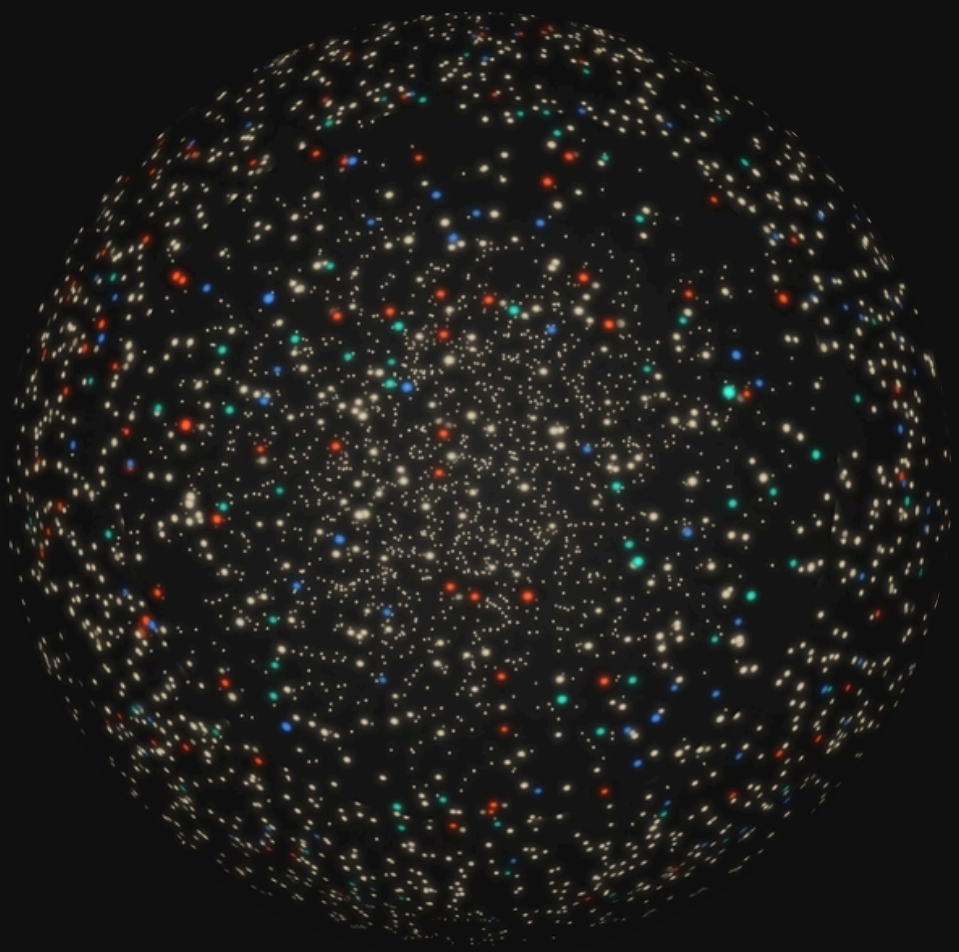
A DEEP DIVE INTO THE CUSTOMER AND PRODUCT DATA ACT



Hudson Gavin Martin
www.hgmlegal.com

Table of Contents

01 What's happening?

New Zealand's much-anticipated "consumer data right" legislation – the Customer and Product Data (CaPD) Act – was passed into law with full cross-party support on 29 March 2025.

The Act provides a framework for the easy and safe exchange of customer data and, importantly, allows customers to require designated data holders (like banks) to share information with accredited data requestors (like fintech companies).

It is intended to:

- Improve customers' access and control of their own data.
- Standardise how data is exchanged.
- Ensure those who request access to data are accredited as trustworthy.

The Act is high-level, and most of the detail of the CaPD regime is left to subsequent regulations and standards. MBIE released two discussion papers on potential sector designations under the CaPD regime – banking and electricity – in August 2024. Regulations relating to banking are expected to be finalised sometime in 2025 so that the banking part of the regime can be fully in force by the end of the year.

So, significant progress has been made towards a regulated "customer data right" and, while there is still much to be decided, we know enough to take a deep dive into what will be a new open data regime for New Zealand.

The legislation is significant, as it's rare that governments seek to participate this actively in the economy – to influence particular commercial outcomes, business models and ways of engaging with customers.

MBIE says that,

> *"the draft law will help innovators in our economy create new products and services and increase competition. This in turn will benefit customers by leading to reduced prices, improved product offerings, and greater productivity. The draft law also creates opportunity to support by-Māori, for-Māori data initiatives, business-to-business applications, and improved accessibility and inclusion."*

This is a sweeping, aspirational statement of intent – no pressure then!

MBIE highlights various possible applications and products for the CaPD regime: "price comparison applications", "carbon footprint calculators", "insights into household expenses", "streamlining the process of applying for a loan", "tailored advice and insights or product recommendations", and "business to business payments products, working capital lending products, and business operations products and services".

These examples scratch the surface of what's possible, but we expect fintechs and other innovators will have many more data-driven applications up their sleeves.

02 The TLDR

For those short on time, here are the highlights in quickly digestible form:

Core Principles

MBIE has summarised the core principles of the legislation as "Respect, Care and Trust". These broadly reflect the three key aspects of the regime – customer consent, data security standards, and accreditation of data recipients.

Access & Action

A fundamental pillar of the regime is that "action initiation" is in scope, not just data access. For open banking, this will enable customers to authorise payments directly from their accounts.

Existing Work

The Government has highlighted its desire to build on existing industry work – particularly the standards already developed by Payments NZ for the API Centre programme. The API Centre is expected to continue to be responsible for a wide range of open banking functions under the Act, including developing and hosting standards and providing best practice guidelines.

Tikanga Māori

MBIE says "the draft law could benefit significantly from looking to and learning from the principles and concepts of Māori Data Governance". This may create an opportunity to address obligations under te Tiriti o Waitangi and to provide for culturally-grounded data governance and regulation where appropriate, although the Act itself only provides for consultation.

Regulators

MBIE is the enforcement agency for CaPD, but MBIE and the Privacy Commissioner will have overlapping jurisdiction. The Commerce Commission has also recommended that it be the main payments regulator for open banking – regulation of pricing is still a key unresolved issue under the legislation.

Regulations Ahead

The Act provides a high-level framework for the CaPD regime, but most of the detail in key areas is left to subsequent regulations and standards. We've included a table at the end of our report.

Consent

Consent is at the heart of the regime. Almost everything that happens (including the initial data exchange and any subsequent transfers by data requestors) needs to happen with express and informed customer consent.

Accreditation

Recipients of CaPD data will need to be accredited. The Act entrenches high-level criteria for accreditation, including a "good character" test for directors and senior managers, adequate information protection and security measures, and evidence of likely compliance with the Act.

International Alignment

The Act was informed by the Australian Consumer Data Right legislation. MBIE has signalled that it is likely to aim for consistency with international standards in the development of any binding data exchange standards, and to enable the setting of accreditation criteria similar to those in Australia and the UK.

Other Players

Regulations will govern how consent and data access will be handled for joint account holders and "secondary users" (e.g. people with authority to act on behalf of companies). The concept of "outsourced providers" has been removed from the Act.

Open Banking First

The regime potentially covers the entire economy but will only be "switched on" for specific sectors and data types on a case-by-case basis. The banking sector will be the first designated and it's likely that the electricity sector will be the second.

Mandatory Regime

Consent is particularly important for CaPD because it's a mandatory regime – data holders have limited ability to decline a valid data request once customer consent is provided. A significant change to the Act following public consultation was the inclusion of a range of valid reasons to decline requests.

Two-Tier System?

In the areas of consent, security and accreditation (as well as the proposed enforcement and penalty regime) the CaPD regime imposes a significant extra layer of compliance on existing data sharing and privacy frameworks. This begs the question whether New Zealand is creating a two-tier system for data privacy, and brings the adequacy of the Privacy Act regime into focus.

No Reciprocity

The Act does not include a "reciprocity" regime – with the Government seemingly prioritising maximising uptake over the risks of an uneven playing field for data holders.

Enforcement

The Act includes an extensive enforcement and penalties regime, involving fines of $20,000-$50,000 for minor infringements through to $1 million-$5 million for intentional/reckless deception or fraud. Individuals may also be imprisoned.

B2B Included

A "customer" is widely defined to include any business or organisation (as well as consumers). This opens the door for B2B relationships and use cases.

Standards-based

Like similar overseas regimes, the Act provides for common data and security standards to be set by regulation (for example, technical standards for developing the APIs that will facilitate data exchange and action initiation).

Operational Complexity

The regime will involve significant operational complexity outside the core data exchange and accreditation standards – for example, handling different buckets of "CaPD" and "non-CaPD" data and requirements around complaints processes.

Intermediaries

The Act does not include a separate class of accreditation for "intermediaries" or data aggregators. They are required to be accredited themselves, and to ensure they have the consent of the underlying customer to pass data onto their data requestor clients.

What Next?

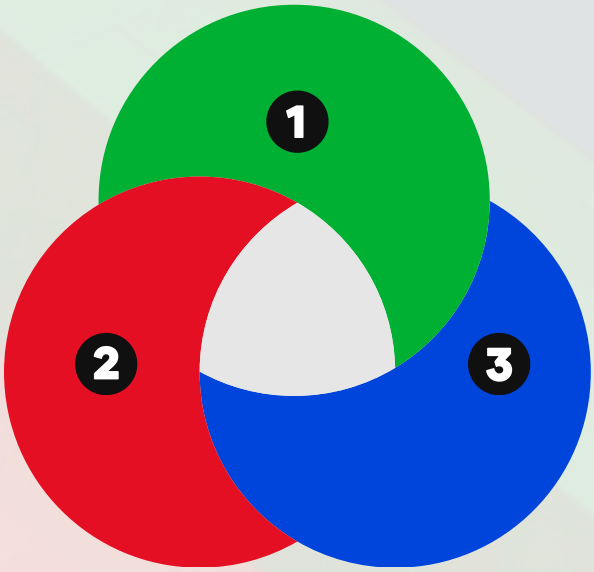
If proposed time frames are met, the open banking regime will commence on 1 December 2025 for ANZ, ASB, BNZ and Westpac, and from 1 June 2026 for Kiwibank. Timing for the electricity sector CaPD regime is still undecided.

03 Core principles

MBIE summarises the core principles of the legislation as **"Respect, Care and Trust"**. This provides a useful framework for interested parties to understand the Act and formulate their positions on key aspects.

RESPECT

Refers to putting customer consent at the heart of the regime. Almost everything happens with customer consent, which can be withdrawn at any time.



CARE

Relates to security and safeguarding of the exchange of data – and the standards the legislation will set in this regard.

TRUST

Refers to the accreditation regime for those who want to receive data under the regime, as well as the overlay of existing privacy law.

04 Key themes

There's a lot to digest in the Act and the various discussion documents MBIE has produced. Here are our views on some key themes to consider and follow as the legislation comes into effect.

We will keep this report updated to cover the introduction of regulations and standards as that process continues.

Tip of the iceberg

The Act provides a high-level framework for the CaPD regime, but most of the detail in key areas is left to subsequent regulations and standards. In this sense, the Act is the tip of a sizeable iceberg of detailed rules sitting underneath it.

Although work on all aspects can be done in parallel, the regulations can't be issued until the Act is passed, and the standards can't be issued until the regulations are in force. This means the regime will be rolled out in a "waterfall" approach.

With the benefit of cross-party support, the Act passed through its second and third readings in less than a month and was passed into law on 29 March 2025. While the Government has expressed the desire to progress the regulations and standards at pace (with a view to going live with open banking by the end of 2025) this process will need substantial industry participation to ensure the rules are fit for purpose.

Open banking up first

The regime potentially covers the entire economy but will only be "switched on" for specific sectors and data types through regulation on a case-by-case basis. The banking sector will be the first designated and this is a logical starting point.

"Open banking" regimes have generally been at the forefront of open data initiatives overseas, while in New Zealand we've had an industry-led open banking programme for the past 5 years – Payments NZ's API Centre. MBIE's banking sector discussion paper (**Open Banking Discussion Document**) notes that an open banking designation under the Act would "complement these efforts to accelerate adoption and ensure that open banking is delivered efficiently and effectively".

MBIE proposes that the open banking designation will initially cover the same banks as the API Centre Minimum Open Banking Implementation Plan, and the same basic categories of customer data and actions as the API Centre Standards. Designation is expected to commence for New Zealand's four largest banks (ANZ, ASB, BNZ and Westpac) on 1 December 2025, and for Kiwibank from 1 June 2026 in respect of payments. Kiwibank would be required to provide customer data from 1 December 2026. Other banks and deposit takers would be invited to opt in to the designation.

In a related move, in August 2024 the Commerce Commission granted Payments NZ authorisation to work with API providers and third parties to develop a new partnering framework relating to the provision of industry-led API services – a process that might otherwise breach competition law. The proposed partnering framework involves the joint development of:

- An accreditation scheme (including accreditation criteria) for third parties; and
- Default standard terms and conditions on which API providers would contract with third parties who meet the accreditation criteria.

There is obvious crossover here with the Act, which the Commerce Commission acknowledged in giving preliminary authorisation to the partnering framework for only 18 months, recognising "the anticipated timing of regulatory interventions that will likely deliver some of the same potential benefits".

The electricity sector will be the second designated industry, which tracks with the Australian approach of applying its CDR to the banking and energy sectors first. In something of a surprise, MBIE released its discussion document on potential designations for the electricity sector at the same time as the Open Banking Discussion Document in August 2024, indicating that progress to a CaPD right for these sectors may end up being almost simultaneous. MBIE has stated that the purpose of the electricity sector designation is to unlock access to product data, so that customers can more effectively compare electricity plans and switch between electricity providers.

Not just *consumers*

While it has colloquially been called the "Consumer Data Right", the Act deliberately steers away from references to consumers. A "customer" is widely defined to include any business or organisation (as well as consumers) acquiring (or seeking to acquire) services from data holders.

This opens the door for B2B relationships and use cases to be covered, and MBIE specifically acknowledges the potential benefits for businesses in areas like B2B payments, working capital lending, and business operations products.

For many corporates, the ability to access their own banking data in more secure and streamlined ways may prove very useful for internal administration. Note however that in the Open Banking Discussion Document, MBIE proposes that to begin with only requests by accredited requestors on behalf of customers will be designated under the Act. This means that customers won't initially be able to make a request for their banking data directly, without the involvement of an accredited requestor.

Action as well as Access

A fundamental pillar of the regime is that "action initiation" is in scope, not just data access. For banking, this will enable payments-related use cases (i.e. the ability for customers to consent to make payments directly from their bank accounts), which are driving a lot of the innovation in the UK but which Australia failed to include in its initial CDR regime. The Open Banking Discussion

Document proposes that to begin with the only designated action under the Act will be payment initiation from bank accounts (although MBIE notes that APIs could be developed for other actions, like making and cancelling automatic payments and direct debits, opening and closing accounts, and amending limits).

Payment initiation can unlock the benefits from other open banking use cases (such as personal financial management apps). It also opens the way for new payments products to be developed to facilitate "account to account" payment. This creates potential competition with existing payment methods like debit and credit cards and Buy Now Pay Later. However, users will have to consider whether the likely lower costs of individual payments outweigh the security and benefits provided by card schemes through charge-back protection and loyalty/points programmes. The Act does provide a mechanism for customers to seek redress if there are errors in action initiation (e.g. payment failures).

It also provides that contravention of certain storage and security requirements (e.g. failing to check an action is within the scope of the customer's authorisation or to verify the identity of the person making the request) will be considered a breach of the Privacy Act 2020 (Information Privacy Principle 5).

The Open Banking Discussion Document also proposes that data requestors will be liable (via regulations) to reimburse any unauthorised payments.

~~Consent~~ Authorisation is king

Consent is at the heart of the regime. Almost everything that happens (including the initial data exchange and any subsequent transfers by data requestors) needs to happen with express and informed customer consent.

Consistently with the Privacy Act (though confusingly in terms of common data privacy parlance) the Act refers to "authorisation" as opposed to consent.

The Act sets out broad requirements for how consent is obtained (e.g. clear information must be provided about the consent process, and it must be just as easy to withdraw consent as to give it) and leaves the detail to regulations.

In the Open Banking Discussion Document, MBIE provides some important information about what it proposes the regulations around "express and informed consent" should look like:

- Accredited requestors seeking authorisation to request customer data must specify the data or action requested, the goods and services that the data will be used to provide to the customer, any intended use of the data that is not necessary to provide the service, and a link to the accredited requestor's customer data policy.
- Customers should be required to opt-in to specific uses that are not necessary to provide the service (so customers are freely consenting to their data being used in other ways, "without simply accepting a bundled all-or-nothing consent").

- Ongoing authorisations will not automatically expire, but accredited requestors will be required to remind customers at least every 12 months of the scope and purpose of the authorisation and that consent can be withdrawn at any time
- If the accredited requestor is an “intermediary” (see below), authorisations must disclose the specific persons the accredited requestor will disclose the customer data to, and the purpose for which they will hold and use that data.
- Subsequent disclosure by the accredited intermediary to a different unaccredited person would require subsequent consent.
- Unaccredited persons receiving customer data will not be required to become accredited or be subject to any restrictions on their use and disclosure of that data, other than (for personal information) complying with the Privacy Act.
- Payment initiation consents will need to state the details of the payment being authorised, who can act on the authorisation, and the account that the funds will be paid to. API standards will be used to further define the requirements of the authorisation, such as the amount and payment frequency.
- Banks and accredited requestors will need to provide a “dashboard” of information about each active authorisation, that must be available to the customer through a website and mobile application at all reasonable times.
- Joint customers will be able to access information about joint accounts and authorise payments under the same conditions as they can under existing account operating authorities and bank terms and conditions, outside of open banking.

These are sensible requirements. However, it’s worth acknowledging that New Zealand’s existing privacy regime is not generally consent-based. Under the Privacy Act, personal information can usually be obtained, used and shared without express consent as long as the relevant agency provides clear information about what it’s doing, and what it’s doing is lawful.

So, this is a change of regulatory approach for the data and services covered by CaPD.

Consent is particularly crucial for CaPD because it’s a mandatory regime – data holders have limited ability to decline a valid data request if the customer has provided consent. Data holders can’t contract out of their obligations under the Act, and any data holder that purports to do so commits an offence under section 13(i) of the Fair Trading Act 1986 (i.e. makes a false or misleading representation concerning the existence, exclusion, or effect of any condition, warranty, guarantee, right, or remedy).

That said, a significant change to the Act following public consultation was the inclusion of a range of valid reasons for data holders to decline requests, including where the request is reasonably believed to be part of a cyber-attack, where a customer is known to have been subject to identity theft, or where the data holder reasonably believes that disclosure of the data would create a significant likelihood of serious financial harm to someone. Commercial realities are also now allowed for, with data holders being entitled to refuse data requests if the customer or accredited requestor owes a directly related debt to the data holder, or if the data holder reasonably believes that the accredited requestor has not fulfilled their requirements or performed their duties.

The customer care duty under the Act is now shared between data holders and accredited requestors, with an accredited requestor being prohibited from accepting an instruction or making a request under a customer's instruction if it believes that the authorisation or instruction was given under the threat of physical or mental harm. This change was made to place consequences and customer recourse on the party best positioned to prevent harm to the customer.

A new defence was also added at the Select Committee stage to protect data holders who become inadvertently exposed to liability by complying with their obligations under the Act (e.g. if a hacker uses an accredited requestor's stolen credentials to request customer data). It is a defence if the data holder proves they provided data in compliance or purported compliance with the Act, in good faith, and took reasonable precautions and exercised due diligence.

A standards-based approach to data security

Like similar overseas regimes, the Act provides for common data and security standards to be set by regulation (for example, technical standards for developing the APIs that will facilitate data exchange and action initiation).

Interested parties have the ability to contribute to this process through consultation.

Standards will relate to the exchange of data (i.e. the interfaces between APIs from a security, data format and structure perspective) and potentially the structure and design of the customer consent process. Importantly, the standards will not cover collection, use and storage of data by recipients, which will continue to be managed under the Privacy Act.

MBIE has highlighted its desire to build on existing industry work – particularly the standards already developed by Payments NZ for the API Centre programme – and states outright in the Open Banking Discussion Document that "[w]here standards have been developed through an industry process and meet expectations, our preferred approach would be to adopt those standards under the Bill". An important change to the Act made at the Select Committee stage was to include provisions enabling MBIE to approve one or more outside organisations to have a principal role in developing standards and providing supporting services, such as accrediting persons as accredited requestors, keeping the register, and providing or facilitating the provision of information. This is likely to have been included to enable the API Centre to perform this role, although no decision on this has been announced as yet.

So, while the Minister of Commerce and Consumer Affairs and MBIE will have an oversight role in the implementation of the Act and will carry out certain functions, the API Centre is expected to continue to be responsible for a wide range of functions in respect of open banking, including:

- Developing and hosting standards;
- Providing best practice guidelines;
- Providing a sandbox for current and prospective accredited requestors to test software;
- The general promotion of open banking; and
- Open banking delivery outside the Act, including accreditation and partnering frameworks for any premium APIs.

The API Centre may also deliver the register of data holders and accredited requestors, based on its existing register of participants.

This raises additional questions about whether the existing governance arrangements within, and fee funding for, the API Centre are fit for the purpose of delivering these outcomes for all participants in the regime. This formed part of the consultation under the Open Banking Discussion Document that closed in October 2024. Notably, the Act also now provides that levies collected from data holders and accredited requestors can be used to fund any approved standards body.

Key to the standard-setting process will be balancing the sometimes-competing interests of security and user experience.

For example, work needs to be done on the customer journey for authentication and consent, to ensure usage doesn't drop off due to clunky processes. Helpfully, a lot of thinking has already been done on this topic both overseas and in the API Centre programme, which we can expect MBIE to leverage (these Customer Experience Guidelines are an example).

Accreditation

Recipients of CaPD data will need to be accredited. Accreditation is a valuable badge, as a data holder generally can't refuse to provide data to (or initiate action for) an accredited requestor on behalf of a consenting customer.

The Act entrenches core, high-level criteria for accreditation:

That the directors and senior managers are of "good character".	That the organisation has "adequate security safeguards" in relation to the data they will receive.	That the organisation is capable of effectively complying with its obligations under the Act and there is no reason to believe they are likely to contravene them.

More detailed accreditation criteria can be prescribed by regulations.

MBIE also proposes that all accredited requestors be required to be a member of a financial services dispute resolution scheme, such as the Banking Ombudsman or the Insurance and Financial Services Ombudsman.

MBIE remains undecided on how prescriptive it should be in its approach to information security requirements on accredited requestors, setting out three options in the Open Banking Discussion Document for public feedback:

Option 1
The applicant meets Information Privacy Principle 5 under the Privacy Act (i.e. the status quo)

Option 2
The applicant meets a set of high-level principles (i.e. similar to the UK approach)

Option 3
A more prescriptive set of information security requirements along the lines of the Australian CDR rules, which might include third party certification against specific standards (e.g. ISO27001)

Given the security implications of permitting new data flows on this scale (not to mention a new way of making payments via bank accounts), we anticipate that relatively prescriptive security standards will be required.

A two-tier system?

The CaPD regime relies on existing laws and obligations relating to data wherever possible. Importantly, the Privacy Act will continue to apply to personal information in the same way, except where the Act says otherwise (for example, the Act clarifies that a request for customer data under the Act that involves personal information is not a request under Information Privacy Principle 6 of the Privacy Act).

However, in the areas of consent, security and accreditation (as well as the proposed enforcement and penalty regime) it's clear that the CaPD regime imposes a significant extra layer of compliance on top of existing data sharing and privacy frameworks.

This begs the question whether New Zealand is creating a two-tier system for data privacy and security.

It is not uncommon for different regimes to apply to different types of data and records. However, the Act will add another layer of operational complexity for agencies because they will need to have new and different policies and processes for retaining and using personal information that is also customer data under the CaPD regime. The enforcement regimes under the Act and Privacy Act may also overlap.

This brings the adequacy of the existing Privacy Act regime into focus, at a time when the Privacy Commissioner himself has lamented the lack of a civil penalty regime in the Privacy Act and noted that "having a full range of effective tools in the regulatory toolbox is increasingly essential for privacy regulators".

For its part, MBIE states that "further policy decisions that relate to privacy more broadly are more appropriately considered in any future review of the Privacy Act".

Some may question whether the Privacy Act in its current form provides a robust enough framework to manage the significant increase in data flows and usage across the economy which is likely to flow from the CaPD regime.

Operational complexity

The Act is deceptively simple. The devil will be in the detail and the operational execution.

While gearing up to comply with the core data exchange standards and accreditation requirements will be a significant exercise in itself, there are other operational complexities to consider.

Both data holders and requestors will need to be set up to deal with two "buckets" of data – CaPD and non-CaPD – and the separate requirements attaching to each. Participants in the electricity industry are also already governed by the Electricity Industry Participation Code 2010, which will intersect with the CaPD regime and may cause complexities for retailers, data holders and customers.

To address industry concerns about the complexity of the system (based on similar issues overseas) the Select Committee made a range of changes to the Act aimed at simplifying the CaPD regime – including removing various policy, reporting and record keeping obligations on data holders and requestors.

A significant change to the Act at the Select Committee stage was the exclusion of derived data requirements on accredited requestors. Derived data is not included within the scope of "customer data" in the Act and is therefore not subject to mandatory sharing. There are good policy reasons for this, as data holders will want to protect their rights in generated, enhanced or "value-added" data, which often involves capital investment and can have intellectual property rights attached.

However, the draft CaPD legislation had initially allowed for requirements or restrictions to be imposed on the use, modification or disclosure of derived data created by accredited requestors.

The rationale for regulating accredited requestors' derived data in this way was not clear, but the Open Banking Discussion Document suggested it stemmed from a concern about the downstream impacts of increasing data flows in the economy from a data security and consumer protection perspective (particularly as some intermediaries are "data aggregators"). The risk to the CaPD regime was that attempting to regulate derived data would create material barriers to entry and incentivise the use of non-regulated methods like screen scraping, which may be less safe and secure (this has been a well-publicised concern with the Consumer Data Right regime in Australia).

The Select Committee recognised this concern and recommended the exclusion of any reference to "derived data" in the Act, saying in its report that the derived data restrictions "could create legal and practical complexities and costs, and reduce the adoption of the proposed data sharing infrastructure".

To ensure the regime is workable, it will be important for the Government to continue to identify and resolve potential pain points before full implementation, as part of the regulation-making process.

Application of Tikanga Māori

MBIE has stated that some Māori data will be a taonga (treasure) and that the Act may be consistent with aspects of tikanga Māori.

MBIE also previously acknowledged that "the draft law could benefit significantly from looking to and learning from the principles and concepts of Māori Data Governance…because of the high value Māori place on care for and use of data". The Act itself doesn't expand on this idea, noting only that before making designation regulations and standards the Minister of Commerce and Consumer Affairs must consult one or more people who have expert knowledge of te ao Māori approaches to data, and must have regard to the interests of Māori customers.

There is an opportunity for New Zealand to do something unique in this area – to address obligations under te Tiriti o Waitangi and to provide for culturally-grounded data governance and regulation where appropriate. Te Pāti Māori gave its support to the Act specifically for that reason: to allow a deeper analysis of the issue and the opportunities that might flow from a CaPD right, including a Māori banking system.

We anticipate those involved in the ongoing work on models for Māori Data Governance will relish the opportunity to work with MBIE and the Minister to promote Māori approaches to data in the CaPD regime.

International alignment

One of the main requests from stakeholders in the lead-up to the release of the Act had been for the Government to learn from other jurisdictions with similar regimes – taking what has worked and discarding what hasn't.

MBIE followed through on this in its discussion documents, noting that the Act was informed by Australia's Consumer Data Right legislation, and making various comparisons to Australia and the UK in areas like expiry periods for ongoing consent (which were changed from 90 days to 12 months in Australia following consultation) and information security standards.

MBIE has signalled it is likely to aim for consistency with international standards in the development of any binding data exchange standards, and to enable the setting of accreditation criteria similar to those in Australia and the UK.

International alignment is important for uptake. There are obvious benefits in making it as straightforward as possible for overseas businesses already operating under similar regimes to enter the New Zealand market (and vice versa for our local innovators). We hope industry participants will take the lead in working with governments and peers in New Zealand and overseas to ensure appropriate interoperability.

No reciprocity

An interesting departure from the Australian regime can be seen in the approach to "reciprocity". In Australia, certain data recipients are required to share CDR data they hold or generate as though they were a data holder for the purposes of the regime. For example, an accredited non-bank lender may become a reciprocal data holder in respect of data they generate for their personal loan products.

This addresses the structural concern that open data regimes can create an uneven playing field, where certain industry participants (e.g. banks) are required to make data available to anyone – including major corporate players and tech giants – who have no reciprocal obligation to make their own data available.

On the flip side, Australia has found that reciprocity requirements can act as a deterrent for entities seeking accreditation to participate in the CDR regime. New Zealand has prioritised maximising uptake over the risks of an "uneven playing field" – as the Act does not include any reciprocity regime.

MBIE left the door slightly ajar on this in the CaPD Discussion Document, saying that a designation process could be used to bring this data into the regime later. However, the Open Banking Discussion Document doesn't pursue the idea and, as it would be complex to implement the designation of specific data types in this way, we think it's unlikely to be on the Government's agenda in the near future.

Intermediaries

The Act doesn't propose a separate class of accreditation for "intermediaries" (entities which collect designated customer data on behalf of other entities) as is the case in Australia.

Sometimes called "data aggregators", intermediaries play an important role in the open data ecosystem, making it easy for requestors to access data and providing value-added services on top of the raw data feeds prescribed by regulatory standards. Providers like Envestnet Yodlee, Plaid and TrueLayer provide these services internationally, while New Zealand has its own local players, such as Akahu.

The Act requires intermediaries to be accredited themselves, and then to ensure they have the consent of the underlying customer to pass data onto their data requestor clients. There are three parties in this chain – the underlying customer, the data requestor and the intermediary, and as we've already discussed, there are additional requirements for express and informed consent when intermediaries are making the request.

Intermediaries and their data requestor clients will need to work together to ensure that authorisations provided by end customers cover the data services provided by the intermediary as well as the direct data requestor. They'll also need to think about what relationship (and contractual terms) each of them has with the end customer for this purpose.

We think the Act's approach to accreditation of intermediaries (and non-accreditation of their downstream users) makes sense in terms of the workability of the regime overall. However, it will be important for regulations and standards to acknowledge and address the potential for intermediaries to be a "single point of failure" in the system, particularly if uptake of their services is strong and this leads to a lack of accreditation of other data users across the designated sectors.

Joint account holders, secondary users and outsourced service providers

The Act provides for regulations to be made governing how consent and data access will be handled for joint account holders and "secondary users" (e.g. people with authority to act on behalf of companies).

The concept of "outsourced providers" – those who exercise obligations or powers under the legislation on behalf of data holders or requestors – has been removed from the Act. Instead, any issues around outsourcing under the Act will be addressed by general legal principles (i.e. the data holder/requestor will be liable for any actions by an outsourced provider on their behalf and will need to address any downstream risk in relevant contracts).

Commerce Commission interventions

An interesting parallel regulatory process for open banking is ongoing, with the Commerce Commission writing to the Commerce and Consumer Affairs Minister in August 2024 recommending designation of the interbank payment network under the Retail Payment System Act 2022.

If granted, the designation would effectively set up the Commerce Commission as the main payments regulator for open banking, allowing it to make rules and standards in areas such as participant conduct, governance, pricing, and driving adoption. In its recommendation letter, the Commission noted that it has a wider remit as a competition and payments regulator than MBIE under the Act and "will be able to address barriers to open banking within the payment system… that cannot all be resolved under the CDR".

Along with its authorisation of the Payments NZ partnering framework, these interventions show a clear intent from the Commission to drive open banking as a key pillar in increasing competition and innovation in the banking and payments sector.

Enforcement powers and penalties

The Act includes an extensive offences and penalties regime ranging from infringement offences for procedural contraventions (e.g. failure to comply with record-keeping requirements) to criminal offences with significant penalties for particularly egregious or harmful conduct (e.g. knowingly making a request for regulated data services they are not permitted to make). Pecuniary penalties range from $20,000 to $5 million. Individuals may also be imprisoned.

Contrast that with the Privacy Act, where the highest penalty for a criminal offence is a fine up to $10,000 only.

The Act also imposes requirements in relation to customer complaints that are likely to require data holders and requestors to establish complaints handling processes – and therefore add to compliance costs.

MBIE proposes that all accredited requestors be required to be a member of a financial services dispute resolution scheme, while any person can apply to a court or the Disputes Tribunal for compensation for loss or damage if a data holder or accredited requestor has breached their obligations under the Act. Any compensatory orders from a court or the Disputes Tribunal may be in addition to compensation under the Privacy Act, and there is no cap on compensation. However, some important pecuniary limitations were introduced to the Act by the Select Committee:

- The court or Disputes Tribunal may not make a compensatory order under the Act for interference with an individual's privacy – the sole remedies for interference are those set out in the Privacy Act.
- The pecuniary penalties for multiple contraventions of a civil liability provision of the same or similar nature that occur at or about the same time will not be aggregated – the total amount of the penalty imposed in that circumstance will be limited to the maximum penalty that could be imposed for a single contravention. So if, for example, multiple data requests could not be fulfilled due to a failure by the data holder to correctly implement a required function, the data holder will not be required to pay a penalty per request.

Regulations will also prescribe specific steps data holders and requestors must take to avoid, remedy or mitigate loss caused by any breach of the legislation (including the requestor's liability for unauthorised payments discussed above).

MBIE and the Privacy Commissioner will need to agree a Memorandum of Understanding to clarify their roles and responsibilities where both privacy and non-privacy considerations are involved.

Charging for regulated data services

The Act anticipates data holders being able to charge for providing regulated data services to requestors. It also provides for regulations to be made setting requirements for how charges can be applied (and identifies caps on charges as an example of what the regulations might cover).

Under Australia's CDR rules, data holders are prevented from charging for access to mandatory data, and from imposing conditions, restrictions or limitations of any kind on the use of the disclosed data by requestors and customers. Similarly, in the UK basic open banking API requests are free, although fees can be charged for access to voluntary "premium" APIs.

The Open Banking Discussion Document starts the discussion on what fees should be permitted to be charged in respect of both account information and payments. MBIE doesn't recommend any option and simply consulted on the possibilities for charging for requests:

1	No charge/free.
2	Subject to pricing limits and tiers set by regulations.
3	Subject to pricing principles set by regulations for example, requiring them to be fair and transparent and in line with efficient long-run costs.
4	Left to commercial negotiation.
5	For payment fees, left to regulation by the Commerce Commission under the Retail Payment System Act. This could be an option if the interbank payment network were designated under that Act.

The Government will recover its own costs associated with the CaPD regime through fees and levies on a user-pays basis, as is customary for regulatory regimes.

Regulation of pricing is a key open issue under the legislation. While overseas regimes have either prevented or severely restricted charges for regulated data services, this has not necessarily incentivised appropriate investment in security, data quality and innovation. For open data regimes to operate effectively and prosper into the future, the interests of all participants need to be considered and taken into account – including ensuring a sustainable commercial model for all.

Stakeholder engagement

Overseas regimes have encountered problems with delays in implementation and some issues with the quality of data provided by data holders.

It will be important for MBIE to incorporate feedback from parties who have experienced these issues, to understand how we can avoid similar traps in New Zealand.

In this context, we need to acknowledge that a significant amount of time, cost and effort is required from data holders to deliver their regulatory obligations – from putting in place the technology and security arrangements to complying with the significant record-keeping obligations the Act imposes (and much more besides).

The regime will work better if it is designed with all parties' interests in mind – setting realistic targets and timeframes and establishing a genuine dialogue with data holders and requestors, rather than imposing unrealistic requirements from on high. The Select Committee recognised this in its report on the Act, stating that the legislation should "reflect the policy intent of fostering a stakeholder-led approach and [provide] assurance that an appropriate range of interests would be represented". The Select Committee also made a change to the Act to require MBIE when making standards to have regard to whether they support consistency and interoperability across multiple sectors.

Encouragingly, both MBIE's discussion documents show a willingness to follow a consultative and open-minded approach.

05 What next?

Engagement on regulations, standards and designations continues, with the Minister of Commerce and Consumer Affairs Scott Simpson stating during the last readings of the Act that he will be seeking Cabinet approval on an open banking designation "very shortly" and is committed to having open banking "fully operational" by the end of 2025.

If proposed timeframes are maintained, the open banking regime will commence on 1 December 2025 for ANZ, ASB, BNZ and Westpac. It will take effect for Kiwibank in relation to payments on 1 June 2026. Kiwibank will be required to provide customer data from 1 December 2026.

The timing to implement a CDR for the electricity sector is less well-defined, with MBIE saying at this stage that, depending on "subsequent Government decisions on whether to progress an electricity sector CDR designation", there will be further consultation on the technical regulations and standards, and more detail on the next steps will be provided "when known".

06 Regulations and standards

The Act leaves a number of important matters to be dealt with in regulations or standards. These include:

1.
Who is considered a "data holder" under the regime, as well as the data or classes of data that are to be regulated. (The coverage of the regime should expand over time, following consultation.)

2.
Technical or performance requirements for data holders' electronic systems. This could include requirements and standards relating to security, data quality and reporting.

3.
The giving of consent or authorisation by customers in relation to their data, including methods for customers to give, view, modify or revoke their consent. Regulations may also provide for consent to be automatically revoked in certain circumstances (for instance, when a customer closes their account with a data holder).

4.
Standards that data holders and accredited requestors will have to meet in connection with their customers' consent – for example, they may be required to take steps to ensure their customers are reasonably informed. Regulations may also prescribe how data holders and accredited requestors deal with requests from joint customers (for instance, holders of a joint bank account).

5.
How data holders are expected to confirm that the service they are providing to a customer is within the scope of the customer's consent, and to verify the identity of both the customer and the accredited requestor.

6.
What sort of information data holders and accredited requestors are required to keep, and for how long.

7.
The criteria against which an application to become an accredited requestor will be considered.

8.
Any fees payable by accredited requestors.

07 Table of regulations

TOPIC	COMMENT	REFERENCE
Ambit of the Act	Regulations will specify who are “data holders” for the purposes of the Act, as well as what data will be considered “customer data” and “product data” and therefore regulated under the Act.	Sections 6, 8 and 9
Refusing request for data	Regulations may specify the circumstances where a data holder may refuse to provide any data requested under sections 14 and 15.	Section 16
Refusing to perform actions	Regulations may specify the circumstances where a data holder may refuse to perform any action requested under sections 18 and 19.	Section 20
Joint customers	Regulations may prescribe ways in which joint customers can make requests or give authorisations, and how data holders and accredited requestors may (or must) deal with these requests or authorisations.	Section 21
Refusing request for data	Regulations may specify the circumstances where a data holder may refuse a request for data despite section 22.	Section 23
Secondary users	Regulations may prescribe when or how a customer may give, view, change or revoke authority to a “secondary user” (e.g. a staff member of a business) to make requests or give authorisations. Regulations may also require requests to be made or authorisations to be given only by secondary users.	Sections 24 and 25
Valid requests	Regulations may prescribe the manner in which a request is valid.	Section 26
Data holders’ electronic systems	Regulations or standards may prescribe technical or performance requirements for the electronic systems used by data holders. These may relate to matters including security, data quality or reporting functionality.	Section 28
General requirements for data holders	Regulations may be made that: (a) Impose requirements on data holders about how much they can charge in connection with regulated data services; (b) Require data holders to notify or otherwise make available information to a person under section 31(3); (c) Specify the manner in which requests for regulated data services are received and responded to; (d) Specify the manner in which authorisations are confirmed under section 39(2).	Sections 31 and 32

TOPIC	COMMENT	REFERENCE
General requirements for accredited requestors	Regulations may be made that require data holders to notify or otherwise make available information to a person under section 33(2).	Sections 33 and 34
Contravention of specified disclosure requirement	Regulations will specify the disclosure requirements which contravention of is an infringement offence.	Section 35
Authorisation	Under the Act, a customer or secondary user on their behalf can give authorisation in a manner prescribed by the regulations and standards. Regulations may provide for a customer's authorisations to be modified, or to end on the occurrence of a specified event (e.g. where a customer closes their account with a data holder). They may also prohibit authorisations being given in certain circumstances. Data holders and accredited requestors who have confirmed or received a customer's authorisation must have systems in place to enable the customer to view or end that authorisation. There may be regulations and standards that set out certain requirements that these systems must meet.	Sections 37, 38, 40 and 41
Confirmation	Where a data holder receives a request from an accredited requestor to provide a regulated data service, the data holder must check that the service is within the scope of the authorisation given by the customer. This is called "confirmation". The regulations and standards may prescribe the way in which data holders carry out this confirmation.	Section 39
Verification	Before data holders provide a service, they must verify the identity of the person who makes a request. Regulations and standards may set requirements for carrying out this verification process.	Section 45
Record-keeping	Regulations may specify types of information that data holders and accredited requestors must keep records of, and in what manner.	Sections 46 and 47
Complaints and dispute resolution scheme	Data holders and accredited requestors must have a customer complaints process and ensure it meets the requirements provided for by any regulations. Regulations may also prescribe and require data holders and accredited requestors to be a member of a dispute resolution scheme. The rules of a scheme may be changed, and the regulations may disapply any requirement or restriction imposed under any other legislation.	Sections 48, 49 and 50

TOPIC	COMMENT	REFERENCE
Duties to take remedial action	Where data holders or accredited requestors contravene a duty in the Act (or the regulations), and a customer suffers or is likely to suffer loss or damage as a result, the regulations may require data holders or accredited requestors to take certain steps to avoid, mitigate or remedy that loss or damage.	Section 58
Infringement offences	Regulations will prescribe the form for an infringement notice and reminder notice.	Sections 65 and 68
Defences	Regulations or standards will prescribe and specify the CPD reliability and availability requirements that apply to the defences specified.	Sections 89 and 90
General regulatory power	The Governor-General is given a broad power to make regulations prescribing matters, procedures and requirements under the Act. This includes prescribing fees and charges payable to the Chief Executive of MBIE by accredited requestors, as well as exempting any classes of persons from any requirement under the Act.	Sections 104-107 and 131-133
Accreditation	Regulations may prescribe the information an applicant must provide to apply to become an accredited requestor, as well as the manner in which the application must be made, and the relevant fee. They may also prescribe criteria for becoming an accredited requestor, the matters the Chief Executive must have regard to when considering an application, and the manner in which the Chief Executive makes their decision.	Sections 109 and 112
Register	The Chief Executive will keep an electronic register, in accordance with regulations, containing information about data holders and accredited requestors. Persons that will become data holders and other data holders under designation regulations must provide information to the Chief Executive within 20 working days of becoming aware that they have become a data holder. Regulations may prescribe the information to be provided for inclusion in the register, as well as the way in which that information must be provided by the data holder. The content of the register will be prescribed by regulations.	Sections 123-127
Levy	Regulations will specify the levies payable by data holders and accredited requestors, including the classes of specified persons required to pay, amount, payment, collection, and other requirements.	Section 135

08 A bit about us

We are corporate, commercial and dispute lawyers specialising in technology, media and intellectual property. We help clients of all sizes navigate the constantly changing world of business in the digital age.

As one of the largest and most experienced legal teams in the country focused on technology, IP, data and their impact on business, our expertise spans various domains and industries.

To explore how this new regime could affect your business, and plan for an open data future, please get in touch.

Simon Martin
Partner
simon.martin@hgmlegal.com

A founding partner, Simon understands the challenges thrown at businesses and enjoys working with them to help maximise the value that can be gained from technology.

Author

Andrew Dentice
Partner
andrew.dentice@hgmlegal.com

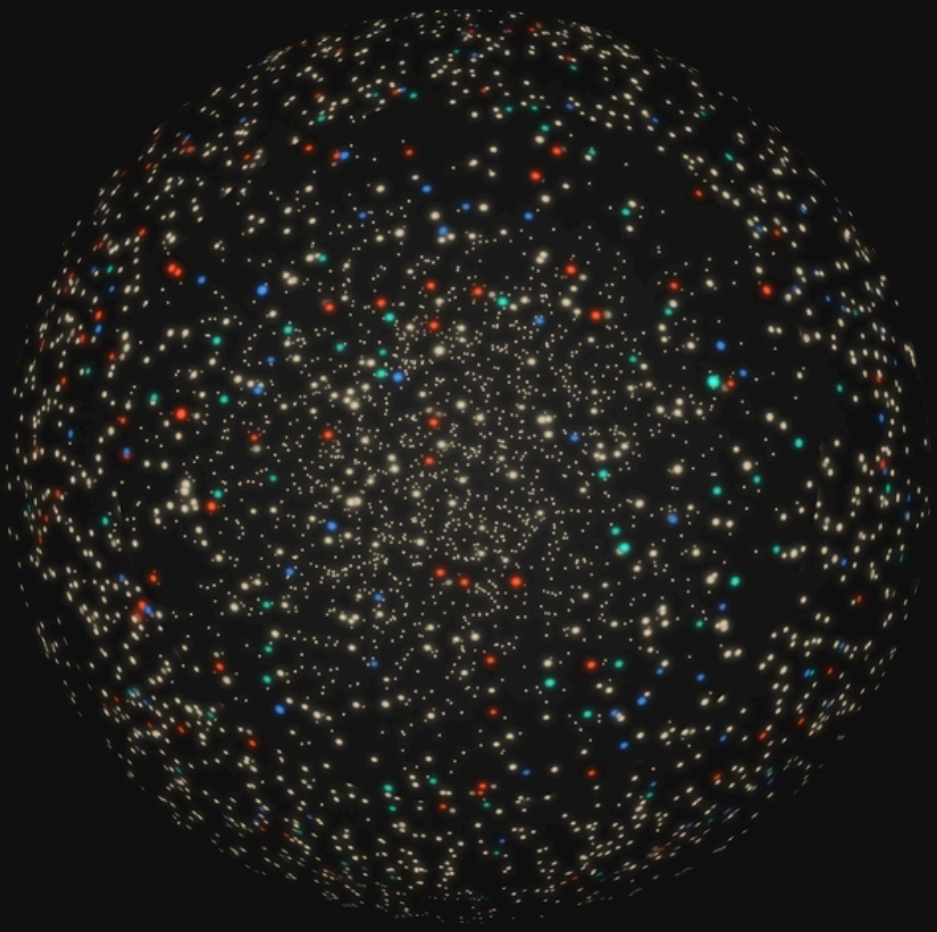
Andrew is an expert in fintech, technology transactions, data protection and commercialisation, and regulatory issues applying to technology.

Anchali Anandanayagam
Partner
anchali.anandanayagam@hgmlegal.com

Anchali specialises in data protection and transactions where technology (including AI), media and telecommunications assets are at the core.

Ed Lim
Partner
edwin.lim@hgmlegal.com

Ed is known for his unique blend of tech and legal expertise, and offers comprehensive advice on business technology issues.



HGM Insights

Scan the QR code to see our latest Insights.

www.hgmlegal.com