



Ngā Tohu Ārahi

Data Handling Guidelines

June 2025

apicentre
paymentsnz

Ihirangi Contents

Ngā whakawhetai Acknowledgements	2
Te Mihi	3
Kupu whakataki Introduction	4
Whakamāramatanga kupu Definitions of terms and concepts	6
Kohinga raraunga Data collection	8
Whakauru me te tiritiri Access and sharing	10
Whakamahinga raraunga Data usage	11
Ārai raraunga Data protection	13
Pūpuri me te whakamoe raraunga Data retention and disposal	15
Kounga me te tūtika o te pūnaha Data quality and system integrity	16

This document is produced by Payments NZ Limited (Payments NZ) and must not be copied, reproduced, or distributed, in whole or in part, without the consent of Payments NZ.

Payments NZ has relied on publicly available information and information provided to it by third parties in the production of this document. While Payments NZ has made every effort to ensure that the information contained in the document is accurate, it takes no responsibility for any errors or omissions in relation to the information contained in this document and Payments NZ will not be liable for any loss sustained in reliance on the information in this document. If you wish to rely on such information, you should obtain your own independent advice. © June 2025 Payments NZ Limited. All rights reserved.

Ngā whakawhetai

Acknowledgements

We warmly acknowledge the mana and leadership of Te Kāhui Raraunga, who created the Māori Data Governance Model on which Ngā Tohu Ārahi, the API Centre Data Handling Guidelines, are based. We are so thankful to our data science partners, Nicholson Consulting, who put us and kept us on track throughout our journey. We are grateful to our cultural advisors, Riki Consulting, for their help with tikanga, reo and moral support.

Finally, but not least, we thank everyone connected with the API Centre who contributed to Ngā Tohu Ārahi. Too many to name, but our gratitude is no less sincere.

Ehara taku toa i te toa takitahi, engari he toa takitini. Success is not the work of an individual but that of many.



Nicholson Consulting Group

Nicholson Consulting partner with public and private sector clients, iwi, NGOs, and philanthropic organisations.

Their expertise spans data science, research, evaluation, and Māori data.

Through their mahi, and as a business, their vision is to create a more equitable Aotearoa.



Te Mihi

E ngā mana, e ngā reo, e ngā karangatanga maha o te motu, tēnā koutou katoa. E mihi ana ki a rātou kua rūpeke atu ki tua o te ārai, ki te pō nui, ki te pō roa. Haere, haere, haere atu rā.

E rere ana ngā whakaaro ki a koutou ngā mana whenua o tēnā rohe, o tēnā rohe puta noa i Aotearoa. Ki ngā maunga whakahī, ngā awa e rere ana, ngā papa kāinga e manaaki ana i a tātou, he mihi kau.

Ko tātou e takahi tonu nei i te mata o te whenua, e whakanui nei i ngā kaupapa whakaū tikanga tiaki raraunga, tēnā tātou katoa.

He taonga te raraunga, he tapu te whakapapa, ā, ko tā tātou mahi, he whakatō i ngā tikanga tika kia noho haumaru, kia noho tika ēnei taonga mā ngā uri whakaheke.

Kia ū tātou ki te tika me te pono kia manaaki tonu ai, kia tiaki tonu ai i ngā raraunga o ngā iwi o Aotearoa.

Tūwhitia te hopo, mairangatia te angitu!

We are grateful to the leaders, community voices and those who paved the way for our achievements today.

We acknowledge the mana whenua of Aotearoa, and the mountains, rivers and ancestral lands that sustain us.

We are grateful to those on the journey to bring best practice to data stewardship.

Data is a treasure. Whakapapa is sacred. We are responsible for protecting these treasures for future generations.

We remain resolute, upholding integrity, truth and care.

Our goal is that people retain authority over their data. Releasing fear, we elevate success!

Kupu whakataki

Introduction

Purpose

The Payments NZ API Centre (API Centre) is on a journey to recognise and uphold Māori data sovereignty (MDS) and Māori data governance (MDG) across its mahi, as it models more responsible ways of caring for data in the Aotearoa New Zealand payments ecosystem. Ngā Tohu Ārahi uses MDS principles and MDG practices to support the management of customer data in a manner which upholds MDG practices.

In Te Ao Māori, data is a treasure that organisations have guardianship over, not to be treated as a commodity. Therefore, the primary aim is to ensure all customer data is safeguarded and managed ethically, in line with the aspirations of the communities from whom it originates.

While MDG and MDS are grounded in Te Ao Māori and support organisations in upholding practices which protect Māori rights and interests in their data, it can also be used as a universal framework and applied more broadly to all types of data to offer a more inclusive and ethical approach to data management.

Ngā Tohu Ārahi address 6 key areas of data handling:

- Data collection
- Data protection
- Access and sharing
- Data usage
- Data retention and disposal
- Data quality and system integrity

Ngā Tohu Ārahi are non-binding and recognise that API Standards Users may have internal data handling requirements that differ from this document.

However, given that many entities within the payments ecosystem are committed to honouring Te Tiriti o Waitangi and have developed Te Ao Māori strategies, following these guidelines can help achieve their goals in this space.

Scope

These guidelines are informed by the [Māori Data Governance \(MDG\) Model](#), which was published by Te Kāhui Raraunga in May 2023. This model contains eight different pou (pillars) that can be used to guide safe and responsible data handling practices.

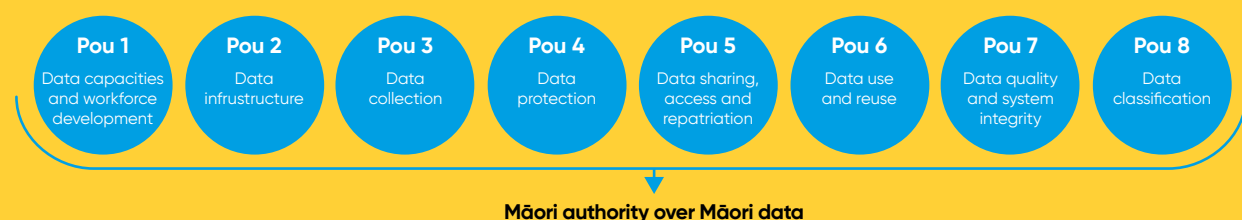
Each section of this document is split into six key areas of data handling, and are associated with a specific MDG pou:

1. Data collection – Pou 3
2. Access and sharing – Pou 5
3. Data usage – Pou 6
4. Data protection – Pou 4
5. Data retention and disposal – Pou 5
6. Data quality and system integrity – Pou 7

Note that the following MDG pou are not covered in the guidelines. These pou may be added in further iterations of the document when broader conversations have been had within the payments ecosystem to understand their application.

- Pou 1: Data capacities and workforce development
- Pou 2: Data infrastructure
- Pou 8: Data classification

The Māori Data Governance (MDG) Model¹



¹ Source: Kukutai, T., Campbell-Kamariera, K., Mead, A., Mikaere, K., Moses, C., Whitehead, J. & Cormack, D. (2023). [Māori Data Governance Model](#). Te Kāhui Raraunga.

Structure

For each key area of data handling, the following information is covered:

- **Horopaki/Overview:** Outlines what the data handling aspect is and how it links to the relevant MDG pou.
- **Focus areas and principles of data handling:** Each aspect of data handling is split into more specific focus areas of data handling. For each focus area, key data handling principles are clearly defined and detailed to guide users in the effective implementation of these principles.
- **What this looks like in practice:** Each section ends with a set of bullet points describing what these principles look like when applied in practice. This further supports users by providing clear, actionable examples of how these guidelines could be implemented effectively.

Intended audience

Ngā Tohu Ārahi are intended for API Centre Standards Users. These guidelines aim to ensure that API Standards Users are aware of ethical data handling and compliance with broader regulatory requirements, especially concerning the protection of Māori data.



Whakamāramatanga kupu

Definitions of terms and concepts

Several Māori data related terms and concepts are referenced throughout this document. Their definitions are provided below to clarify their application within the guidelines.

MDG and MDS

As defined in the [Māori Data Governance Model report](#) developed by Te Kāhui Raraunga, **Māori data sovereignty** (MDS) is “the inherent rights and interests that Māori have in relation to the collection, ownership and application of Māori data” (p. xi). On the other hand, **Māori data governance** (MDG) is “the principles, structures, accountability mechanisms, legal instruments and policies through which Māori exercise control over Māori data” (p. xi). Implementing MDG practices upholds the rights and interests of Māori, which are represented by the MDS principles from Te Kāhui Raraunga (defined in the below section).

Though MDG and MDS primarily relate in the management of Māori data, they also provide best data practices that are universally beneficial to all types of data and ultimately to all peoples of Aotearoa. These practices have been woven into these guidelines to support ethical data management practices.

MDS principles

Developed by Te Kāhui Raraunga, the Māori Data Sovereignty Network, the [MDS principles](#) are a set of six principles that can support organisations to protect the rights and interests Māori have in relation to their data. The application of the MDS principles have been highlighted across this document to help users of these guidelines understand how they have been upheld.

At a high level, these six principles cover:

1. **Rangatiratanga (Authority)** – relates to Māori having the inherent right to control their data and

ecosystems. This data interacts to ensure decisions around storage, access and use enable self-determination and governance.

2. **Whakapapa (Relationships)** – relates to the whakapapa (or lineage) of data, which requires collecting appropriate metadata on its origins and disaggregating Māori data to meet Māori needs.
3. **Whanaungatanga (Obligations)** – relates to balancing the rights of individuals, groups, and communities, with those managing Māori data being accountable to the people from whom the data originates.
4. **Kotahitanga (Collective benefit)** – relates to ensuring data systems benefit Māori individuals and collectives, and supporting connections with other indigenous peoples to share knowledge.
5. **Manaakitanga (Reciprocity)** – relates to respectful and ethical data collection and use, which requires consent and governance to avoid harmful or stigmatising analysis.
6. **Kaitiakitanga (Guardianship)** – relates to Māori informing decisions on the guardianship of their data, and ensuring ethical storage and sharing is guided by tikanga Māori.

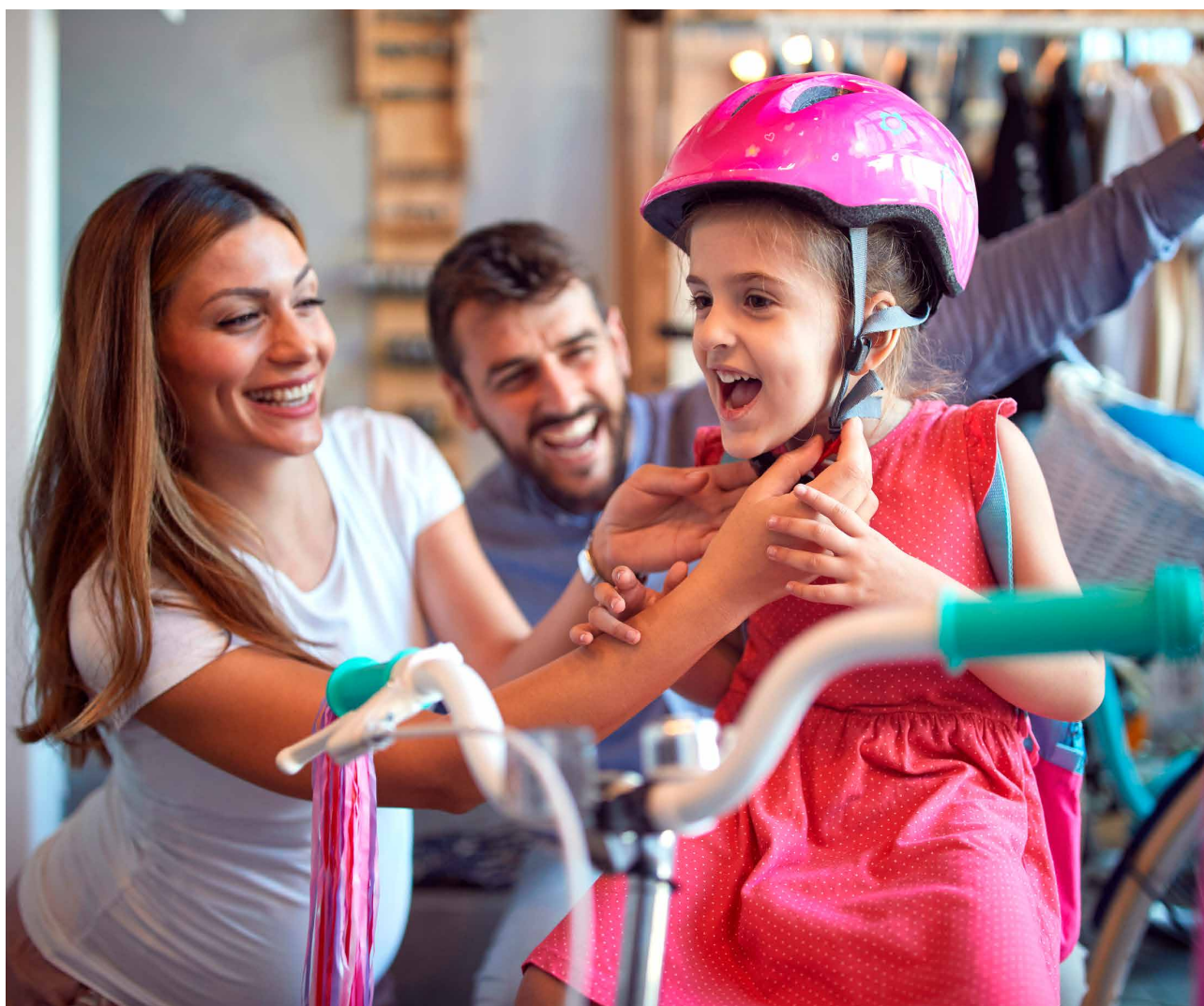
Ngā Tikanga Paihere

[Ngā Tikanga Paihere](#) is a framework that uses 10 tikanga Māori (Te Ao Māori concepts) to ensure data is used in a safe, responsible and appropriate manner. This framework can be applied to guide safe and ethical data use in various organisational contexts.

Some of the tikanga have been used in Ngā Tohu Ārahi to describe traditional data concepts in a way that is grounded in Te Ao Māori. These terms (as defined in Ngā Tikanga Paihere²) are provided below:

- **Tapu** refers to data that is considered sacred or restricted, requiring special protection due to its cultural or spiritual significance. Access to tapu data must be carefully controlled to respect its sensitivity.
- **Noa** represents data that is unrestricted and free to be shared or accessed without special conditions. It contrasts with tapu, allowing more open use and distribution.

- **Mauri** is the life force or vitality within data, ensuring its integrity and purpose. It reflects the idea that data has a living essence that must be preserved and respected throughout its lifecycle, from collection to use.
- **Mana** refers to the authority and respect that data holds, especially when it relates to Māori people or culture. It highlights the need to treat data with care, ensuring it is used in a way that honours the people it comes from. Mana can also mean having control over how Māori data is collected, managed, and shared, protecting the rights and dignity of Māori communities.



² Note that the definitions of the tikanga provided in Ngā Tikanga Paihere refer to Māori data, however in this document these tikanga have been applied more broadly to all types of data.

Kohinga raraunga

Data collection

Horopaki | Overview

As outlined by MDG Pou 3 (Data collection) of the MDG model, it is important to assess what data is collected and the ways in which that data is collected to ensure it is relevant, necessary and gathered in a manner that aligns with manaakitanga – i.e., with care and respect to the customer – and upholds the mana and mauri of their data. This pou emphasises the importance of ensuring that collection practices uphold the principles of informed consent (which are also covered within the United Nations Declaration of the Rights of Indigenous Peoples (UNDRIP)), cultural relevance, and respect for the whakapapa (lineage) of data, all of which are important elements of maintaining the mauri and mana of the data collected.

Safe data collection

Ethical data collection: Ensure data collection practices prioritise transparency and informed consent to avoid the exploitation of customers.

Data collection should be conducted with respect to customers and their unique contexts, particularly when they may be in vulnerable situations. Data collection purposes should be clearly communicated to the customer, including what data is being collected and what is being used for (see the [Data usage section](#) for more guidance on this). Providing this additional support can be especially important in the payments ecosystem, as customers may have their own financial contexts that could impact their ability to understand the implications of sharing their data or granting the ability to make payments from their bank accounts. This reflects the MDS principle of manaakitanga through the prioritisation of customer wellbeing and integrity through a more caring data collection approach.

In addition, it is worth noting that there are proposed changes to the Privacy Act 2020 to clarify certain obligations for agencies collecting personal information. It emphasises the need for transparency in communicating the purpose and intended recipients

of the information and their contact information. Considering these proposed changes is important, as they help ensure that personal data is handled with transparency and accountability, protecting individuals' privacy while allowing organisations to use information responsibly.

Data minimisation: Collect only the necessary data required to complete a process or task.

When customer data is to be collected, it is essential that there is a clearly defined purpose for its collection that benefits the customer – e.g., it is essential to providing or improving services that the customer has agreed to receiving. From a data management perspective, this can reduce the risk of handling excessive or irrelevant information. If new data needs to be collected, a practical assessment should be undertaken to determine whether data that has already been collected can be used again for this new purpose (with customer consent), which can further minimise the amount of data collected and stored about a customer. This is relevant to the MDS principle of manaakitanga as it prioritises the collection of data that provides benefit to those who the data is being collected from.

If data has been collected and stored but has no further use, customers should be given an opportunity to either dispose or have the data returned to them – see the [Data retention and disposal section](#) for further guidance.

What does this look like in practice?

- Provide clear and accessible information about the data collection process, including the purpose and use of the data, before customers provide their information. Additional support mechanisms, such as dedicated staff support or resources, could be established to support customers through this process.
- Provide mechanisms for the customer to see what data has been collected through the APIs and what it has been used for to promote transparency. It is important that the whakapapa of this data is documented from its origin (i.e., the data lineage)

to its use(s) by the third party and/or other entities, to ensure there is transparency around its entire lifecycle.

- Before a new data use purpose is established, determine the minimal amount of customer data that would be required to fulfil this purpose. Where possible and in accordance with customer consent, use data that has already been collected to minimise the amount of new data collected.
- Periodically reassess the purpose for which data is collected. If the original purpose has been served or is no longer relevant, the data should be presented back to the customer to determine how it should be dealt with.



Whakauru me te tiritiri

Access and sharing

Horopaki | Overview

MDG Pou 5: Data access, sharing and repatriation. Managing access, sharing, and disposal of data is crucial for protecting privacy, ensuring security, and complying with legal regulations. It helps maintain data accuracy, confidentiality, and ethical standards, while also reducing risks related to data breaches or misuse. Proper data management enhances efficiency, mitigates reputational risks, and demonstrates a commitment to safeguarding sensitive information. Māori perspectives on data access, sharing, and disposal emphasise making data accessible and shared with communities. When the data is no longer needed, discussions and/or activities should focus on returning it to the communities from which it originated (see the [Data retention and disposal section](#) for further details).

Access to customer data

Appropriate access: Manage access to customer data using the appropriate access controls that consider using concepts of tapu and noa to determine access levels.

Establishing appropriate access controls can bring greater control over what data individuals or collectives can access within an organisation, which has strong links to the MDS principles rangatiratanga and kaitiakitanga. The level of information that is accessed may be determined by specific roles and rules. Defining access levels may be informed by the tapu and noa concepts – e.g., data that is sensitive in nature (such as PII data) would require higher security measures (e.g., multi-factor authentication), whereas noa data (such as customer support resources or API documentation) may be less restricted or require strict confidentiality.

What does this look like in practice?

Work with customers to understand if there are other types of tapu information that should have restricted access and what type of access control model would be required to implement such access.

If working in a development or a test environment ensure that there is no access to tapu information. Instead use noa forms of data (such as synthetic data).



Whakamahinga raraunga

Data usage

Horopaki | Overview

MDG Pou 6: Data Use and Re-Use. Empowering customers to have control over their data involves ensuring their data is used (and potentially re-used) in a manner that upholds their rights and interests in relation to their data. Customer consent plays a key role in ensuring this is upheld; when customers provide their data, it should only be used according to the usage purposes agreed to by the customer, and any additional usage requires additional consultation with the customer to obtain their consent again. All instances of data use should be responsible and strictly related to the use of providing services that customers have explicitly agreed to.

Using customer data

Informed consent: Obtaining informed customer consent should empower customers to maintain control over how their data is used (in alignment with the MDS principle of Rangatiratanga).

Consent processes should go beyond regulatory compliance, respecting cultural protocols such as manaakitanga and upholding the mana (authority) of individuals over their own data. When obtaining customer consent, it is important that:

- Information related to the specific use of their data is clearly communicated to the customer;
- The use of vague language³ is not used to explain data usage (e.g., implying the potential for additional purposes i.e., secondary use);
- Customers are given the option to reject data use; and
- Consent is an ongoing process. Customers have the ability to view the details of their consent and revoke it at any given time, even after consent is obtained.

In the context of enduring consent, it is critical to strike a balance between convenience and respect for user autonomy, ensuring that users are neither

overwhelmed with constant consent requests nor disengaged through passive, unchecked permissions.

Use restrictions: Data must only be used for the purposes defined at the point of collection, and with customer consent.

Customer data should strictly be used for purposes that are relevant to the services they have signed up and agreed to. For instance, API logs and transaction data should be utilised solely for operational purposes or analytical improvements that are directly related to the API's function, which in turn support customers to use services offered by third party apps. Any deviation from the original use purposes communicated to the customer requires their explicit authorisation, and should align with relevant privacy laws and organisational policies (see the "Secondary use" principle below). This enables customers to have greater control over how their data is used, which has strong alignment with the MDS principle of rangatiratanga.

Ensuring appropriate use: Customer data should be used in a safe and responsible manner, with respect to the rights and interests of those who the data belongs to.

In addition to the guidance provided for the above principle, safe and responsible data use should also include ensuring customer data is not used in a manner than harms them in any way, which relates to the manaakitanga MDS principle. This means that data should not be used in a way that:

- Perpetuates biases or discriminates against customers;
- Exposes customer data that may be tapu (sensitive) in nature (see the [Data protection section](#) for guidance on this point); and
- Inhibits customers to have control and oversight on how their data is being used.

³ The GDPR website provides guidance on how to avoid the use of vague language in privacy notices which may be helpful to reference.

This helps to reinforce customer trust and confidence in organisations that hold and use their data, and can help to mitigate the potential for harmful or manipulative use of customer data.

Secondary use: Any secondary use of data for additional purposes must receive explicit consent from the customer

Secondary data use relates to uses that fall outside the original or primary use purpose, such as for research or marketing purposes, or for use by third parties. If customer data is to be used for these additional purposes, customer consent should be obtained prior to secondary use. If customer data is shared with a third party to fulfil services on behalf of permitted users, the only purpose of the data use should be to fulfil the customer's original service request. Clear agreements that outline the terms of data use, security measures, and compliance requirements should be established.

What does this look like in practice?

- When collecting customer data, ensure that in-app messaging related to consent is clear and explicit, and explains in plain language what data is being collected and how it will be used.
 - If a customer provides enduring consent for recurring payments, ensure that they are provided a detailed summary of the consent terms, including the frequency, the types of payments that will be made, the limitations (such as dollar amount) and information on how to review or withdraw their consent if desired. Changes to consent settings should be documented, and the customer should be informed about the update.
 - Account information, which is enduring by default, should follow a similar practice to the recurring payments.
 - Creating functionality within the user experience to view a summary of what a customer has consented to and the type of consent can help provide transparency on what data customers have consented to being collected and used.
 - 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.
 - Any additional purposes for using the data, even if it has already been collected via APIs, must be approved by the customer before proceeding.
- Separate consent should be obtained for additional purposes for using the data that is not specifically related to the service being provided to the customer (e.g., marketing or research purposes), and is compliant with relevant regulations.
 - Sharing data with other users such as third parties should be restricted only to provide services on behalf of the permitted users, i.e., consent can be given to third parties that enables permitted users (through the third party) to access the data/services. Customers must be appropriately informed about the use and purpose of sharing with a third party, and must provide consent before it is accessed, stored, shared and used by the permitted user.
 - Consents could be surfaced within the user experience and be searchable within the apps to make it easier for customers to discover and review their consents.

Ārai raraunga

Data protection

Horopaki | Overview

MDG Pou 4: Data protection. The MDG model looks at data protection from the lens of the privacy and security measures (such as encryption and multi-factor authorisation) that can be put in place to safeguard customer data, but it also touches on the jurisdictional challenges that arise if that data is stored offshore in the cloud. Depending on the sensitivity of the data, different protection measures may need to be applied – e.g., data that is more tapu in nature will have a higher level of protection, as opposed to data that may be more noa. Additionally, a unique aspect of Pou 4 is the importance of acknowledging collective privacy considerations to respect the privacy of all individuals represented within it. Overall, these practices not only enable technical safeguards to be put in place, but they also use culturally aligned practices that uphold the mauri and mana of data and the people who it belongs to.

Privacy

Anonymisation: Anonymisation should be approached with sensitivity to Māori cultural values and the broader implications of data handling. The Māori concepts of tapu and noa should be used to determine appropriate security levels for different data types

The MDS principle of manaakitanga emphasises the need to respect the dignity and privacy of Māori communities. While anonymising data in digital systems reduces risks related to personally identifiable information (PII), Māori views on privacy extend beyond standard data protection measures. These perspectives are closely linked to the concepts of mana, tapu, and whakapapa. Data linked to whakapapa or personal identity requires greater care as a taonga and should remain restricted, while aggregated deidentified data could be more accessible.

Compliance: Organisations should ensure their data practices adhere to both legal data protection requirements and MDS principles.

The MDS principle of whanaungatanga highlights the need to balance individual and collective rights within the community. Therefore, privacy protocols must consider both local laws, such as the Privacy Act 2020, and international standards. However, there should also be respect for tikanga Māori. This entails engaging with customers (which will also include whānau, Māori businesses and hapū) about how their data is protected stored, accessed, and used, ensuring that policies align with Māori values of autonomy and consent.

Security

Securing tapu information: Information such as whakapapa (biometrics in this context) should apply both standard security procedures as well as cultural procedures.

Multi-factor and strong customer authentication have increased the capture of data that represents a person's whakapapa such as their voice, fingerprints or face (which may include tāmoko or moko kauae whakapapa markings). Many technology devices use this type of information and API Providers are likely to use this type of information to approve consent. At the same time, there has been an increase in identity theft, which reinforces the need to protect whakapapa information. Tapu data may have additional security elements from a cultural perspective.

Jurisdiction

Understand jurisdictional implications for storage: Ensure data storage solutions enable customers to maintain control of their data, and are not at risk for unauthorised access, disclosure or use.

While local storage options are preferable from a MDG perspective, these options may not be realistic or enable full control over the data. The MDS principle of rangatiratanga covers jurisdiction and aspiring to having data stored in Aotearoa where possible so that there is greater control and to protect the wairua of the data. However, the USA CLOUD Act means that US-based technology companies can be forced to provide data stored on their servers, even when the data is stored in Aotearoa, diminishing part of the control element. All data storage solutions should be assessed to determine whether they offer protection against overseas jurisdictional claims, are compliant with relevant legal requirements, and uphold the MDS principle of rangatiratanga, which supports customers having control and authority of their data. If data is stored offshore, customers should be made aware and understand the implications of this to make an informed decision about whether they agree to sharing their data.

What does this look like in practice?

Privacy

- Collaborate with key stakeholders to identify data that is considered more tapu, and determine whether this should be stored within Aotearoa and subject to Aotearoa privacy law or if there are offshore storage options that still enable control over the data.
 - Ensure that data anonymisation methods are effective enough to prevent the identification of individuals, whānau (through joint accounts) or collectives such as businesses.
 - When data is retrieved via the APIs and stored then this data should be protected through either randomising, truncation, tokenising or encryption to make the data inaccessible.
- Recognise that certain financial data may be linked to significant cultural practices or events, such as koha (gifts) or pūtea (funding). When storing tapu data consider additional data protection.
 - Data protection mechanisms must ensure that anonymised data cannot be de-anonymised or traced back to identify individuals.

Security measures

- Use multi-factor authentication and Strong Customer Authentication. Before determining the factors of authentication ask if it is necessary to collect whakapapa information in the form of biometrics or whether other factors of authentication can be used (security keys, pin, password etc.).
- Tapu biometric data should be stored separately, which may be through either logical or physical separation.

Jurisdiction

- Present key information to customers relating to privacy notices and legislation such as the CLOUD Act and ask them to balance this in consideration with the functionality that services residing in a different jurisdiction provide so that they can determine whether they want to use these services.
- Utilise data residency services to ensure that data is processed within a specific geographic boundary.
- When using data residency services state whether these services ensure all backups of data remain resident.

Pūpuri me te whakamoe raraunga

Data retention and disposal

Horopaki | Overview

MDG Pou 5: Data access, sharing and repatriation outlines the principles and practices surrounding the retention and disposal of customer data, emphasising the importance of meeting cultural values as well as legal requirements. It reinforces the concept of kaitiakitanga (guardianship) by advocating for respectful and responsible management of data throughout its lifecycle. Key principles include ensuring that customers are involved in decisions relating to retention and disposal of their data, consulting with Māori stakeholders for culturally significant data, and adhering to tikanga during the secure disposal process. Documentation plays a critical role in ensuring transparency and accountability, capturing essential details about data management practices. Overall, this section highlights a commitment to upholding MDS and cultural integrity in all data retention and disposal activities.

Customer Involvement

Customer involvement in retention and disposal decisions: The customer should be engaged with when it comes to decisions relating to retention and disposal of data.

Retaining customer data should comply with legal obligations and MDS principles. Beyond standard requirements, such as keeping financial records for seven years (or longer), organisations should empower customers to make decisions about what happens to their data when it comes to retention and disposal supporting the principle of kaitiakitanga (guardianship).

Disposal of data

Documentation: Documentation must ensure accountability and capture the reasons and methods for disposal, to align with cultural and legal standards.

Thorough documentation of the disposal process is essential for MDS principle of whanaungatanga

through accountability and adherence to MDS principles. This should include the reasons for disposal (e.g., legislation, offboarding policies etc.), methods used, and consultations where appropriate with Māori data custodians, ensuring that practices align with both cultural and legal standards while respecting the whakapapa and ongoing significance of the data.

What does this look like in practice?

Customer involvement

- **Informing early on:** Inform customers early about their opportunity to decide what happens to their data (as far as the law permits).
- **Contact details:** Use best efforts to contact people either through contact details that are less likely to change or through the app itself.
- **Conspicuous mechanism:** The mechanism for customers making decisions needs to be obvious within the user experience.

Disposal of data

- Include default processes for archiving (to meet legal requirements) or offboarding that will be used if there is no response from the customer.
- **Deletion of data:** If you are utilising cloud providers, customers should be warned that whilst the bulk of the data can be deleted it is hard to confirm that all data has been deleted due to replication and multi-storage.
- **Removing access to data as a form of deletion:** A crypto shredding model could be applied to ensure that those users without keys can no longer access the data, which would help mitigate some of the issues with deleting data from cloud hosted services.
- **Comprehensive documentation:** Maintain thorough documentation of the disposal process, detailing the reasons for disposal, methods used, and whether this was a decision made by the customer or a default decision.
- Additionally, it is recommended to retain records of the disposal event itself, such as an audit of trail of disposal activities undertaken by people or systems, to ensure transparency and accountability.

Kounga me te tūtikao te pūnaha

Data quality and system integrity

Horopaki | Overview

MDG Pou 7: Data quality and system integrity, data quality and system integrity are critical for delivering more accurate outcomes and enhancing customer satisfaction. Maintaining high standards in data and systems builds trust with customers. Ultimately, this supports long-term success by driving better outcomes and ensuring a seamless, reliable experience for customers. In some cases, there may be specific examples of what data quality and system integrity looks like in practice when handling Māori data. In Te Ao Māori, data is seen as having a mauri, a life force that must be maintained to preserve its integrity. Organisations handling data must ensure that it is accurate, used responsibly, and stored in ways that uphold its mana, preventing any misuse or misrepresentation.

Data Quality

Accuracy of words: Ensure correct spelling of words, particularly for names or words with diacritics.

Traditionally, older systems have used encoding formats like ASCII, which cannot display diacritics, instead of newer formats like UTF-8 that support diacritics. Safeguarding the mauri of data requires maintaining its integrity and quality throughout its lifecycle. For Māori words, this means ensuring accurate orthography, including the correct use of macrons (tohutō), which are vital for properly representing names and places. Failure to demonstrate the MDS principle of manaakitanga to these cultural markers could lead to misrepresentation and cultural disrespect. In a multicultural society, it is likely that there are other names or words that will require accents, so enabling the use of diacritics has benefits across the entire customer base.

Timeliness: Systems should be in place to support prompt payments.

Research has identified that the [top customer pain point in the payments space is late payments](#) which has impacted both cashflows and relationships. The MDS principle of whanaungatanga speaks to accountabilities that organisations have to ensure that data is managed appropriately and there is accountability to the individuals and communities from whom the data is derived. In a payments context, this could speak to accountabilities that payers have to payees to ensure timeliness of payments and what Standards Users can do to support payers to make more timely payments.

System integrity

Audit logs: Systems should be able to easily surface audit trails that include the user, the timestamp and the changes.

Audit trails should be maintained to preserve the whakapapa history and enable timely identification of any unauthorised access or data breaches. In addition, research identified one of the top customer pain points is challenging payment issues. Having the lineage of system changes can help track down issues with payments. Having audit trails to describe the lineage of consent is also of importance when Third Parties or Permitted Users may access data.

Data lineage: Solutions should implement mechanisms that allow you to track the whakapapa lineage of data.

Lineage of data is another focus area. Third Parties may change data, which impacts the mauri of the data and can make it difficult to enact kaitiaki responsibilities to understand the changes that have been made to the data.

Monitoring: Establish regular monitoring of data handling practices to ensure compliance with ethical data handling standards.

Monitoring is an important component of measuring system integrity. Monitoring may include measuring the performance API Providers and Third Parties and Permitted Users.

Review: Ensure that there are regular reviews in place.

By adopting these practices, API Standards Users can ensure that data policies, processes, procedures and guidance evolve with technological and regulatory changes while fostering collaboration and shared learning among all parties involved.

What does this look like in practice?

Data quality

- Supporting the UTF-8-character or UTF-16 encoding to ensure the preservation diacritics within words across systems.
- Adopting the ISO20022 standard, which supports UTF-8 XML. Note that the API Centre standards use JSON with full UTF-8-character support but it is important that Standards Users do not limit character encoding within apps.

- Encourage the Bank for International Settlements to review their standards for international payments, which currently support an ASCII Latin-1 character set.
- Providing a mechanism for timely automatic payments underpinned by enduring consent.
- Apps may wish to inform users about pending payments or other tasks that impact workflow.

System integrity

- Audit trails could be exposed to help trace the whakapapa or lineage of changes that have occurred.
- Lineage should be tracked to identify which parties have accessed data and under which consent approval.
- The lineage should be tracked to identify which parties have accessed data and under which consent approval. A history of API/data requests or payments initiated using a consent could help track the lineage of payments.
- API Providers and third-party partners should opt in to self-assessing their progress against Ngā Tohu Ārahi.
- API Providers and third-party partners could share insights on adherence to Ngā Tohu Ārahi within the working groups.
- Ensure there is a review function in place to confirm that guidelines, standards, policies and procedures relating to data are continuously improved.





apicentre
paymentsnz

+64 4 890 6750

apicentre@paymentsnz.co.nz

www.apicentre.co.nz

