access and sharing, data use (including consent), data quality and system integrity, and data classification. The pou relating to data capacities and work force development, data infrastructure, and data classification have not been commented on until the future improvements section as there was little that could be recommended within the implementation time frames.
11. The draft regulations and the regulatory impact statement on MBIE's website were reviewed for alignment with MDG against the MDG pou.
12. The Payments NZ API Centre Standards v.2.3.3 were reviewed. This is the standard that the banks have committed to implement by the time the regulations come into force. In addition, the API Centre Operational Standards, which cover how the API Centre Standards should be used, were also reviewed to see how MDG could be supported.
13. Other documents that were read to inform the response and create better alignment with the MDG model included previous work that Nicholson Consulting delivered for Payments NZ such as Ngā Tohu Ārahi – the data handling guidelines.
14. Meetings were held with the MBIE Commerce, Consumer and Business team to ask clarifying questions about the regulation and a hui with Payments NZ to confirm the understanding of some of the APIs.

Regulation alignment with MDG

15. The Customer and Product Data Act 2025 sets out the legal framework. There are two sets of regulations that set out the rules made under the authority of the legislation. These include the Customer and Product Data (General Requirements) Regulations 2025 and the industry-specific Customer and Product Data (Banking and other Deposit Taking) Regulations 2025.

Pou 3: Data collection

16. The regulations clearly outline possible types of data that could be collected from data holders. The data collected seems to be close to the minimum amount of data necessary for customers to use effectively.
17. From a digital equity perspective requiring an electronic system to provide regulated data services may mean that parts of the community that have digital connectivity issues may find it more challenging to request their data.

Pou 5: Data access, sharing and repatriation

18. The Customer Data and Product Act, 2025 is designed improve the ability of customers, and third parties they authorise, to access and use the data held about them by participants in those sectors. Having the customer decide who their data is shared with and removing barriers to access strongly aligns with MDG principles around data access and data sharing.

Pou 6: Data use

19. How the data will be used is the decision of the customer. Some of the potential uses might include: budgeting, making payments, home loan applications. It appears that some potential uses for customers and businesses will be out of scope for the current regulation such as: KiwiSaver, investment platforms, overseas payments or data for any use from those who are not accredited data holders. In addition, corporates such as iwi asset-holding companies will find that many of their use cases such as lending for business acquisition or trade financing for exports will also be out of scope.
20. Consultation with Māori has occurred and presented within the regulatory impact statement. It was felt that the regulation would help family trusts and Māori organisations access the personal information more effectively. However, with the added complexities that come with whenua Māori, some Māori trusts that have complex account ownership and policies around approving transactions may still find

it challenging to access data. Over time, the regulation may wish to expand the required accredited data holders or the breadth of designated actions.

21. The regulation does not speak to consent which is considered important from an MDG perspective. However, consent is covered extensively in the API Centre Standards which are referenced in the regulatory impact statement. All the currently listed data holders in s6(1) of the regulation have committed to consent requirements covered in the API Centre Standards.

Payments NZ API Centre standards to support MDG

22. Payments NZ is a governance organisation at the heart of Aotearoa New Zealand's payments system. In 2019, Payments NZ established the API Centre. It aims to develop a standardised approach to data-sharing arrangements between banks and fintechs to increase efficiency, reduce costs and further enable uptake of open banking services.
23. The Customer and Product Data Act 2025 requires certain controls, standards, and functionality in connection with these data services. The Payments NZ API Centre standards can be used to support the requirements set out in the legislation and regulations.

Pou 3: Data collection

24. The regulation may need to expand to capture data that is needed. The API Centre Standards make it optional to provide a unique transaction id even in the latest v3.0.1 standard. A unique identifier would minimise risks of transactions being processed twice due to timing out or retry attempts. Without unique, immutable identifiers, it is difficult for accredited requestors to reconcile new transactions that have been received from a data holders API and which are existing transactions that require updates which could lead to issues displaying the correct balances. Having a mandatory transaction id in future API Centre Standards would help minimise potential risks.
25. In addition, the status does not fully capture end-to-end status. Currently, domestic payments today have a 'pending' and 'booked' status that capture whether the payment is ready for further processing and that the bank has agreed to pay. From a Māori data perspective, capturing a richer whakapapa or lineage of payments is important. Adding additional statuses such as 'cleared' will make it easier for customers to understand when the money has been transferred to the other party. Collecting this information could be relevant for customers and businesses who have tight cashflows.
26. The API Centre Customer Standard notes that data collection is necessary for the purpose. Currently, API calls do not have a field to describe data use purposes

instead it can be covered through terms and conditions. From a MDG perspective, data use purposes should be clearly presented to the customer at the point of data collection and should be used strictly for that purpose only as outlined in the secondary share requirements within the Operational Standards which describe who is sharing, what data is being shared, why, and for how long.

Pou 4: Data Protection

27. From an MDG perspective, there are also collective privacy considerations. For instance, some of the data might represent a collective such as a whānau. Through the API Centre Standards it appears that it is possible to create a simple concept of a whānau, hapū or trust through a joint account or through retrieving designated data from multiple individual accounts. However, more complex corporate structures might be easier to replicate through social graph structures which are not currently part of the API Centre standards. Furthermore, the current regulations note that designated actions cover payments that do not require the authorisation of 2 or more persons.
28. The API Centre Security Standard notes that appropriate security measures must be in place. In addition, the Register Standard also cover public keys and the signing of certificates. The API Centre security profile provides more details of what this would look like in practice covering access tokens, refresh tokens, OAuth 2.0, certificates and private keys. One additional MDG consideration from a security perspective is the whakapapa information such as facial ids, voice id or fingerprints. This information is considered tapu and should be stored separately either logically or physically.

Pou 5: Data access sharing and repatriation

29. The API Centre Standards provide a mechanism for data holders to access and share account information and payments information. Having standardised APIs will make development easier which will further reduce barriers to access for customers including Māori customers.
30. Currently data holders would need to make available the previous 2 years' worth of designated data. Whilst some might argue from an MDG perspective that more previous data should be made available, looking at the possible use cases (budgeting, loan applications etc), it is likely that 2 years is sufficient. Some special use cases such as risk modelling or tax auditing – which could require up to 7 years of data would be out of scope.

Pou 6: Data Use

31. The Operational Standards particularly the customer standard is very explicit that consent can be revoked at any point in time by the customer. In addition, for enduring payments a duration must be specified with the consent alongside a maximum amount limit. With lapsed or revoked consent the customer can request that their data be deleted and no longer used.
32. The standards speak specifically to scenarios around informing customers about other service providers who may have access to the data to perform a specific task. It must be clear who the party is, the purpose of the service and the terms and conditions. There could be more detailed standards such as creating functionality within the user experience to view a summary of what a customer has consented to and the type of consent to help provide transparency on what data customers have consented to being collected and used.
33. The API Centre Standards have strong MDG alignment with best practice around consent. In this context consent is explicit, informed, and customer driven. The consent mechanism also provides the ability for customers to revoke long lived consent regarding a recurring payment to a beneficiary or access to a customer's account information. Separate consents are used for account information and initiating of a payment. In a scenario where multiple bank accounts are held, consent would need to be obtained for each bank account. This could be seen as an extra layer of protection, but it does require multiple consent flows, so care needs to be taken to ensure data holders cater for separate consents.

Pou 7: Data quality and system integrity

34. The API Centre Standards use JSON with full UTF-8-character which allows macrons and other diacritics from other languages to be displayed correctly. Most New Zealand banks rely on mainframes that use the EBCDIC character set which are unable to display diacritics. From a Māori data perspective, names should be correctly spelt which includes correctly displaying macrons.
35. In addition, restricting character sets that exclude macrons and other diacritics makes digital identity proofing harder because of the difficulty in finding an exact match to the name of a person, business, government institution, or a place. Data quality is very important for digital identity. Fuzzy matching on names and dates may not be appropriate in this context because people and businesses will want their payments and their account information accurate. Data holders, where possible, should not limit character encoding when creating mechanisms to provide the designated data.
36. From an MDG perspective data quality is very important. The Iwi Data Needs Paper noted that data should be relevant, timely, appropriate, available and accessible. Payment information is highly volatile with pending payments and fraud checks

before a payment is complete. Consequently, the data requestors may need to build functionality on top of the existing Payments NZ APIs to check for accuracy and that payments information from data holders is up to date.

37. The Operational Standards by the API Centre provide a set of standards that apply to all data including Māori data. These standards outline expectations relating to consent, privacy, collection of the minimum amount of data required to fulfil a lawful purpose. The standards also outline expectations around obtaining consent from the customer to disclose data to other parties who provide other support services required to carry out the purpose of the data collection.

Further improvements to better align with MDG

38. The following sections comments on elements that were not explicitly mentioned in the regulation of the API Centre Standards. These considerations would take longer to implement and should be considered in future iterations of the regulations.

Pou 2: Data infrastructure

39. The regulation may also wish to consider the role of middleware providers. Having the main banks separately build their own APIs on top of the Payments NZ APIs will require more efforts from fintechs to ensure that their products integrate with each of the banks, investment platforms and other third-party tools they use.
40. Using consistent infrastructure could also help Māori businesses, and businesses in general, with pou 1 data capacities and workforce development by building fintech capability faster by simplifying data integration. This allows teams to focus more on developing features and innovating. This sentiment was echoed in the regulatory impact statement with feedback from the consultation noting that the regulations will make it easier for Māori organisations to become accredited fintechs to offer specialist data capability and functionality for Māori groups. Without the appropriate middleware, the current data holders who are the major banks could become entrenched and make it more difficult for Māori fintechs to enter the market.

Pou 4: Data protection

41. V3.0.1 of the API Centre Standards provide major upgrades to the security profile to align with international standards and best practice. In v3.0.1, the security standards and functional specifications are decoupled meaning it is easier to quickly make security updates. From a MDG perspective, regulation should explore the adoption of the v3.0.1 API Standard in due course to allow quicker upgrades to specs in response to the changes to the security landscape, international standards and allow for more complex consent scenarios to be managed.

42. In addition, a major change with v3.0.1 is the event notification which provides the ability to push notifications out to customers in scenarios where consent has been revoked or expired. This could be useful for scenarios such as Māori organisations with multiple signatories or whānau with joint accounts to promptly notify customers of changes that might impact their ability to pay.
43. The latest version of the API Centre Standards (v.3.0.1) do not allow for multi-authorisation consent. This should be addressed in subsequent iterations of the API Centre Standards to allow for more complex collective use cases that are relevant to Māori whānau, whenua trusts and tribal collectives. When introducing new standards to cater for collective there should also be considerations for collective privacy. In scenarios with collective information such as joint account information, there should be no cross over in identifiers that would enable an individual to correlate payment information relating to other individuals. Furthermore, when providing information to a collective, for instance a loan application, the feedback should treat the collective as its own entity rather than highlighting specific financial attributes of the individuals.
44. From a MDG perspective, it is preferred to have data stored in Aotearoa where it is easier to assert control. There are now organisations, some of which are iwi owned, that offer data residency within Aotearoa. In addition, the larger banks must comply with the BS11 Reserve Bank of New Zealand's Outsourcing Policy to ensure that outsourcing arrangements do not compromise a bank's ability to maintain critical functions such as basic banking services. Given, most of the data holders are Australian owned there might be questions raised about whether more control and independence could be maintained through having infrastructure in Aotearoa. MDG considerations should form part of the decision on where to store and process data alongside redundancy and failover options and compliance.

Pou 6: Data use

45. Current regulations note that designated actions cover payments that do not require the authorisation of 2 or more persons. This should cover use cases such as budgeting, making payments, home loan applications. However, there are scenarios where collective ownership and a focus on collective outcomes that are more likely to surface in a Māori context such as collective marae fundraising, managing whenua Māori, microfinancing for Māori businesses or whānau needing a small loan or iwi-based insurance. Scenarios that require authorisation from multiple people are out of scope. Longer term, there could be changes to regulation to allow for scenarios where there are multiple people authorising. More coverage of various use cases will increase the usefulness of the regulation. V3.0.1 of the API Centre standards does not handle multi-authorisation-consent authorisation but subsequent versions of the standards could introduce multi-authorisation consent.

Pou 7: Data quality and system integrity

46. The regulatory impact statement notes monitoring system performance with the API Centre Operational Standards confirming that aggregate reporting on APIs will occur monthly. These cover non-functional requirements around availability and response time of APIs. A more ambitious form of monitoring is system equity such as financial inclusion or measuring equity of outcomes such as improving pricing deals across different customer segments. Targeted products may also help data holders retain customers and improve profit margins. Equity monitoring, would require engagement first to understand the appetite for such monitoring and would require a lot of preliminary work such as determining how consent would work in such a scenario, the capturing of data to classify Māori businesses and Māori customers, standards relating to Māori data including determining whether the API Centre register should identify Māori businesses, and updating the API Centre Standards to surface demographic information.

Addendum to Māori data governance expert advice on open banking

3rd October 2025

Purpose

1. A short report titled *Māori data governance expert advice on open banking* was delivered 5th September 2025. The report can be viewed here

Māori data governance expert ad

2. Following the deliverable of this report, MBIE requested that the scope of the work be revised to understand: What are the implications, if any, of the proposed accreditation fees for fintechs on Māori data governance (MDG)?
3. This document is an addendum designed to answer that specific question and should be read in conjunction with the original report containing guidance on MDG expert advice on open banking.

Approach to review

4. The MDG model published by Te Kāhui Raraunga covers eight pou (pillars). Under the data use pou it is noted that barriers to accessing and using data should be removed. Examples of barriers include financial costs and interoperability issues. In addition, transparency is an important component of the data use pou.
5. Given that the MDG model doesn't go into depth around costing guidance, the MDG values of being accountable, nurturing data as a taonga, and putting iwi-Māori data in iwi-Māori hands are also referred to in this report.
6. The Customer and Product Data Act Fees document was reviewed for alignment with the MDG data use pou.

Customer and Product Data Act Fees

7. MBIE is proposing to charge accreditation fees in regulated open banking under the Customer and Product Data Act 2025. The Customer and Product Data Act Fees document includes proposed fees and rationale.

Pou 6: Data Use

8. Accreditation will promote confidence among customers that data requestors will hold data safely and securely which aligns with the MDG value of nurturing data as a taonga.
9. The fees are set at a level that recovers costs. Accredited requestors are the primary beneficiaries and responsible for generating the cost of accreditation. Cost recovery ensures that accredited requestors are responsible for the costs they are generating without being excessive which could prevent putting iwi-Māori data in iwi Māori hands.
10. The accreditation costs could be considered large for smaller accredited requestors which could create barriers to accessing and using data. MBIE should review feedback from accredited requestors and potentially introduce a new application type if the fees are considered a barrier by the smaller accredited requestors.
11. The rationale for the fees is clearly articulated in the document. From an MDG perspective, this information should be published publicly for transparency purposes.
12. In addition, any changes to fees should be communicated in advance for transparency so that data requestors know any fee changes ahead of time.